COLUMBIA LAW REVIEW

VOL. 117 OCTOBER 2017 NO. 6

ARTICLE

PAYING FOR PRIVACY AND THE PERSONAL DATA ECONOMY

*Stacy-Ann Elvy**

Growing demands for privacy and increases in the quantity and variety of consumer data have engendered various business offerings to allow companies, and in some instances consumers, to capitalize on these developments. One such example is the emerging "personal data economy" (PDE) in which companies, such as Datacoup, purchase data directly from individuals. At the opposite end of the spectrum, the "pay-for-privacy" (PFP) model requires consumers to pay an additional fee to prevent their data from being collected and mined for advertising purposes. This Article conducts a simultaneous in-depth exploration of the impact of burgeoning PDE and PFP models. It identifies a typology of data-business models, and it uncovers the similarities and tensions between a data market controlled by established companies that have historically collected and mined consumer data for their primary benefit and one in which consumers play a central role in monetizing their own data.

The Article makes three claims. First, it contends that PFP models facilitate the transformation of privacy into a tradable product, may engender or worsen unequal access to privacy, and could further enable predatory and discriminatory behavior. Second, while the PDE may allow consumers to regain a semblance of control over their information by enabling them to decide when and with whom to share their data, consumers' direct transfer or disclosure of personal data to companies for a price or personalized deals creates challenges similar to those found in the PFP context and generates additional concerns associated with innovative monetization techniques. Third, existing frameworks and proposals may not sufficiently ameliorate these concerns. The Article concludes by offering a path forward.

* Associate Professor of Law, New York Law School. For their valuable comments and insights, I am grateful to Julie Cohen, Paul Schwartz, Chris Jay Hoofnagle, Jan Whittington, Peter Swire, Kirsten Martin, Angela Campbell, Olivier Sylvain, Mary Madden, LaVonda Reed, Pamela Foohey, Jim Hawkins, Stephen Sepinuck, Creola Johnson, Heather Hughes, Melissa Lonegrass, Esme Caramello, Bennett Capers and Serena Williams.

INTRODUCTION

> "*The benefits of the Internet have been proven and privacy is in demand and people are willing to pay.*"[1]
>
> Nico Sell, Wickr

> "*It would make for a far more efficient market if consumers were consciously aware of the trade-off occurring with regards to their data, and were able to participate in the value-chain of their data, beyond the opacity of a free app or service that appears unrelated to data sales.*"[2]
>
> Matt Hogan, Datacoup

> "*Prior to Meeco, the power to capture, analyse and profit from personal data has resided with businesses, government and social networks. Meeco flips that model entirely around so that the individual is an equal participant in the value created, controlling the use of his or her personal data derived from every day occurrences and transactions.*"[3]
>
> Katryna Dow, Meeco

In 2017, the *Economist* magazine proclaimed that "the world's most valuable resource is no longer oil, but data."[4] Companies, such as Facebook and Google, have based their business models on collecting and analyzing user data.[5] These companies have amassed vast quantities of data, which "give[] them enormous power."[6]

---

1. Cadie Thompson, The Next Thing You'll Pay for: Your Online Privacy, CNBC (Mar. 7, 2014), http://www.cnbc.com/2014/03/07/the-next-thing-youll-pay-for-your-online-privacy.html [http://perma.cc/ACM5-K93M].

2. Hollie Slade, Here's How Slice Is Monetizing Over Two Million People's Everyday Online Purchases, Forbes (Sept. 26, 2014), http://www.forbes.com/sites/hollieslade/2014/09/26/heres-how-slice-is-monetizing-over-two-million-peoples-every-online-receipt/#1a8db21068a6 [http://perma.cc/773X-EVH2].

3. Liz Leigh, Meeco Is a Life Management Platform that Gives Users Total Control of Their Data, Startup Daily (Apr. 13, 2016), http://www.startupdaily.net/2016/04/meeco-life-management-platform-gives-users-total-control-data/ [http://perma.cc/6XBH-H8RH].

4. Regulating the Internet Giants: The World's Most Valuable Resource Is No Longer Oil, but Data, Economist (May 6, 2017), http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource [http://perma.cc/NRW8-DG7T] [hereinafter Regulating the Internet Giants].

5. See generally Chris Jay Hoofnagle & Jan Whittington, Free: Accounting for the Costs of the Internet's Most Popular Price, 61 UCLA L. Rev. 606, 628 (2014) [hereinafter Hoofnagle & Whittington, Accounting for the Costs] (discussing Facebook's and Google's business models); Nathan Newman, The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google, 40 Wm. Mitchell L. Rev. 849, 865 (2014) (discussing Google's business model).

6. Regulating the Internet Giants, supra note 4.

Established data brokers have played a central role in the market for consumer data.[7] A U.S. Senate Committee on Commerce, Science, and Transportation staff report notes that data brokers compile information about consumers from various sources, including social media and contracts with other businesses.[8] It is estimated that Acxiom, one of the largest data brokers, has approximately twenty-three thousand servers scrutinizing the data of millions of individuals.[9] Once data brokers obtain consumer data, they frequently transfer this information to unaffiliated parties.[10]

The Internet of Things (IOT)—a network of connected devices—presents new opportunities for data brokers and other businesses to collect real-time and increasingly detailed data about the habits, lives, and activities of consumers.[11] Companies that provide IOT consumer products, such as Internet-enabled washing machines, thermostats, baby monitors, and security cameras, can use consumer data for their own purposes, and in many instances these companies may also transfer or disclose this information to third parties.[12] These data include consumption-rate data, location data, health-related data, and recordings of children's voices.[13] Thus, what has "changed [in the data market] is the volume and nature of the data being mined from the Internet[,] . . . mobile

---

7. Staff of S. Comm. on Commerce, Sci. & Transp., 113th Cong., A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes 1 (2013) [hereinafter Staff of S. Comm. on Commerce, Sci. & Transp., Review of the Data Broker Industry]; How Much Is Your Personal Information Worth?, WebpageFX, http://www.webpagefx.com/blog/general/what-are-data-brokers-and-what-is-your-data-worth-infographic/ [http://perma.cc/UHR4-3HLX?type=image] [hereinafter PI Worth] (last visited July 28, 2017).

8. Staff of S. Comm. on Commerce, Sci. & Transp., Review of the Data Broker Industry, supra note 7, at 15.

9. Natasha Singer, Mapping and Sharing the Customer Genome, N.Y. Times (June 16, 2012), http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html (on file with the *Columbia Law Review*); see also PI Worth, supra note 7.

10. Data Brokers and "People Search" Sights, Privacy Rights Clearinghouse (Sept. 1, 2014), http://www.privacyrights.org/consumer-guides/data-brokers-and-people-search-sites [http://perma.cc/4DC6-PBYG] (last updated June 8, 2017).

11. AIG, The Internet of Things: Evolution or Revolution?, 4 (2015), http://www.aig.com/content/dam/aig/america-canada/us/documents/business/casualty/aigiot-english-report.pdf [http://perma.cc/98YJ-MCCC] (last visited July 28, 2017). See generally Stacy-Ann Elvy, Commodifying Consumer Data in the Era of the Internet of Things, 59 B.C. L. Rev. (forthcoming 2018) [hereinafter, Elvy, Commodifying Consumer Data] (on file with the *Columbia Law Review*) (describing the different types of data that can be generated by IOT devices).

12. Elvy, Commodifying Consumer Data, supra note 11, at 5 (describing the various ways in which companies can disclose and monetize consumer data and discussing companies' rights in consumer-generated data).

13. Adam Greenfield, Rise of the Machines: Who Is the 'Internet of Things' Good for?, Guardian (June 7, 2017), http://www.theguardian.com/technology/2017/jun/06/internet-of-things-smart-home-smart-city [http://perma.cc/7L9H-9ZTP] (discussing consumption, health and biometric data, and IOT devices).

devices [and IOT devices]."[14] As former Federal Trade Commission (FTC) Commissioner Julie Brill has noted, consumers are losing "control over [their] most private and sensitive information."[15]

Today, companies have developed various approaches to monetizing consumer data and privacy to exploit the rising data gold rush and corresponding demands for more privacy. The discount pay-for-privacy (PFP) approach—which requires consumers to pay higher fees to avoid data collection and targeted advertisements while offering discounts to consumers who consent to these practices—is the latest business scheme to receive widespread attention.[16] In other types of PFP offerings, companies simply charge higher prices for products that offer more privacy controls and data protection without encouraging consumers to consent to data tracking and disclosures by providing discounts.[17]

At least one Internet service provider (ISP) previously implemented a PFP discount program. In response to the Federal Communications Commission's (FCC) privacy rules (FCC Rules), some ISPs contended in 2016 that they should be permitted to charge higher prices to consumers who want to opt out of tracking and the use of their data for advertisement purposes.[18] The FCC Rules would have imposed various notice-and-consent requirements and were intended to "give consumers the tools they need to choose how their [ISPs] use and share their personal data."[19] Congress subsequently repealed the FCC Rules and the FCC's

---

14. Steve Kroft, The Data Brokers: Selling Your Personal Information, CBS News (Mar. 9, 2014), http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/ [http://perma.cc/K6MP-HM2L].

15. Julie Brill, Demanding Transparency from Data Brokers, Wash. Post (Aug. 15, 2013), http://www.washingtonpost.com/opinions/demanding-transparency-from-data-brokers/2013/08/15/00609680-0382-11e3-9259-e2aafe5a5f84_story.html?utm_term=.da2a9a935d04 [http://perma.cc/A6Z9-G95X].

16. Letter from Senator Elizabeth Warren to Tom Wheeler, Chairman, FCC 2 (June 21, 2016) [hereinafter Warren Letter], http://www.warren.senate.gov/files/documents/2016-6-21_Letter_to_FCC_re_Privacy_Rulemaking.pdf [http://perma.cc/9WWT-7362] (describing Internet service provider discount plans as "requir[ing] consumers to pay hundreds of dollars extra each year so that [a company] does not collect and sell information on the websites they visit, the ads they see, and the terms they enter into search engines").

17. See infra section II.B.1.

18. Curtis Silver, Comcast Wants to Charge You Less for Broadband at the Expense of Privacy, Forbes (Aug. 4, 2016), http://www.forbes.com/sites/curtissilver/2016/08/04/comcast-broadband-privacy-fcc/#6a2308e6226d [http://perma.cc/PTW9-5KRP] (reporting that Comcast wants to "present lower tiered broadband options to customers who have no problem with their data being mined and exposed to advertisers"); see also Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274 (Dec. 2, 2016), repealed by Act of Apr. 3, 2017, Pub. L. No. 115-22, 131 Stat. 88 (codifying a joint resolution disapproving of the FCC "Broadband and Telecommunications Services" privacy rules).

19. Fact Sheet: FCC Adopts Order to Give Broadband Consumers Increased Choice over Their Personal Information, FCC [hereinafter FCC Fact Sheet], http://apps.fcc.gov/edocs_public/attachmatch/DOC-341938A1.pdf (on file with the *Columbia Law Review*) (last visited July 28, 2017).

ability to adopt similar rules in the future appears to be restricted.[20] Industry trade associations filed several petitions attacking various aspects of the FCC Rules, including the notice and customer-approval requirements that would have been applicable to PFP discount programs.[21] The repeal of the FCC Rules is concerning in light of the common carrier exemption under the Federal Trade Commission Act and ongoing litigation challenging the FTC's ability to regulate certain potentially harmful practices of common carriers.[22] These recent developments suggest that the issues this Article evaluates are timely and significant.

While ISPs and other companies have been busy finding new ways to capitalize on consumer data and demands for privacy, the growing "personal data economy" (PDE) threatens to challenge the central role of data brokers and other established companies in the consumer data market. The PDE is a "user-centric" data concept that permits "individuals [to] take ownership of their information so they can share it with businesses on their terms."[23] Commentators use various names to describe the PDE, including "the API of Me" and the "Internet of Me."[24] In the last few years several domestic and foreign Internet start-ups, such as Datacoup, Digi.me, and Meeco, have emerged with the stated goal of allowing consumers to choose what data they share and disclose to businesses.[25] PDE companies depend significantly on consumers, rather than data brokers and conventional businesses, to provide consumer data, and some provide a venue for consumers to monetize their own data.[26]

---

20. See 131 Stat. at 88 (codifying a joint resolution disapproving of the FCC "Broadband and Telecommunications" Services privacy rules); 163 Cong. Rec. S1941 (daily ed. Mar. 23, 2017) (statement of Sen. McConnell regarding the Congressional Review Act resolution to disapprove of the FCC privacy rules); see also 5 U.S.C. § 801(b)(2) (2012) (noting that a rule that is "substantially the same" as an agency rule disapproved under the Congressional Review Act "may not be reissued" unless "specifically authorized by a law"); Jenna Ebersole, Trump Signs Bill Nixing FCC's Broadband Privacy Rules, Law360 (Apr. 3, 2017), http://www.law360.com/articles/908812/trump-signs-bill-nixing-fcc-s-broadband-privacy-rules [http://perma.cc/8FHN-97H2].

21. Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., 32 FCC Rcd. 1793, 1794 (Mar. 1, 2017) (granting stay petition in part).

22. See FTC v. AT&T Mobility LLC, 835 F.3d 993, 998 (9th Cir. 2016) (reasoning that the common carrier exemption under the Federal Trade Commission Act is a "status-based" exemption), reh'g en banc granted, No. 15-16585, 2017 WL 1856836, at *1 (9th Cir. May 9, 2017).

23. Mobile Ecosystem Forum, Understanding the Personal Data Economy: The Emergence of a New Data Value-Exchange 3 [hereinafter MEF White Paper], http://mobileecosystemforum.com/wp-content/uploads/2016/11/Understanding-the-Personal-Data-Economy-Whitepaper.pdf [http://perma.cc/A6HZ-W79T] (last visited July 28, 2017).

24. Id.

25. Id.

26. Id.; see also Jaron Lanier, Who Owns the Future 20 (2014) (describing a proposal similar to PDE monetization options in which consumers are compensated with "nanopayments" for their contributions to customer databases).

Some PFP and PDE models adopt seemingly divergent approaches to consumer privacy and data collection. The discount PFP program maintains the existing data-market model whereby the benefits of mined consumer data flow primarily between companies, with the added twist that consumers can pay extra fees to avoid data collection and disclosures.[27] In contrast, PDE programs are described as empowering consumers to extract value from their own data by, for instance, selling or providing access to their information to data buyers.[28]

PFP and PDE models raise crucial questions about data collection, privacy, and the role of consumers in the data market. Are PFP programs that offer discounts to consumers that consent to data collection, data disclosures, and data transfers beneficial to consumers? In the PDE setting, will companies give consumers the opportunity to play a meaningful role in negotiating data trade terms with PDE companies and unaffiliated entities as well as in determining who can subsequently obtain and use their data? If consumers are provided with a marketplace to actively monetize their own information, should restrictions be imposed on the ability of parents to monetize the data of their children pursuant to agreements with PDE companies? Should landlords be able to monetize data generated by renters to obtain discounts from companies? Should landlords be permitted to require renters to consent to providing access to their social media accounts or data from household IOT devices to enable PDE companies to provide landlords with insights about renters? What legal frameworks should be used to structure and govern agreements between PDE companies and consumers? Should courts view PDE data-exchange arrangements as enforceable contracts if significant portions of the terms of the arrangement are contained in a privacy policy?[29] Are there new ways in which high-value, data-generating consumers can begin to monetize their own data—for instance, by using their data as collateral to obtain financing in a transaction subject to Article 9 of the Uniform Commercial Code (UCC)?

Rather than seeking to provide complete and comprehensive answers to all of these inquiries, this Article aims to evaluate these questions with the goal of generating discourse about the long-term viability

---

27. See, e.g., Warren Letter, supra note 16, at 2 (describing the practice of ISPs that charge consumers extra fees to prevent the provider's collection and sale of their data).

28. See generally Tony Abraham & Marguerite Oneto, Consumers as Data Brokers: Should They Sell Their Own Personal Data? 1–5 (May 6, 2015) (unpublished student paper, University of California, Berkeley), http://www.ischool.berkeley.edu/sites/default/files/projects/abraham-oneto-final-paper.pdf [http://perma.cc/T7ZS-YGTG] (suggesting the PDE model may give consumers more control over their privacy).

29. See Pamela Samuelson, Privacy as Intellectual Property?, 52 Stan. L. Rev. 1125, 1137 (2000) (describing a licensing framework for the privacy market prior to the rise of the PDE); Abraham & Oneto, supra note 28, at 4 (hypothesizing a world of personal data markets).

of PFP and PDE models and their potential impact on consumers.[30] In doing so, this Article makes contributions to pressing privacy debates about how regulators, legislators, and courts should respond to the collection, transfer, disclosure, and use of consumer data.

The Article makes three points. First, it contends that PFP models facilitate the transformation of privacy into a tradable or luxury product that is primarily affordable by a select few, subsequently engendering or worsening unequal access to privacy and further enabling predatory and discriminatory behavior.

Second, while the PDE may seemingly allow consumers to regain a semblance of control over their information by enabling them to decide "when and with whom to share their data,"[31] the direct transfer or disclosure of personal data by consumers to companies for a price or personalized deals creates challenges similar to those found in the PFP context. The PDE also generates additional concerns associated with innovative monetization options, including the possible monetization of the data of minors and renters. As more domestic companies begin to adopt the PDE model, these concerns may become more prevalent. Some PDE companies may subsequently monetize consumer data. If data access and transfer restrictions are not imposed, it may be possible for the data to be bought by or disclosed to data brokers after the initial transfer or disclosure by the consumer for a meager price or customized discounts. Data transferees may use user data to make inferences about consumer preferences as well as combine PDE data with consumer data from other sources.

Third, current frameworks, such as the Children's Online Privacy Protection Act (COPPA) and other regulatory responses suffer from several limitations and may not consistently remedy the concerns noted

---

30. Legal scholars have addressed related questions; however, this Article focuses on the nascent PDE and PFP models. See generally Ian Ayres & Matthew Funk, Marketing Privacy, 20 Yale J. on Reg. 77, 96–97 (2003) (proposing a consumer opt-in regime for telemarketing); Scott R. Peppet, The Unraveling of Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future, 105 Nw. U. L. Rev. 1153, 1162–63 (2015) [hereinafter Peppet, The Unraveling of Privacy] (discussing the signaling economy); Paul M. Schwartz, Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2055, 2066–68 (2004) [hereinafter Schwartz, Property, Privacy, and Personal Data] (discussing issues regarding compensating consumers for agreeing to listen to telemarketing calls); Adam B. Thimmesch, Transacting in Data: Tax, Privacy, and the New Economy, 94 Denv. L. Rev. 145, 157–81 (2016) (discussing the tax implications of the personal-data market); Scott R. Peppet, Smart Mortgages, Privacy and the Regulatory Possibility of Infomedia 5 (Univ. of Colo. Law Sch., Working Paper No. 09-13, 2009) (calling for "fiduciary information intermediaries to serve as trustees to sensitive information flows"); Abraham & Oneto, supra note 28 (discussing PDE companies exclusively).

31. Dutch eHealth Start-Up 112Motion Introduces Wearable and a New Open Healthcare Platform, Medica Mag. (Oct. 3, 2016), http://www.medica-tradefair.com/cgi-bin/md_medica/lib/pub/tt.cgi/Dutch_eHealth_start-up_112Motion_introduces_wearable_and_a_new_open_healthcare_platform.html?oid=81828&lang=2&ticket=g_u_e_s_t [http://perma.cc/L2CT-ZFXZ].

above. For instance, COPPA, the main federal statute governing the data and privacy of children, is limited to protecting the information of children under the age of thirteen.[32] Statutory and regulatory frameworks that rely excessively on a notice-and-choice model are unlikely to adequately protect the interests of consumers in the IOT setting.[33] A sectoral approach to privacy may also lead to regulatory gaps.

While there will likely be various instances in which PFP and PDE models may be problematic, the Article not only highlights concerns about discriminatory and predatory behavior and unequal access to privacy faced by low-income consumers but also concentrates on the potential impact of PDE models on children and tenants. The Article focuses on these groups for several reasons. Housing is a necessity, and evidence suggests that members of marginalized groups are more likely to rent.[34] Poor families contribute a significant share of their income to rent.[35] Moreover, children are particularly vulnerable to exploitation. The digital dossiers that may be compiled about children from a young age may have long-term consequences once a child reaches adulthood. The ubiquitous nature of IOT toys, social networks, and various devices that minors use to access the Internet ensure that children begin leaving digital footprints much earlier than previous generations.[36]

The Article concludes by proposing initial steps to alleviate potential concerns associated with PFP and emerging PDE models. These steps include, among other things, restrictions on the use of PFP discount programs in industries that provide products that are necessary for equal participation by citizens in the digital age; recommendations to PDE companies to ensure that consumers have sufficient control over their data; evaluations of whether restrictions should be imposed on the monetization of certain types of data, including the data of children and renters; guidance on the best ways to structure PDE agreements; and

---

32. 15 U.S.C. § 6501(1) (2012); see also Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814, 1891–92 (2011) [hereinafter Schwartz & Solove, The PII Problem] (noting limitations of the COPPA framework, including that it applies only to children under the age of thirteen).

33. See Elvy, Commodifying Consumer Data, supra note 11, at 10.

34. Matthew Desmond, Inst. for Research on Poverty, Fast Focus: Unaffordable America: Poverty, Housing and Eviction 1 (2015) [hereinafter Desmond, Unaffordable America], http://www.irp.wisc.edu/publications/fastfocus/pdfs/FF22-2015.pdf [http://perma.cc/W3J8-HKWF] (noting that the majority of African American and Hispanic families rent their homes); see also Matthew Desmond, Housing, Pathways, Special Issue 2017, at 16, 16, http://inequality.stanford.edu/sites/default/files/Pathways_SOTU_2017.pdf [http://perma.cc/TY23-KEMK] ("Whereas 71 percent of white families live in owner-occupied housing, only 41 percent of black families and 45 percent of Hispanic families do.").

35. See Desmond, Unaffordable America, supra note 34, at 1.

36. See generally Amanda Lenhart, Pew Research Ctr., Teens, Social Media & Technology Overview 2015 (2015), http://www.pewinternet.org/files/2015/04/PI_TeensandTech_Update2015_0409151.pdf [http://perma.cc/XVN3-ZWLC] (discussing recent trends in social media and technology use by teenagers).

increased regulation of existing data brokers and PDE markets to ensure that PDE companies keep their promises of providing consumers with control over their data.

The remainder of this Article proceeds as follows: Part I evaluates the role of the rapid expansion of the IOT, increases in the quantity and variety of data, and the large number of prominent data breaches and leaks. These developments have likely created an atmosphere in which consumers desire some level of privacy, data control options, and data security. This Part suggests that given potential increases in data volume and quality and privacy demand, it is not surprising that companies are offering and generating various programs to exploit these developments.

Part II identifies a typology of data business models for use by scholars doing future work in this area and highlights the connections between older data business schemes and PDE and PFP programs.

Part III argues that while some of the concerns highlighted in earlier data models discussed in Part II can also be found in both PFP and PDE models, these new schemes may widen the gap between the "privacy haves and have-nots."[37] Moreover, these models may permit companies to continue to monetize consumer data to the detriment of consumers and engage in predatory and discriminatory behavior while hiding behind the veneer of consumer empowerment and control. These challenges, as well as issues associated with how to structure monetization transactions involving consumers, must be addressed.

In light of the concerns discussed in previous sections, Part IV evaluates the efficacy of existing legislation and regulatory responses, such as COPPA; the activities of the FTC; and recent proposals to restore the FCC Rules. Part V concludes by discussing a path forward to begin addressing the concerns noted in this Article. PDE companies face significant challenges that must be considered in order to effectuate socially beneficial change across the data market.

I. PRIVACY DEMAND AND DATA VOLUME

The precipitous growth of the IOT and the frequently reported data leaks suffered by large companies will likely contribute to an environment in which consumer demands for privacy and data security rise along with increases in the quantity and types of consumer data. This presents various opportunities for companies to monetize consumer privacy.

---

37. Colin J. Bennett & Rebecca Grant, Conclusion, *in* Visions of Privacy: Policy Choices for the Digital Age 263, 266 (Colin J. Bennett & Rebecca Grant eds., 1999) (discussing the "privacy haves and have-nots"). See generally Colin J. Bennett & Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective 40 (2003) (same).

The IOT is expected to have a substantial impact on the lives of consumers.[38] Increasingly, ordinary objects, such as refrigerators and washing machines, are being connected to the Internet. Technology consulting firms project that by 2020 there will be billions of Internet-enabled devices "in use worldwide."[39] These IOT devices will likely provide convenience and efficiency to consumers. However, this increased level of connectivity simultaneously provides multiple opportunities for everyday objects to serve as continuous surveillance equipment that monitors and collects data about the activities of consumers.

A 2017 FTC staff report illustrates this problem.[40] Companies are frequently using cross-device tracking—connecting the activities of users "across [their] smartphones, tablets, desktop computers," and IOT devices—to collect information about consumers.[41] Companies can pervasively monitor consumers' activities and behaviors and create a "device graph"—"a map of devices attached to each consumer, their devices and home."[42] Cross-device tracking allows consumers to access their various online accounts from several devices and supports businesses' goals to combat fraud—for instance, by flagging unknown devices.[43] However, companies can combine a consumer's device graph data with offline information for data analytics and targeted advertising purposes.[44] Cross-device tracking can also be done not only by the company that provides the initial service or product to the consumer but also by third-party businesses.[45] Companies frequently do not adequately disclose cross-device tracking to consumers.[46] The FTC's review of the privacy policies of one hundred top websites uncovered only three privacy policies that specifically addressed "third-party cross-device tracking."[47]

---

38. See generally Scott R. Peppet, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85 (2014) [hereinafter Peppet, Regulating the Internet].

39. Press Release, Gartner, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016 (Feb. 7, 2017), http://www.gartner.com/newsroom/id/3598917 [http://perma.cc/56R3-8AYR].

40. FTC, Cross-Device Tracking, at ii (2017) [hereinafter FTC Cross-Device Report], http://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf [http://perma.cc/EF7V-JSQU].

41. Id. at i.

42. Id. Other scholars have also forecasted the effects of "privacy-destroying technologies" prior to the rise of the IOT. See generally A. Michael Froomkin, The Death of Privacy?, 52 Stan. L. Rev. 1461 (2000).

43. FTC Cross-Device Report, supra note 40, at 5.

44. Id. at i.

45. Id. at 3–4, 8.

46. Id. at 8.

47. Id.

Despite this lack of disclosure and the likelihood that consumers may not thoroughly understand the implications of continuous cross-device tracking, surveys indicate that a significant number of consumers are using various self-help measures to protect their privacy.[48] A Pew Research Center survey found that approximately eighty-six percent of Americans have tried to hide their online activities by deleting cookies and encrypting emails, and fifty-five percent of those surveyed have also "taken steps to avoid observation by specific people, organizations, or the government."[49] Results from another report indicate that at least 309 million consumers currently use advertisement-blocking tools,[50] and another study found that thirty-two percent of American respondents use these tools because of concerns about privacy.[51] These studies suggest that consumers have some level of awareness about the extent to which their online activities are being monitored.

In the IOT setting, a consumer's online activity now includes the performance of ordinary tasks, such as doing laundry using an Internet-enabled washing machine[52] and drinking water from an Internet-enabled Brita water pitcher.[53] Thus, in the age of the IOT "virtually every activity creates a digital trace—more raw material for the data distilleries."[54]

Given that the nature of online activities has expanded, it is not surprising that the IOT and the development of smart cities provide new opportunities for companies and institutions to track consumer activities and behaviors. In a case currently before the Seventh Circuit, the court has to determine whether Fourth Amendment protection extends to data smart-city readers collect regarding citizens' energy usage.[55] The meters

---

48. Id. at 8–9.

49. Lee Rainie et al., Pew Research Ctr., Anonymity, Privacy, and Security Online 2 (2013), http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf [http://perma.cc/66XH-A8CR].

50. PageFair, Adblocking Goes Mobile 5 (2016), http://pagefair.com/downloads/2016/05/Adblocking-Goes-Mobile.pdf [http://perma.cc/4E4U-4QNB].

51. FTC Cross-Device Report, supra note 40, at 9 (citing Mimi An, Hubspot Research, Why People Block Ads: And What It Means for Marketers and Advertisers 8 (2016), http://research.hubspot.com/reports/why-people-block-ads-and-what-it-means-for-marketers-and-advertisers [http://perma.cc/BBH6-YEMQ]).

52. See, e.g., Connected Washers & Dryers, GE Appliances, http://www.geappliances.com/ge/connected-appliances/washer-dryer-laundry.htm [http://perma.cc/7644-36UK] (last visited July 28, 2017).

53. See, e.g, Brita Infinity Wi-Fi Connected Pitcher, Brita, http://www.brita.com/water-pitchers/infinity [http://perma.cc/AK4D-VNZ4] (last visited July 28, 2017).

54. Regulating the Internet Giants, supra note 4.

55. Allison Grande, Smart Meter Data Needs Privacy Protection, 7th Circ. Told, Law360 (Mar. 2, 2017), http://www.law360.com/articles/897628/smart-meter-data-needs-privacy-protection-7th-circ-told [http://perma.cc/Y3P4-3CNF] [hereinafter Grande, Smart Meter Data]; see also Naperville Smart Meter Awareness v. City of Naperville, No. 11 C 9299, 2016 WL 5373052 (N.D. Ill. Sept. 26, 2016) (granting summary judgment in favor of the city), appeal docketed, No. 16-3766 (7th Cir. Oct. 26, 2016); Naperville Smart Meter Awareness v. City of Naperville, 69 F. Supp. 3d 830, 841 (N.D. Ill. 2014) (granting defendant's motion

at issue generate 2,880 readings per month, in contrast to predecessor analog meters that "provided only a single monthly assessment, and a single reading per month."[56] The meters also allegedly provide information about the time at which the energy was used by the homeowner.[57]

The copious quantities of data that consumers generate from use of everyday objects that are now connected to the Internet will increase the amount of data and information about consumers and members of their households and communities that are available for collection, analytics, disclosure, and transfer to third parties. This new wealth of data can be used to more accurately make inferences about consumer preferences and to target consumers for contracting.[58]

Additionally, in the IOT setting, "Cyberattacks and data breaches are facts of life for government agencies, businesses and individuals alike . . . ."[59] Notable cyberattacks have involved the Democratic National Committee and Yahoo.[60] The recent voter-data leak suffered by Deep Root Analytics, a data analytics company employed by the Republican National Committee, exposed the profiles of almost 200 million voters.[61] A 2016 survey of consumer responses to the prevalence of data breaches found that sixty-four percent of Americans "have personally experienced a major data breach, and relatively large shares of the public lack trust in key institutions . . . to protect their personal information."[62] A 2017 report on consumer attitudes in ten countries, including the United States, found that forty-nine percent of respondents were concerned that their information could be stolen, and forty-eight percent were worried that their data could be disclosed without their permission.[63]

---

to dismiss plaintiff's amended complaint alleging Fourth Amendment claims, among other things). Additionally, the Supreme Court's anticipated decision in *Carpenter v. United States* is expected to address the connections between data collection and disclosures and privacy expectations in specific circumstances. See United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016) (holding that "the government's collection of business records containing cell-cite [location] data was not a search under the Fourth Amendment"), cert. granted, 137 S. Ct. 2211 (2017).

56. Grande, Smart Meter Data, supra note 55.

57. Id.; see also *Naperville Smart Meter Awareness*, 69 F. Supp. 3d at 836.

58. Regulating the Internet Giants, supra note 4 ("Algorithms can predict when a consumer is ready to buy . . . or a person is at risk [of] a disease.").

59. Kenneth Olmstead & Aaron Smith, Pew Research Ctr., Americans and Cybersecurity 3 (2017), http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf [http://perma.cc/86SM-QEP5].

60. Id.

61. Natasha Bertrand, GOP Data Firm that Exposed Millions of Americans' Personal Information Is Facing Its First Class-Action Lawsuit, Bus. Insider (June 22, 2017), http://www.businessinsider.com/deep-root-analytics-sued-after-data-breach-2017-6 [http://perma.cc/TE98-SMZJ].

62. Olmstead & Smith, supra note 59, at 3.

63. Mobile Ecosystem Forum, Global Consumer Trust Report 2017, at 21 (2017) [hereinafter MEF 2017 Consumer Report], http://mobileecosystemforum.com/wp-content/uploads/2017/06/MEF_Global_Consumer_Trust_Report_2017.pdf [http://perma.cc/HB9H-

The IOT will significantly impact the app economy, which is already a $143 billion market.[64] The IOT is expected to "drive the development of millions of new [mobile] apps"—software programs that facilitate access to services and other products.[65] In some instances, companies describe mobile applications as services in the terms of service agreements provided to consumers.[66] Users frequently control IOT devices through mobile and other online applications.[67] As manufacturers create more IOT devices, there will likely also be a corresponding increase in the number of applications companies provide and additional opportunities for the collection of IOT consumer data.

A Pew Research Center survey evaluating consumer perceptions of smart products found that consumers are "often cautious about disclosing their information and frequently unhappy about what happens to that information once companies have collected it."[68] Consumers are concerned about identifying which entities are collecting their data, the types of data that those entities are collecting, and who can subsequently obtain their data after it is collected.[69] Another Pew Research Center sur-

---

Z82C] (discussing a survey of 6,500 consumers in ten countries, including the United States).

64. Brian Scarpelli et al., ACT | The App Ass'n, State of the App Economy 2 (5th ed. 2017), http://actonline.org/wp-content/uploads/App_Economy_Report_2017_Digital.pdf [http://perma.cc/B6EH-8LGE].

65. The App Economy Forecast 2016, Waracle (June 21, 2016), http://waracle.net/app-economy-forecast-2016/ [http://perma.cc/69JS-8Q5A]; see also Louis Columbus, Roundup of Internet of Things Forecast and Market Estimates, 2016, Forbes (Nov. 27, 2016), http://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#73848438292d [http://perma.cc/L8AK-6W79] (discussing the economic impact of the IOT and applications); Understanding Mobile Apps, FTC Consumer Info., http://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps#basics [http://perma.cc/FKX3-FGM8] (last visited July 28, 2017) ("A mobile app is a software program you can download and access directly using your phone or another mobile device, like a tablet or music player.").

66. Mobile Applications as a Service: The SaaS Approach to Enterprise Mobile Apps, mediafly, http://www.mediafly.com/news/mobile-applications-as-a-service [http://perma.cc/LH6V-US4P] (last visited July 28, 2017) (describing mobile applications as services and discussing a software-as-a-service approach to mobile applications); Terms of Service, Nest, http://nest.com/legal/terms-of-service/ [http://perma.cc/5AP2-V5TW] (last updated Mar. 10, 2016) (describing the company's mobile application as services); Terms of Use, Weather Channel, http://weather.com/legal [http://perma.cc/34NJ-RKLL] (last updated Dec. 6, 2013) (same).

67. Stacy-Ann Elvy, Hybrid Transactions and the Internet of Things: Goods, Services or Software?, 74 Wash. & Lee. L. Rev. 77, 96, 98 (2017) [hereinafter Elvy, Hybrid Transactions] (explaining how consumers control Nest thermostats through a mobile application); see also Scarpelli et al., supra note 64, at 2 ("Without mobile apps, the $8 trillion internet of things (IoT) revolution would not exist.").

68. Lee Rainie & Maeve Duggan, Pew Research Ctr., Privacy and Information Sharing 2 (2016) [hereinafter Rainie & Duggan, Privacy Study], http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf [http://perma.cc/URE8-G4KB].

69. See Mary Madden & Lee Rainie, Pew Research Ctr., Americans' Attitudes About Privacy, Security, and Surveillance 3 (2015), http://www.pewinternet.org/2015/05/20/

vey reports that seventy-four percent of individuals believe that it is "very important" that they have the ability to control who is able to obtain their data.[70] Consumers across various age ranges are concerned about their online privacy.[71] These survey results suggest that there is some level of consumer demand for mechanisms that provide consumers with the ability to control their data and protect their privacy, even though consumers may not be fully aware of when and how companies use their data.

As consumers obtain more knowledge about the types of data that online entities can collect from their use of everyday Internet-enabled products, it is likely that consumer concerns about privacy will become even more prevalent, resulting in additional calls for more privacy and options for consumers to control their IOT-generated data. When privacy is in demand and data volume and quality increases significantly, enterprises are likely to develop offerings to exploit these developments.

II. TYPOLOGY OF DATA AND PRIVACY MODELS

This section identifies a typology of several business approaches to user data and privacy. The typology includes earlier models, such as the data-as-payment and freemium models, and variations of PFP and PDE models. The typology fosters a better understanding of the various privacy and data-collection issues each approach raises and uncovers the similarities and differences between these new approaches and older business models.

By relying significantly on mining consumer data and the resulting advertising revenue, large Internet companies successfully using the data-as-payment and freemium models have likely also contributed to a setting in which some consumers are interested in obtaining more privacy and data controls. The success of companies using these older approaches has likely encouraged other businesses, including ISPs and a new generation of start-ups, to adopt innovative methods to capitalize on consumer data and demands for privacy, resulting in the rise of PFP and PDE offerings.

---

americans-views-about-data-collection-and-security/#few-feel-they-have-a-lot-of-control-over-how-much-information-is-collected-about-them-in-daily-life [http://perma.cc/W5JM-ZNNS].

70. Lee Rainie, The State of Privacy in Post-Snowden America, Pew Research Ctr.: Fact Tank (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ [http://perma.cc/7ZD7-D98J]; see also Jay P. Kesan et al., A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy, 91 Ind. L.J. 267, 267 (2016) (contending that survey data on the question of consumer demand for privacy indicates that "consumers often want more options than the market gives them").

71. Jay Stanley, Do Young People Care About Privacy?, ACLU: Free Future (Apr. 29, 2013), http://www.aclu.org/blog/do-young-people-care-about-privacy [http://perma.cc/2X9P-TJY5] (discussing various polls indicating that millennials and young people are deeply concerned about their online privacy).

A. *Traditional Data and Privacy Models*

The data-as-payment (free) and freemium models raise significant privacy concerns for consumers. While consumers may have some understanding of the types of data that companies collect, as discussed in Part I above, consumers may not fully understand the extent to which they have traded away their data and privacy in exchange for a "free" product. The interconnected world of the IOT, where it may eventually be possible to link an Internet-enabled washing machine to a user's Facebook or Google account, exacerbates these concerns. Imagine what companies could do with this wealth of information.

The term freemium refers to a combination of "free" and "premium," whereby the introductory features of a product are offered for free but a user must pay a fee to access advanced features.[72] The freemium model generates similar privacy concerns as the data-as-payment model. Consumers generally have little control over their data and privacy under both models. Consumers may not always be aware of the extent to which companies that use freemium models monitor their activities and how their data can be used and disclosed to third parties. Despite this lack of awareness, as other privacy scholars critiquing the notice-and-choice model have noted, more notice and choice is not likely the solution since Internet companies could use additional notice of privacy and data policies to justify data practices that are detrimental to consumer interests.[73]

1. *Data-as-Payment Model.* — Numerous companies base their business models on the collection and monetization of consumer data.[74] Twitter, Instagram (Facebook), Google, and the makers of hundreds of mobile applications advertise their products as "free" to consumers.[75] At least

72. Anja Lambrecht et al., How Do Firms Make Money Selling Digital Goods Online?, 25 Marketing Letters 331, 332 (2014) ("Firms can also combine multiple revenue streams, for example, charge customers for a subset of services and generate additional revenues from selling advertising or information."); Clarence Lee et al., Designing Freemium: Strategic Balancing of Growth and Monetization 2 (July 14, 2017) (unpublished manuscript), http://faculty.som.yale.edu/vineetkumar/research/Freemium_LeeKumarGupta_2017.pdf [http://perma.cc/VD2Z-5YBQ] (describing the freemium model as a hybrid strategy); Vineet Kumar, Making "Freemium" Work, Harv. Bus. Rev. (May 2014), http://hbr.org/2014/05/making-freemium-work [http://perma.cc/6WL2-GU57].

73. See, e.g., Helen Nissenbaum, A Contextual Approach to Privacy Online, Dædalus, J. Am. Acad. Arts & Sci., Fall 2011, at 32, 34 ("[T]here is considerable agreement that transparency-and-choice has failed.").

74. See, e.g., Bernard E. Harcourt, Exposed: Desire and Disobedience in the Digital Age 6 (2015) (describing Facebook's Atlas product, which shares user information collected through data-mining technology).

75. See, e.g., Erin Bernstein & Theresa J. Lee, Where the Consumer Is the Commodity: The Difficulty with the Current Definition of Commercial Speech, 2013 Mich. St. L. Rev. 39, 40 ("Companies like Facebook, Google, and Twitter offer services used by billions of users that have become central to our day-to-day lives. These services are free to users." (footnote omitted)); Nicole A. Ozer, Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change, 36 N.Y.U. Rev. L. & Soc. Change 215,

one scholar has critiqued the use of the data-as-payment label, contending that such a description is misleading since "Internet users do not know the 'prices' they are paying for products and services . . . because they cannot reasonably estimate the marginal disutility that particular instances of data collection impose on them."[76] While this is likely true, regardless of the label used to describe this model (for example, "free model," "data-as-payment model," "bartering-with-data model," "online advertisement-based business model," "zero-price model," or "ad-supported model"), consumers generally provide their data (and perhaps their attention) to companies when using products that are described as "free." Thus, these products are not actually "free," and as such, use of the terms "free model" or "zero-price model" is perhaps also misleading. Once a consumer elects to use a "free" mobile application software or other "free" online product, the consumer engages in an unequal bargain of sorts in which data generated from their use of the product will be provided to the company.[77] Data are traded (whether knowingly or unknowingly) by the consumer to acquire the "free" product.[78] It is an imperfect barter transaction in which data are swapped for a product. The value of the data may exceed the value of the product provided. Of course, use of the term "data-as-payment" in this Article is not meant to suggest that data are money or currency, or that consumers understand the "price" they pay for "free" products. Instead, it is simply one of many imperfect labels that could be used to describe consumers' provision of data in order to obtain "free" or "zero-price" products in the online setting.

226–28 (2012) (discussing Facebook's and Google's use of the data-as-payment model and noting that users pay for "free services" with "data about themselves"); see also John M. Newman, Copyright Freeconomics, 66 Vand. L. Rev. 1409, 1439 (2013) [hereinafter Newman, Copyright Freeconomics] (discussing the ad-supported model in which "consumers . . . are able to access zero-price content that is accompanied by advertisements" and firms "pay the content provider for advertisement space").

76. Katherine J. Strandburg, Free Fall: The Online Market's Consumer Preference Disconnect, 2013 U. Chi. Legal F. 95, 96–99.

77. Hoofnagle & Whittington, Accounting for the Costs, supra note 5, at 624–25 (describing the exchange of consumer data for a free product as "trade, even if the trade occurs without a price"); see also 16 C.F.R. § 251.1 (2017) (discussing the meaning of "Free," "the offer of 'Free' merchandise or service as a special bargain," and the potential for consumers to be misled).

78. See generally Bernstein & Lee, supra note 75, at 82 n.208 ("In many ways the new information economy is a barter economy, with something of value, in this case data, exchanged for a good or service in lieu of using money."); Hoofnagle & Whittington, Accounting for the Costs, supra note 5, at 626 (describing the use of the data-as-payment business model); Thimmesch, supra note 30, at 147 (describing the data-as-payment model as a "barter transaction" and contending that "the digital products of today's economy are not free even though they are provided without a cash charge [because] consumers buy access to those products with their data."); Sparks & Honey Cultural Strategists, Bartering with Personal Data: In the Future, Everyone Will Be Private for 15 Minutes, Big Think, http://bigthink.com/amped/bartering-with-personal-data-in-the-future-everyone-will-be-private-for-15-minutes [http://perma.cc/D6LX-XSMG] (last visited July 28, 2017) (describing the exchange of data for free services).

Companies can monitor a consumer's habits, including Internet browsing on third-party websites, not only from the consumer's direct use of the product but also by using cookies and other mechanisms that enable data collection and tracking even when the product is not in use.[79] The Twitter, Facebook, and Google icons on various websites enable this process.[80]

Further evidence of the use of the data-as-payment model can be found in a report on the app economy by the Organization for Economic Cooperation and Development.[81] The report found that free apps, which frequently depend on the use of targeted advertising as a revenue model, are significantly more "likely to ask for permissions to see account information, location information, personal information and messages."[82] Additionally, in some instances companies that provide free apps obtain additional revenue from "in-app purchases," "promotion of non-digital goods," and "resale of data collected via app use."[83]

When products are provided for "free" in exchange for data, claims of alleged violations of statutes aimed at protecting consumers may not be viable.[84] For instance, in *Ellis v. Cartoon Network, Inc.*, the Eleventh Circuit held that "a person who download[ed] and use[d] a free mobile application on his smartphone to view freely available content, without more, [was] not a 'subscriber' and therefore not a 'consumer' under the [Video Privacy Protection Act]."[85] The court reasoned that while an indi-

---

79. Harcourt, supra note 74, at 3–4; see also Cookies & Other Storage Technologies, Facebook, http://www.facebook.com/policies/cookies/ [http://perma.cc/8MZ5-GXGW] (last updated Mar. 20, 2017).

80. Harcourt, supra note 74, at 3–4; see also What Kinds of Information Do We Collect?, Facebook, http://www.facebook.com/about/privacy/update#what-kinds-of-information-do-we-collect [http://perma.cc/DCT7-QMFN] (last updated Sept. 29, 2016).

81. Deborah Alcocer Delano & Taylor Reynolds, The App Economy 25 (OECD Dig. Econ. Papers, No. 230, 2013), http://dx.doi.org/10.1787/5k3ttftlv95k-en (on file with the *Columbia Law Review*); see also Mark Hachman, The Price of Free: How Apple, Facebook, Microsoft and Google Sell You to Advertisers, PC World (Oct. 1, 2015), http://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html [http://perma.cc/QX5L-457E] (describing the data-collection practices of companies that provide free services).

82. Delano & Reynolds, supra note 81, at 41 (noting that these permissions may not always be necessary in order for the app to function).

83. Id. at 22–25.

84. Hoofnagle & Whittington, Accounting for the Costs, supra note 5, at 658–59 (suggesting that "the transfer of personal information [should be viewed] as an exchange for value").

85. 803 F.3d 1251, 1252 (11th Cir. 2015); see also id. at 1253, 1256 (stating that under the Video Privacy Protection Act "the term 'consumer' means any renter, purchaser, or subscriber of goods or services from a video tape service provider" and that payment is one factor a court should evaluate in assessing whether an individual qualifies as a subscriber under the statute); Recent Cases, Statutory Interpretation—The Video Privacy Protection Act—Eleventh Circuit Limits the Scope of "Subscriber" for VPPA Protections.—*Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251 (11th Cir. 2015), 129 Harv. L. Rev. 2011, 2011 (2015).

vidual need not pay for a mobile application in order to qualify as a subscriber, "some type of commitment, relationship, or association (financial or otherwise) between a person and an entity" was required.[86]

2. *Freemium Model.* — Over the last several years, freemium has been the "dominant business model among internet start-ups and smartphone app developers."[87] Dropbox and LinkedIn are examples of companies that have used this model.[88] With freemium, companies may obtain revenue not only from advertisements but also from the subscription fees users pay to access upgraded options.[89]

Under the freemium model, consumers are still exchanging their data or privacy to access the free features of the product, but some consumers are also paying a monetary price to access the other features of the product.[90] As Professors Chris Hoofnagle and Jan Whittington have noted, "Many firms with freemium business models have products to sell, yet devote remarkable amounts of attention and investment to the collection of data from and about free-riding consumers of their products."[91] For instance, Everalbum was recently accused of deceiving its users into providing information from their contacts and subsequently sending automated text messages to every person in a user's contacts.[92]

B. *Pay-for-Privacy Models*

The most significant concern raised by PFP models is the further transformation of privacy into a product that can be sold and purchased. This occurs when consumers must pay for privacy (whether as a luxury

---

86. *Ellis*, 803 F.3d at 1256.

87. Kumar, supra note 72; see also Newman, Copyright Freeconomics, supra note 75, at 1439–40 (suggesting that "'freemium' allows content providers to price discriminate by offering one version of their platform (typically with fewer products, more advertisements, bandwidth limitations, or some combination of the three) for $ 0.00, while offering a premium version of the platform at a positive price"); Koen Pauwels & Allen Weiss, Moving from Free to Fee: How Online Firms Market to Change Their Business Model Successfully, 72 J. Marketing 14, 27–28 (2008) (discussing how companies can transition from a data-as-payment model to a freemium model).

88. Kumar, supra note 72.

89. Newman, Copyright Freeconomics, supra note 75, at 1441 ("[T]o the extent some freemium models contain an ad-supported, zero-price element, that element similarly generates revenues based on usage.").

90. See, e.g., Life Is Connected, Ever, http://www.ever.com/#lifes-connected [http://perma.cc/2MZQ-J9GG] (last visited July 28, 2017) (describing free and paid options Ever offers).

91. Hoofnagle & Whittington, Accounting for the Costs, supra note 5, at 634; see also Privacy Policy, LinkedIn, http://www.linkedin.com/legal/privacy-policy [http://perma.cc/MW7B-HLDV] (last visited July 28, 2017) ("We use cookies and similar technologies . . . to recognize you and/or your device(s) on, off and across different Services and devices. . . . You can also opt out . . . .").

92. Shayna Posses, App Maker Faces Suit over Text to Users, Law360 (May 15, 2017), http://www.law360.com/articles/923105/app-maker-faces-suit-over-texts-to-users-contacts [http://perma.cc/9XAB-YR7W].

product offered at moderate or expensive prices or a higher price offered in conjunction with a privacy-invasive discount). Pay-for-privacy models also raise concerns similar to those found in traditional models, including a potential lack of consumer knowledge and understanding about data and privacy-related issues. Consumers may simply purchase products that lack privacy and security features because they are cheaper than devices that have such features without considering broader privacy and security issues associated with less expensive products. Moreover, consumers may not understand the implications associated with accepting a discount in exchange for permitting companies to collect, mine, and disclose their data. As a result, these models exacerbate concerns about unequal access to privacy and questionable control and choice as will be discussed in Part III below.

1. *Privacy-as-a-Luxury Model.* — Under the privacy-as-a-luxury model, companies offer services and devices that provide consumers with more privacy and data-protection options at a higher price than other competing products. Companies using aspects of this model recognize the growing demand for privacy and security controls described in Part I above.

Primium, a term that consulting firm Arthur D. Little appears to have coined, means "privacy at a premium."[93] This proposed model recognizes that some consumers are prepared to pay higher fees for privacy. [94] This model "considers privacy control by the user as a key product attribute that can be used to differentiate [related] offerings from current free and paid (including Freemium) offerings that provide low levels of privacy control to users."[95] Arthur D. Little estimates that by 2020 the "market size" for businesses using the primium model will expand to $5 to $6 billion.[96] The consulting firm expects the user base of the data-as-payment and the freemium models to splinter into additional segments with an increase in the number of users that are willing to pay higher prices for better privacy options.[97] Thus, a company could offer three types of products to consumers: (1) a free product, (2) a basic paid product (freemium), and (3) a primium product that combines the basic paid product with more privacy and data controls.[98] The revenue streams

93. Sai Prakash Iyer et al., Primium—Business Models for a Privacy-Conscious World, 2014 Prism, no. 1, at 55, 55–57, http://www.adlittle.com/downloads/tx_adlprism/Primium.pdf [http://perma.cc/4Q8P-64ZD] (describing primium and distinguishing it from the free and freemium models). The consulting firm suggests that "[s]ome intermediaries" currently provide "Primium-like products to specific customer segments such as schools, government institutions and enterprises." Id. at 57.

94. Id. at 55.

95. Id. at 56.

96. Id. at 57.

97. Id. at 57–58.

98. Id. at 58 (discussing a visual depiction of the market evolution of primium business models).

of companies using this model would include advertisement revenue and fees freemium and primium customers pay.[99]

Companies that do not adopt the primium model could also begin to offer products with more privacy controls while simultaneously charging consumers higher prices in order to access such products. At this point, one can only assume that companies that adopt the privacy-as-a-luxury model will attempt to ensure third parties do not have unlimited access to consumer data generated from the use of their products. This could eventually impact the ability of data brokers to obtain consumer data associated with such products. Despite arguments that suggest that consumers are unwilling to pay for privacy, given the expected data gold rush and privacy issues associated with the IOT discussed in Part I, there may very well be high consumer demand for such products.[100]

Although one could view privacy as being different from security, evidence of some aspects of the privacy-as-a-luxury model can also be found in the smartphone context. Android is the most frequently used operating system on smartphones;[101] yet, commentators suggest that Google's efforts to encrypt Android devices lags significantly behind Apple's encryption mechanisms[102] and that very few Android phones are

---

99. Id.

100. Alastair R. Beresford et al., Unwillingness to Pay for Privacy: A Field Experiment 6 (Inst. for the Study of Labor, Discussion Paper No. 5017, 2010), http://ftp.iza.org/dp5017.pdf [http://perma.cc/2TP4-DUP2]; see also Adam Shostack & Paul Syverson, Naval Research Lab. Release No. 04-1221.1-1128, What Price Privacy? (And Why Identity Theft Is About Neither Identity nor Theft) 1 (2004), http://www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files/pdfs/ShostackSyverson2004.pdf [http://perma.cc/23A9-FUFT]; David Hoffman, Privacy Is a Business Opportunity, Harv. Bus. Rev. (Apr. 18, 2014), http://hbr.org/2014/04/privacy-is-a-business-opportunity [http://perma.cc/69SS-84AV] (contending that because of the IOT, "individuals will need products to manage their online reputations and protect their identities"). See generally L. Jean Camp & Stephen Lewis, "Economics of Information Security," Advances in Information Security (2004).

101. Adrian Fong, The Role of App Intermediaries in Protecting Data Privacy, 25 Int'l J.L. Info. Tech. 85, 86 (2017) ("Apple's iOS [has] more than 700 million active iOS users, and Google's Android OS [has] more than 1.4 billion users."); Steven J. Vaughn-Nichols, Sorry Windows, Android Is Now the Most Popular End-User Operating System, ZDNet (Apr. 3, 2017), http://www.zdnet.com/article/sorry-windows-android-is-now-the-most-popular-end-user-operating-system/ [http://perma.cc/3W7S-WL82].

102. Kaveh Waddell, Encryption Is a Luxury, Atlantic (Mar. 28, 2016), http://www.theatlantic.com/technology/archive/2016/03/the-digital-security-divide/475590/ [http://perma.cc/2ATJ-SF2H] ("Google recently required that all new Android devices encrypt device data by default—but exempted slower (and therefore cheaper) phones, making encryption a de-facto luxury feature."); see also Conner Forrest, The State of Mobile Device Security: Android vs. iOS, ZDNet (July 11, 2016), http://www.zdnet.com/article/the-state-of-mobile-device-security-android-vs-ios/ [http://perma.cc/X92L-FVZ2] (contending that IOS systems offer more security than Android systems); Matthew Green, The Limitations of Android N Encryption, A Few Thoughts on Cryptography Engineering (Nov. 24, 2016), http://blog.cryptographyengineering.com/2016/11/24/android-n-encryption/ [http://perma.cc/36J6-LG7Y] (describing ineffective Android encryption in comparison to Apple's); Ari Levy, Can Apple Still Claim Its iPhones Are Secure?, CNBC (Mar. 29, 2016), http://www.cnbc.com/2016/03/29/can-apple-still-claim-its-iphones-are-secure.html [http://

encrypted when compared to iPhones.[103] Consumers can purchase less secure Android phones for as little as $49.99.[104] On the other hand, Silent Circle offers a privacy and security-centered Android smartphone at a premium price of $799.[105]

Companies may also use a subscription-based, pay-for-privacy model. These companies charge seemingly moderate monthly fees for privacy-centered products.[106] For instance, businesses that provide virtual private network (VPN) products require users to pay monthly or annual subscription fees.[107] VPN products can secure a user's Internet connection and provide users with "greater control over how [they]

---

perma.cc/R967-74S4] (stating that Android phones are "known for being less secure than iPhones"); Christopher Soghoian, Your Smartphone Is a Civil Rights Issue, TED (June 2016), http://www.ted.com/talks/christopher_soghoian_your_smartphone_is_a_civil_rights_issue [http://perma.cc/4HMM-6ZEY] (describing the encryption differences between Android and Apple); Liam Tung, iPhone Encryption Is Six Years Ahead of Android: Cryptographer, CSO (Nov. 25, 2016), http://www.cso.com.au/article/610671/iphone-encryption-six-years-ahead-android-cryptographer [http://perma.cc/ST4V-LDRB] (describing Google's allegedly ineffective full-disk encryption system and comparing it to Apple's).

103. Jack Nicas, Google Faces Challenges in Encrypting Android Phones, Wall St. J. (Mar. 14, 2016), http://www.wsj.com/articles/google-faces-challenges-in-encrypting-android-phones-1457999906 (on file with the *Columbia Law Review*) (suggesting "that less than ten percent of Android phones worldwide are encrypted in comparison to ninety-five percent of iPhones"); Nathan Olivarez-Giles, Google's Android Security Improves—for the Few; Only 4.6% of Supported Android Devices Run Latest, Most Secure Version, Wall St. J. (Mar. 14, 2016), http://www.wsj.com/articles/as-googles-android-security-improves-fragmentation-problems-linger-1461240003 (on file with the *Columbia Law Review*); see also Andrew Cunningham, Why Are So Few Android Phones Encrypted, and Should You Encrypt Yours?, Arstechnica (Mar. 16, 2016), http://arstechnica.com/gadgets/2016/03/why-are-so-few-android-phones-encrypted-and-should-you-encrypt-yours/ [http://perma.cc/FFV5-Z6RC].

104. See Dan Cohen, It's Not Only the Rich Teens that Have Smartphones, Atlantic (Apr. 15, 2016), http://www.theatlantic.com/technology/archive/2016/04/not-only-rich-teens-have-cell-phones-digital-divide/478278/ [http://perma.cc/YA48-FJJJ] [hereinafter Cohen, Rich Teens]; Sascha Segan, Get America's Cheapest Android Nougat Phone via Amazon, PC Mag. (Mar. 24, 2017), http://www.pcmag.com/news/352602/get-americas-cheapest-android-nougat-phone-via-amazon [http://perma.cc/E89T-77PG] (discussing Android phones ranging in price from $49.99 to $99.99).

105. See Devices, Silent Circle, http://silent-circle.myshopify.com/collections/devices [http://perma.cc/7BQS-P3PX] (last visited Sept. 7, 2017) (offering a refurbished Blackphone 2 for $539); see also Zack Whittaker, Silent Circle Blackphone 2 Review: A Secure Android Phone with a Privacy Punch, ZDNet (Sept. 28, 2015), http://www.zdnet.com/product/silent-circle-blackphone-2/ [http://perma.cc/R5W6-MQ2D].

106. See, e.g., Pricing, HideIPVPN, http://www.hideipvpn.com/pricing [http://perma.cc/EEH4-5DFG] (last visited July 28, 2017) (describing VPN products ranging from $9.99 per month (or $119.88 per year) to $5.99 per month (or $71.88 per year)).

107. Max Eddy, The Best VPN Services of 2017, PC Mag. (Feb. 28, 2017), http://www.pcmag.com/article2/0,2817,2403388,00.asp (on file with the *Columbia Law Review*) [hereinafter Eddy, Best VPN Services]; see also Max Eddy, Spotflux Premium VPN Review, PC Mag. (May 1, 2017), http://www.pcmag.com/article2/0,2817,2453787,00.asp (on file with the *Columbia Law Review*) (noting that one provider's VPN subscription fees range from a mobile-only plan for $29.99 a year to more costly subscription fees that cover multiple devices for $37.99 a year).

appear online" by hiding a user's IP address, thereby "making it harder for advertisers (or spies, or hackers) to track . . . online [activity]."[108] Rather than paying a subscription fee to access an additional service that is seemingly unrelated to privacy protection, consumers are paying a subscription fee for privacy protection. Since the repeal of the FCC Rules, interest in consumer use of VPNs has increased.[109] In some instances, a VPN company may also provide some of its services for "free" through an "ad-supported" freemium model.[110] Other companies, such as FastMail, provide privacy driven services through monthly or yearly subscription fees as an alternative to companies that offer similar products via the data-as-payment model.[111]

2. *Privacy-Discount Model.* — When a company implements a privacy-discount program, consumers also pay for privacy controls by incurring higher fees. However, unlike in the privacy-as-a-luxury model, consumers are encouraged to relinquish their privacy and data through the use of discounts. For instance, one ISP previously provided a plan that gave consumers approximately $30 off monthly fees if they allowed the company to use their web-browsing information "to tailor ads and offers."[112] Not surprisingly, the company reported that since it began offering its PFP program, a large segment of its customers chose to participate in the program.[113]

The use of PFP discount programs suggests that companies are aware that some segments of consumers are willing to pay for privacy and data controls. In the data-as-payment model, companies monetize consumer data and rely significantly on advertisement revenue. In the freemium context, "the user pays for enhanced features," which may include

---

108. Eddy, Best VPN Services, supra note 107.

109. Congress Voted to Roll Back Internet Privacy Rules. Now People Are Looking to VPNs, Fortune (Mar. 28, 2017), http://fortune.com/2017/03/28/congress-internet-privacy-rules-vpns/ [http://perma.cc/VT8E-JB9Z].

110. Max Eddy, Protect Yourself with a Free VPN, PC Mag. (May 11, 2017), http://au.pcmag.com/software/47857/feature/protect-yourself-with-a-free-vpn-service (on file with the *Columbia Law Review*).

111. FastMail, http://www.fastmail.com/ [http://perma.cc/9ENE-YF9N] (last visited July 28, 2017) ("As a paid service, we only serve you, our customer. This means we have no split loyalties, no mining of your personal data, no sharing it with third parties, and no ads, ever."); see also Pauline Glikman & Nicolas Glady, What's the Value of Your Data?, TechCrunch (Oct. 13, 2015), http://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ [http://perma.cc/MM3P-LVJC] (describing FastMail as an alternative to Gmail and Zoho as an alternative to Google Docs).

112. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 23,360, 23,392 (proposed Apr. 20, 2016). But see Warren Letter, supra note 16, at 2 (explaining that AT&T's PFP program may have required "consumers to pay as much as $66 in additional monthly costs for service that maintains their privacy").

113. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. at 23,392.

"the absence of adverts."[114] With the discount model consumers are providing various sources of revenue to companies, including but not limited to: (1) data provided by consumers who accept discounts, which can be analyzed and used to generate advertisement revenue, among other things, and (2) higher fees paid by those consumers who are willing to pay for privacy and opt out of data collection.

In the discount-program setting, consumers who choose to take the discount must trade in their privacy and data. Under the data-as-payment model, consumers may unknowingly barter using their data to acquire a "free" service. In the discount model, consumers exchange their data and privacy for a discount. One could argue that consumers receive compensation (a reduced price) in exchange for their data. Consumers who elect to take the discount could be viewed as active brokers who monetize their own data. This monetization may not always be subject to transfer and disclosure restrictions as the companies that offer these discounts are also likely to subsequently monetize the data.

Given the pressing security issues associated with the IOT and the FTC's efforts in this area, companies concerned about their reputation may refrain from using the discount model and may instead choose to build privacy and security into their products. Such options may come with a higher price tag. However, companies may simply manufacture or offer more secure and privacy-oriented products without charging premium prices for such options. For instance, DuckDuckGo, a search engine, promises not to "collect or share personal information [such as search terms]" of its users.[115] The IOT may also create an environment in which consumers demand that privacy and data protection mechanisms be offered at affordable rates, and companies that choose not to do so may lose customers to companies with strong user privacy and security controls. To date, this environment has not yet emerged as IOT manufacturers continue to inundate the market with insecure IOT products that can be used to enable distributed denial of service attacks, among other things.[116]

---

114. Iyer et al., supra note 93, at 55. To the extent that freemium customers are required to pay subscription fees to avoid advertisements, a user could be described as paying for privacy.

115. We Don't Collect or Share Personal Information, DuckDuckGo, http://duckduckgo.com/privacy [http://perma.cc/9GVC-3MD8] (last visited July 28, 2017); see also Chris Matthews, DuckDuckGo: We're Profitable Without Tracking You, Fortune (Oct. 9, 2015), http://fortune.com/2015/10/09/duckduckgo-profitable/ [http://perma.cc/5AU9-MGFX].

116. Letter from Senator Mark Warner to Tom Wheeler, Chairman, FCC (Oct. 25, 2016) [hereinafter Warner Letter], http://www.scribd.com/document/328854049/DDoS-Letter-to-Chairman-Wheeler [http://perma.cc/QMU9-CHZ5]; Bree Fowler, Hackers Apparently Used Internet-Enabled Cameras, Toys in Cyberattacks, Yahoo! Tech (Oct. 22, 2016), http://www.yahoo.com/tech/hackers-apparently-used-internet-enabled-184903923.html [http://perma.cc/YD5M-ATSF].

C. *Personal Data Economy Models*

The data-insights model and the data-transfer model are the two models PDE companies currently use. The primary goal of companies using the data-insights model appears to be providing users with platforms to control, compile, aggregate, and obtain insights from their data while in some cases also offering a marketplace for users to monetize their data through various means. In contrast, the main objective of a company using the data-transfer model is seemingly to provide a marketplace for users to transfer their data (or rights in the data) directly to the PDE company or to unaffiliated third parties. Data monetizations by consumers via PDE marketplaces presume to some extent that consumers have transferable rights in or ownership of the data they generate, but various non-PDE companies may also simultaneously assert rights in such data. This may be particularly true in the IOT setting. The data insights that PDE companies offer allow users to more easily recognize the inherent value of their data to themselves and companies. These offerings could potentially increase consumer knowledge and understanding of data value. Unlike traditional data models in which the products offered are seemingly unconnected to data transfers, PDE models may increase transparency surrounding data-trade arrangements. However, a primary concern associated with the use of PDE models is whether this transparency and consumer understanding of data value and data-trade arrangements will also extend to how companies use data once consumers provide access to data via PDE marketplaces. Lack of consumer understanding and knowledge about data value, data-trade arrangements, and companies' use of data analytics to aggregate and manipulate data has long been a concern even in traditional data models. Yet PDE companies have been described as offering something new to consumers.[117] PDE models also raise additional concerns that will be explored in detail in Part III below.

1. *Data-Insights Model.* — A 2020 cybersecurity scenario developed by U.C. Berkeley's Center for Long-Term Cybersecurity describes a potential future in which "[t]he privacy calculations that people make in 2016 when it comes to their Fitbits, smartphones, and connected cars will seem anachronistic, because what you get in return for your data in 2020 will be a new set of insights about yourself . . . that are barely distinguishable from magic."[118] The stated aims of PDE companies, such as Digi.me, Meeco, and Cozy include helping individuals organize and obtain insights from their data, giving users control over whom they share their

117. See, e.g., Leigh, supra note 3 (discussing new options provided by Meeco).

118. Ctr. for Long-Term Cybersecurity, Cybersecurity Futures 2020, at 34 (2016), http://cltc.berkeley.edu/files/2016/04/cltcReport_04-27-04a_pages.pdf [http://perma.cc/B9S9-G72R].

data with, and recognizing the valuable role that consumers play in generating data.[119]

These companies achieve their goals through various means. For instance, Cozy provides a "personal cloud solution" that allows "customers to host their data [including IOT data, emails, and bills] on a personal server."[120] Digi.me's application allows users to combine data from multiple sources, and the company forecasts that its product will serve as a hub for various types of data, including financial data and health-related data.[121] Meeco offers a free platform that permits users to "curate

---

119. About Cozy, Cozy, http://cozy.io/en/about/ [http://perma.cc/3F82-SP7Z] [hereinafter Cozy, About Cozy] (last visited July 28, 2017) ("We see Cozy evolving from a personal private cloud and app platform into a universal tool that can help you organize your life . . . . We [] believe in empowering users by providing them free and open source tools that can help them . . . remain independent from commercial service providers."); About, Digi.me, http://www.getdigime.com/about [http://perma.cc/6UCR-7GZJ] (last visited July 28, 2017) ("Get your data, see how powerful it is, and control how you share it on your terms . . . ."); Why Meeco?, Meeco, http://meeco.me/why-meeco.html [http://perma.cc/5HVJ-NEKM] [hereinafter Meeco, Why Meeco] (last visited July 28, 2017) ("Meeco is about helping you gain the insight and have the data to negotia[te] better outcomes for you and your family."); see also MEF White Paper, supra note 23, at 13 (stating that Cozy "is a high-profile supporter of the personal data economy"). Beagli is another PDE-like company with the stated goal of providing users with insights about their data. About Us, Beagli, http://www.beagli.com/about/ [http://perma.cc/3GZC-CAYU] (last visited July 28, 2017) ("Personal data is a tremendously useful asset but at the moment there just aren't that many tools out there that will help the user obtain the type of powerful learning from his data that will actually enable him to improve his work-life. Beagli is set out to remedy this."); Terms & Conditions, Beagli, http://beagli.com/legal/ [http://perma.cc/2TVG-Z9NF] (last visited July 28, 2017) ("Beagli is a platform that allows users to store their data and analyze it."). The company's website suggests that it is still in the testing phase. See id.

120. MEF White Paper, supra note 23, at 13; see also Cozy, About Cozy, supra note 119. Cozy currently offers its products for free to users but the company notes that it eventually plans to charge users a fee. FAQ, Cozy, http://cozy.io/en/faq/ [http://perma.cc/P3VT-SSRD] (last visited July 28, 2017) ("Cozy is available free of charge as software you can run on your own Linux machine. The hosted version of Cozy is free during the beta period. After that, the hosting plan is expected to cost between €5 and €10 per month."). The company's products appear to also target businesses. See Cozy, About Cozy, supra note 119 (describing three types of potential clients: "hosting providers," "chief digital officers," and "educational and academic institutions"). But see Run Your Cloud at Home, Cozy, http://cozy.io/en/run-your-cloud-at-home/ [http://perma.cc/73LZ-5K2G] (last visited July 28, 2017) ("Cozy is a versatile and extensible platform that can be put to a variety of practical uses: from sharing your photos with friends and family to contacts and schedule management.").

121. Eileen Brown, Digi.me Gives Away Free Backup Software to Keep Your Social Media Memories Intact, ZDNet (Mar. 26, 2015), http://www.zdnet.com/google-amp/article/digi-me-gives-away-free-backup-software-to-keep-your-social-media-memories-intact/ [http://perma.cc/N42S-ULTP] (stating the Digi.me application allows users to "download [their] online social life and unite [their] social networks"); MEF White Paper, supra note 23, at 11–12; see also Emma Firth, Evolution of a Personal Data Start-Up: The Digi.me Story, Digi.me: Blog (Apr. 27, 2017), http://blog.digi.me/2017/04/27/evolution-of-a-personal-data-start-up-the-digi-me-story/ [http://perma.cc/PEU6-PNZD] [hereinafter Firth, The Digi.me Story] (noting the product will continue to allow users to back up

a huge amount of information about themselves [such as] . . . basic profile information, contacts, browsing habits, favourite brands and so on."[122] The company's products also allow users to obtain insights from the data they provide as well as prevent their online activity from being tracked.[123]

Additionally, some PDE companies either currently provide or intend to provide consumers with the opportunity to monetize their own data.[124] Meeco forecasts that users will use its products to create an anonymous wish list of items from certain brands that can make offers (such as rewards and discounts) to users using the wish list.[125] Digi.me

---

information they post on social media sites and the company's new application will allow users to include health, financial, and shopping data).

122. MEF White Paper, supra note 23, at 12–13; see also Meeco, Online Advertising—Booming or Broken?: Meeco Case Study 14 (2015), http://meeco.me/assets/pdf/Meeco_Case_Study_Online_Advertising-Booming_or_Broken_Sept_2015.pdf [http://perma.cc/X9HY-Y67L] (noting that in Meeco's "intentions marketplace" users can store and curate "data in their own secure Personal Data Store," communicate with brands, and broadcast "their purchasing intentions . . . in the Data Marketplace" to brands making tailored offerings); How It Works, Meeco, http://meeco.me/how-it-works.html [http://perma.cc/U35L-434P] [hereinafter Meeco, How It Works] (last visited July 28, 2017) (stating that Meeco is a free platform that "is designed to be part of your every-day digital life"). User data are "encrypted and securely stored on non-US based infrastructure." Introduction to Meeco, Meeco, http://blog.meeco.me/guide/introduction/ [http://perma.cc/FE57-JTAQ] [hereinafter Meeco, Introduction to Meeco] (last visited July 28, 2017).

123. MEF White Paper, supra note 23, at 13; see also Bookmark, Meeco, http://blog.meeco.me/guide/bookmark/ [http://perma.cc/H4FP-Y5RH] (last visited July 28, 2017) ("Bookmark is your personal web to browse and visit your favourite sites without leaving a data trail or being tracked by cookies."); Experience Meeco, Meeco, http://meeco.me/experience.html [http://perma.cc/M27T-V7C3] (last visited July 28, 2017) ("New plugins for Chrome and Firefox give you even more control over your online activity and anonymity."); Meeco, How It Works, supra note 122 ("Meeco provides a more holistic view of your digital behaviour and is a more accurate picture of who you really are. More importantly it is insight you own. Analytics and reports bring new insight to your connected life, providing a visual dashboard of your quantified self."); Learn, Meeco, http://blog.meeco.me/guide/learn/ [http://perma.cc/5G2L-CNWL] (last visited July 28, 2017) ("Meeco provides you with the context and wisdom to fully appreciate the value of your personal data, digital behaviour, preferences and purchasing intentions."); My Insights Is Your Quantified Digital Self, Meeco, http://blog.meeco.me/guide/my-insights-archive/ [http://perma.cc/6X3J-KTEX] (last visited July 28, 2017) (describing how Meeco provides analytical insights through "actionable charts and graphs").

124. Laura Secorun, Ozy.com: Selling Your Own Data, USA Today (June 30, 2014), http://www.usatoday.com/story/money/business/2014/06/30/ozy-selling-data/11760339/ [http://perma.cc/VV3D-VXU4] (stating that Meeco and Handshake "are personal data marketplaces . . . and their goal is to cut out the data-mining middleman by allowing users to share their personal information with companies—and get paid for it").

125. MEF White Paper, supra note 23, at 13; see also Leading in the Intention Economy, Meeco, http://meeco.me/business/ [http://perma.cc/SG8E-6XXV] [hereinafter Meeco, Business] (last visited Aug. 19, 2017) ("Bypass data brokers and advertising costs by incentivising your customers [sic] loyalty with status, discounts or financial rewards."); Signal, Meeco, http://blog.meeco.me/guide/signal/ [http://perma.cc/3AN6-L5NE] (last visited July 28, 2017) ("Signal is your private list of wishes and goals; a place to capture the products and services you need or wish for. Your identity remains anonymous so you can

expects that consumers will share their data on its platforms with companies in exchange for a more personalized service and offers that could include customized discounts.[126] For instance, Digi.me suggests that rather than a bank going to a data aggregator to obtain information about a user, the bank could obtain access to the user's data directly from the user through Digi.me's platforms for the limited purpose of assessing the user's creditworthiness.[127]

The data-insights model seems quite similar to the data-as-payment and privacy-discount models in that consumers also appear to be bartering away their privacy and data in exchange for discounts or a free product. However, PDE companies may offer more control to consumers. Digi.me's website indicates that user data are stored in such a manner that the company cannot access the data.[128] Meeco touts that it uses a "Privacy by Design approach."[129] In the PDE setting, consumers may be

---

decide the right time to share more information under your own terms when the market comes to you.").

126. MEF White Paper, supra note 23, at 13; see also Firth, The Digi.me Story, supra note 121 (stating that the consent access aspect of the company's product will "allow businesses, who want access to these rich, deep datasets that our users will soon hold, to approach them directly and offer them personalised offers in exchange for seeing some slices of that data").

127. Julian Ranger, Fixing the Personal Data Privacy Paradox by Sharing More, Digi.me: Blog (May 23, 2017), http://blog.digi.me/2017/05/23/fixing-the-privacy-paradox-by-sharing-more-personal-data/ [http://perma.cc/7HWJ-7NK2].

128. Privacy Comes as Standard, Digi.me, http://digi.me/privacy [http://perma.cc/M7QW-8X3M] [hereinafter Digi.me, Privacy] (last visited July 28, 2017) ("We never sell or share your data. We can't see it and don't hold it, so we couldn't even if we wanted to—and we don't."); Your Security Detail, Digi.me, http://www.digi.me/security [http://perma.cc/7LCK-PHUY] [hereinafter Digi.me, Security] (last visited July 28, 2017) ("Your digi.me library is securely held on the cloud storage service of your choice, such as DropBox, GoogleDrive, Microsoft OneDrive or a device such as a Western Digital myCloud (with more storage options to come)."); see also Firth, The Digi.me Story, supra note 121 (noting that a user's data are stored on the user's device instead of Digi.me's servers). Digi.me's approach to storing data is somewhat similar to the Coasean filter approach Professor Eric Goldman proposed in that users retain control and possession of their data. See Eric Goldman, A Coasean Analysis of Marketing, 2006 Wis. L. Rev. 1151, 1214 [hereinafter Goldman, Coasean Analysis] ("[T]he Coasean filter could store the consumer's dataset on the device itself rather than in central third-party-operated repositories. Thus, the data remains within the consumer's control, giving consumers the benefit of personalized content without the risks associated with third-party possession of the personalization data.").

129. Meeco, Why Meeco, supra note 119 ("Privacy by Design is a principle and international standard. It makes privacy a core foundation in the way products and services are designed. Meeco has adopted PbD as the guiding principle for the design and architecture of all our applications."); Meeco, Meeco Privacy Policy 1 [hereinafter Meeco, Privacy Policy], http://meeco.me/meeco-privacy.pdf [http://perma.cc/U3B4-LMWP] (last visited July 28, 2017) ("We will never sell, or give access to Your Data to a third party (unless we are legally required to), because we know that it is yours.").

able to choose which businesses may advertise their products to them.[130] Additionally, some PDE companies may provide users with searchable, organized, and aggregated copies of their own data, unlike companies that use a data-as-payment model and other established companies.[131] One PDE company suggests that users' having a copy of their own data can decrease the effects of cyberattacks on large entities.[132] Alternatively, attacks targeting individual consumers could increase.

Large data brokers that have collected data about consumers for decades may have more sophisticated mechanisms and capabilities to generate insights from large sets of consumer data in comparison to the insights that a single start-up PDE company could provide to a consumer. To the extent that PDE companies act as vaults for consumer data and access to the data by third-party companies is significantly reduced, some types of consumer data could be less accessible to data brokers. Of course, this would not impact other sources of consumer data that data brokers use, such as public records, and data brokers may still be able to obtain information from social media websites and other companies using the data-as-payment model.

Through the data-insights model, consumers serve as active brokers by monetizing their own data in exchange for personalized deals, thereby becoming active rather than passive players in the consumer-data market. As a result, some PDE companies obtain consumer data directly from consumers rather than from existing data brokers who rely on various sources to indirectly obtain information about consumers. By providing opportunities for consumers to capitalize on their data, consumers can share in the profits their data create.[133] Both consumers and companies are able to extract value directly from consumer-generated data. If existing PDE data-insight companies are successful, more domestic entities may begin widely using this model.

2. *Data-Transfer Model.* — Companies using the data-transfer model purchase or obtain rights to use consumer-generated data directly from users. Datacoup's stated "mission is to help people unlock the value of

130. Meeco, Business, supra note 125 ("Meeco is an advertising free platform. That means your content is permissioned by your customers because it is relevant and gives them priority access.").

131. Mecast by Meeco, Meeco, http://www.mecast.me/ [http://perma.cc/2NV6-3KQG] (last visited Aug. 19, 2017) (describing Mecast, a new Meeco app that provides a "searchable personal timeline" of users' social media posts); MEF White Paper, supra note 23, at 11–13 (discussing Cozy's ability to allow users to aggregate their data and Digi.me's ability to aid users in organizing their social media data).

132. Emma Firth, NHS Cyber Attack Shows Perils of Not Holding Our Own Personal Data, Digi.me: Blog (May 15, 2017), http://blog.digi.me/2017/05/15/nhs-cyber-attack-shows-perils-of-not-holding-our-own-personal-data/ [http://perma.cc/UAS5-8ANT] (contending that recent cyberattacks on the UK health system emphasize "the loss of control that we all have over our personal data, when instead of having a copy ourselves, it is held in giant siloes controlled by others").

133. Meeco, Why Meeco, supra note 119.

their personal data . . . [by] getting people compensated for the asset that they produce . . . [and placing them] in control of [their] data."[134] The company anticipates creating a marketplace for third parties to purchase consumer data or obtain access to data directly from consumers.[135] Datacoup allows consumers to connect their social media accounts, among other things, to the company's services and compile financial and demographic data.[136] Once the company assigns "data attributes," value, and a potential price to the consumer's information, the company transfers the data into its marketplace where buyers can purchase it, and users are then subsequently notified and compensated once their data are purchased.[137] Datacoup's target audience for purchasing the user data it collects and anonymizes includes "brands, retailers, media agencies, wireless carriers, insurance companies and banks."[138]

---

134. About Us, Datacoup, http://datacoup.com/docs#about [http://perma.cc/M96S-6SCW] [hereinafter Datacoup, About Us] (last visited July 28, 2017). Datacoup suggests that one of the company's goals is to change the "asymmetric dynamic that exists around our personal data" in which data brokers "offer no discernible benefit" to consumers who are the producers of data. Id.

135. How It Works, Datacoup, http://datacoup.com/docs#faq [http://perma.cc/49DM-4233] [hereinafter Datacoup, How Datacoup Works] (last visited July 28, 2017) ("Datacoup is lining up data purchasers to sustainably purchase data on the platform. However, to get the ball rolling, Datacoup is the primary purchaser of your data."); see also Thimmesch, supra note 30, at 156 n.57 (contending that scholars have experimented "with cash markets for data in laboratory experiments" and companies such as Datacoup are providing such services); Privacy Policy, Datacoup, http://datacoup.com/docs#pp [http://perma.cc/6P78-SYTA] [hereinafter Datacoup, Privacy Policy] (last visited July 28, 2017) ("Datacoup also enables you to sell or otherwise share your information with third parties."). Datacoup is also a member of the Personal Data Ecosystem. See Personal Data Ecosystem Consortium Directory, PDE, http://pde.cc/directory/ [http://perma.cc/4MMW-TAC5] (last visited July 28, 2017). Professors Hoofnagle and Whittington have described the Personal Data Ecosystem Consortium as representing a second generation of companies focused on helping consumers obtain control over their data. Chris Jay Hoofnagle & Jan Whittington, Unpacking Privacy's Price, 90 N.C. L. Rev. 1327, 1347 (2012) [hereinafter Hoofnagle & Whittington, Unpacking Privacy's Price].

136. Datacoup, How Datacoup Works, supra note 135; see also MEF White Paper, supra note 23, at 27. The company's website also indicates that the company does not view or store the usernames and passwords of users' social-network accounts, and the company promises to anonymize data before transferring the information into the large pool of user data that purchasers can access. See Datacoup, How Datacoup Works, supra note 135. Users may eventually have the ability to opt in to having data purchasers contact them. Id.

137. Datacoup, How Datacoup Works, supra note 135.

138. Id. But see Adam Tanner, Others Take Your Data for Free, This Site Pays Cash, Forbes (Mar. 3, 2014), http://www.forbes.com/sites/adamtanner/2014/03/03/others-take-your-data-for-free-this-site-pays-cash/#4574f3379461 [http://perma.cc/GS52-7EPT] (suggesting new PDE companies face several challenges including "that marketers will not pay much for details about just thousands of people when data brokers who pay nothing to individuals offer detailed dossiers on millions" and that "few users will sign up to share their data for just pennies").

As with the data-insights model discussed above, consumers are permitted to monetize their data, and companies obtain the data directly from consumers. However, with the data-transfer model, in some instances, the PDE company seems to provide direct monetary compensation to the user in exchange for the data in contrast to other PDE models. At the launch of Datacoup's operations, the company offered to purchase consumer data for $8 per month.[139] Datacoup's website suggests that the company determines how much to pay the consumer based on its analysis of the value of the data, and it is unclear whether users have the ability to negotiate terms or the price of the data.[140] Companies adopting the data-transfer model could also provide data insights to users,[141] but it appears that the primary goal of data-transfer companies is to transfer (sell) or provide access to data to third parties or the PDE company.[142]

In the current consumer-data marketplace that data brokers dominate, "most people have no idea that [their data are] being collected and sold, and that it is personally identifiable and that the information is in basically a profile of them."[143] In fact it is not entirely clear how many companies purchase and sell consumer data.[144] Datacoup has indicated that as its marketplace grows the company may provide users with additional features that allow them to control the transaction between themselves and the data buyer.[145] To the extent that PDE companies purchase data directly from consumers and disclose the identity of data purchasers,[146] users may be able to more easily obtain information about who is buying their data. In contrast, "It's much harder for Americans to get information on [data brokers, such as] Acxiom."[147] Other types of companies may also provide a marketplace for consumers to monetize

139. Datacoup, How Datacoup Works, supra note 135 ("Today, Datacoup is purchasing your data."); MEF White Paper, supra note 23, at 27.

140. Datacoup, How Datacoup Works, supra note 135.

141. See id. ("You also may use our data analysis tools to visualize summaries of your data and identify trends or patterns."); Unlock the Value of Your Personal Data, Datacoup, http://datacoup.com/ [http://perma.cc/LYW2-A633] (last visited Sept. 12, 2017) (stating that Datacoup gives users the tools to "better understand" their data and themselves).

142. MEF White Paper, supra note 23, at 27 (stating that Datacoup's "premise was that as companies buy anonymous aggregated data to better understand consumer behaviour, why not just buy it from the people themselves rather than from a data broker").

143. Kroft, supra note 14; see also FTC, Data Brokers: A Call for Transparency and Accountability 46 (2014) [hereinafter FTC Data Broker Report], http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (on file with the *Columbia Law Review*).

144. See Kroft, supra note 14.

145. Datacoup, How Datacoup Works, supra note 135.

146. MEF White Paper, supra note 23, at 27 (stating that Datacoup allows users to "see what information is bought, who is buying it and why it is of value").

147. Kroft, supra note 14. But see AboutTheData, http://aboutthedata.com [http://perma.cc/8N3Z-GPXT] (last visited July 28, 2017) (providing information about the data that companies hold).

their data. For instance, at least one individual has used Kickstarter to trade his information for $2 per day.[148]

III. IMPLICATIONS OF PFP AND PDE MODELS

PFP and PDE models generate significant concerns for consumers, such as a possible widening of the gap between the "privacy haves and have-nots," companies' continued monetization of consumer data, and the enablement of predatory and discriminatory behavior while simultaneously hiding behind a shroud of consumer empowerment, control, and choice.[149] Concerns associated with new monetization methods may prove challenging to existing legal frameworks.

A. *Unequal Access to Privacy*

1. *PFP Models.* — To the extent that financially disadvantaged consumers cannot afford the prices of companies that adopt a privacy-as-a-luxury model charge, use of this model is likely to contribute to the divide between those that can afford privacy and those that cannot.[150] Research on the historical digital divide and the demographics of smartphone users indicates that iPhone users tend to have significantly higher incomes than Android users, and low-income individuals frequently rely on smartphones for internet access since "they do not have

148. Federico Zannier, A Bite of Me, Kickstarter, http://www.kickstarter.com/projects/1461902402/a-bit-e-of-me [http://perma.cc/6VE4-DJA5] (last visited July 28, 2017) (discussing a service through which one individual sells his data, including websites visited, webcam images, cursor movements, and geolocation, for $2 per day); see also Billy Ehrenberg, How Much Is Your Personal Data Worth?, Guardian (Apr. 22, 2014), http://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth [http://perma.cc/WKB9-CTWM].

149. Brian Fung, Your Internet Privacy Shouldn't Be a Luxury Item, FCC Chief Says, L.A. Times (Aug. 5, 2016), http://www.latimes.com/business/technology/la-fi-tn-internet-privacy-fcc-20160805-snap-story.html [http://perma.cc/6TVK-KL4W].

150. Other commentators have discussed the relationship between unequal access to privacy and vulnerable communities and consumers in several contexts. See, e.g., Kimberly D. Bailey, Watching Me: The War on Crime, Privacy, and the State, 47 U.C. Davis L. Rev. 1539, 1565 (2014) (discussing the relationship between stops-and-frisks and unequal access to privacy); Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 Stan. L. Rev. 1373, 1398 (2000) [hereinafter Cohen, Examined Lives] ("[A]n important determinant of choice within markets is wealth. If data privacy costs money—or, conversely, if surrendering privacy saves money—access to privacy will be more unequal than if it did not."); Elaine Gibson, Wired Identities: Retention and Destruction of Personal Health Information in an Electronic World, 38 Dalhousie L.J. 385, 406 (2015) (evaluating access to privacy in the Canadian health care context and stating "[p]rivacy may be experienced differently by persons from disabled, racialized, and otherwise socially and economically marginalized groups"); Kami Chavis Simmons, Future of the Fourth Amendment: The Problem with Privacy, Poverty and Policing, 14 U. Md. L.J. Race, Religion, Gender & Class 240, 251 (2014) (discussing poor communities' unequal access to privacy rights in the transportation context and the impact of the Fourth Amendment).

broadband."[151] The cost of an Apple iPhone can range from $399 to as much as $1149, while some Android phones with weak privacy and security protections can be bought for much less.[152] This is not to suggest that iPhone users are absolutely free from "surveillance capitalism" or attempts at government intrusion.[153] Companies can use tracking technologies to monitor the online activities of smartphone users.[154] However, iPhone users obtain the benefit of a company that is willing to implement measures to ensure some level of information protection and may actively attempt to guard against government requests for user data.[155]

---

151. See Pew Research Ctr., U.S. Smartphone Use in 2015, at 3–4 (2015) [hereinafter U.S. Smartphone Use 2015], http://www.pewinternet.org/files/2015/03/PI_Smartphones_0401151.pdf [http://perma.cc/R59H-6VHU] (describing the "smartphone-dependent" population); Aaron Smith, Pew Research Ctr., Smartphone Ownership—2013 Update 6 (2013), http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_Smartphone_adoption_2013_PDF.pdf [http://perma.cc/HCX5-4JWU] ("[Cell phone owners] from the upper end of the income and education spectrum are much more likely than those with lower income and educational levels to say they own an iPhone."); Jim Edwards, These Maps Show that Android Is for Poor People, Bus. Insider (Apr. 3, 2014), http://www.businessinsider.com/android-is-for-poor-people-maps-2014-4 [http://perma.cc/F4EJ-W3A5] ("The rich, it seems, use iPhones while the poor tweet from Androids . . . . Android users are less lucrative than iPhone users . . . . It's a socio-economic split on class lines, in favor of iPhone over Android."); see also Monica Anderson, Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption, Pew Research Ctr.: Fact Tank (Mar. 22, 2017), http://www.pewresearch.org/fact-tank/2017/03/22/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/ [http://perma.cc/H3LM-32RJ] (noting that "[i]n 2016, one-fifth of adults living in households earning less than $30,000 a year were 'smartphone-only' internet users—meaning they owned a smartphone but did not have broadband internet at home").

152. See Buy iPhone7 and iPhone7 Plus, Apple, http://www.apple.com/shop/buy-iphone/iphone-7 [http://perma.cc/VBN7-4XG7] (last visited Aug. 19, 2017); iPhone X, Now Choose Your Capacity, Apple, http://www.apple.com/shop/buy-iphone/iphone-x#00,10,31 [http://perma.cc/S72L-ATK4] (last visited Sept. 25, 2017); see also Cohen, Rich Teens, supra note 104; Alfred Ng, These Cheap Phones Come at a Price—Your Privacy, CNET (July 27, 2017), http://www.cnet.com/news/these-cheap-phones-are-costing-you-your-privacy/ (on file with the *Columbia Law Review*) (describing a $60 Android phone available for sale on Amazon that surreptitiously transfers users' "private data to China" and summarizing research on the privacy and security failings of other cheaper Android products).

153. See generally Shoshana Zuboff, Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, 30 J. Info. Tech. 75 (2015) (defining and discussing surveillance capitalism).

154. See Ghostery, http://www.ghostery.com/lp1/product-offers/?pk_campaign=goga_us6 [http://perma.cc/KXJ2-6FHB] (last visited July 28, 2017) (offering a "browser extension and mobile browser" to combat tracking).

155. See Eric Lichtblau & Katie Benner, Apple Fights Order to Unlock San Bernadino Gunman's iPhone, N.Y. Times (Feb. 17, 2016), http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?mcubz=2&_r=0 (on file with the *Columbia Law Review*); Soghoian, supra note 102 (discussing issues associated with a lack of encryption).

Currently, many IOT devices have insufficient security features, and limited encryption mechanisms are provided in connection with such products.[156] In the IOT setting, one could easily imagine a scenario in which companies that offer devices accompanied by high-level encryption technology and other privacy and security mechanisms charge significantly higher prices than those that do not. In such an instance, more secure, privacy-oriented products would be beyond the reach of low-income consumers.

To avoid continuous online tracking and data collection, commentators have suggested that all consumers should use a VPN.[157] However, as noted in section II.B(i), VPN services are generally paid products that require users to pay monthly subscription fees.[158] This cost highlights concerns about unequal access to privacy, as not all consumers may be able to afford an additional monthly subscription fee to protect their privacy. Low-income consumers may be at a distinct disadvantage.

Users who are able to pay for privacy and security-centered products, such as smartphones with encryption technologies and VPN services, are better off than those who cannot. Those who can afford to pay for privacy obtain at least some level of data protection when compared to those who cannot afford to pay for such products and services. This privacy gap threatens to exacerbate the socioeconomic digital divide. The Pew Research Center reports that in today's digital age, low-income and minority consumers continue to have "fewer options for online access."[159] PFP models complicate this problem. Even when these groups of consumers obtain access to the Internet, they may be subjected to increased data collection and a lack of privacy and control with respect to their data unless they are able to pay for the products and services offered by PFP companies to minimize these concerns. These consumers may also lack knowledge of privacy protection options or products. Unequal access to information may contribute to unequal access to privacy.

Admittedly, there is a plethora of free products that companies offer to consumers of all socioeconomic groups to combat data surveillance and security concerns. Moreover, PFP products may not provide complete protection or anonymity to users. As explained in section II.A, when companies offer products for free, consumers usually trade in their data and some level of privacy to obtain the product. For instance, in 2016, Web of Trust, a free browser extension,[160] was accused of recording

156. Elvy, Hybrid Transactions, supra note 67, at 87; Warner Letter, supra note 116.

157. See, e.g., Lee Mathews, What a VPN Is, and Why You Should Use It to Protect Your Privacy, Forbes (Jan. 27, 2017), http://www.forbes.com/sites/leematleem/2017/01/27/what-is-a-vpn-and-why-should-you-use-one/#5933448b4b8f [http://perma.cc/AQ6D-FAWS].

158. Eddy, Best VPN Services, supra note 107.

159. Anderson, supra note 151; see also U.S. Smartphone Use 2015, supra note 151.

160. Rick Broida, How to Tell Whether a Website Is Safe, PC World (Jan. 23, 2011), http://www.pcworld.com/article/217248/safe_websites.html [http://perma.cc/2AZR-EVWT]

and selling user data.[161] To the surprise of many of its users, Unroll.me, a free service[162] that helps users unsubscribe from email lists, was recently accused of selling to unaffiliated companies anonymized data obtained from users' emails.[163] The scandal highlights consumers' lack of understanding about the privacy trade-offs associated with free services.[164] Perhaps this is because, as the FTC notes, there is not much clarity about when data are sold or disclosed, how data are sold or transferred, and to whom.[165] A company may simply inform users that it collects and anonymizes their data to provide either targeted advertising or a better experience to the consumer. While these reasons seem benign, the inferences that could be made about consumers by compiling previously disparate sources of data are concerning. A 2017 report on corporate surveillance suggests that this data compilation is not anonymous and that social media companies provide a platform for businesses "to find and target exactly those persons they have email addresses or phone numbers on."[166]

Research suggests that social media data and information about a user's website choices can be used to determine a user's personality.[167] One can only envision the inferences that companies could make by combining social media and website choice information with IOT data.[168] Consumers who can pay for privacy are in a more advantageous position than those who cannot in that they can afford to avail themselves of

---

(describing Web of Trust as "a free browser plug-in" that inspects online search results and recommends links to avoid).

161. Matthew Humphries, Web of Trust Browser Extension Cannot Be Trusted, PC Mag. (Nov. 4, 2016), http://www.pcmag.com/news/349328/web-of-trust-browser-extension-cannot-be-trusted [http://perma.cc/EE3T-J6RM].

162. Unroll.me, http://unroll.me/ [http://perma.cc/HQK7-XYFL] (last visited July 28, 2017).

163. Joe Kukura, Unroll.me Founder Unloads in Wake of Uber Scandal, SF Wkly. (Apr. 26, 2017), http://www.sfweekly.com/news/unroll-me-founder-unloads-in-wake-of-uber-scandal/ [http://perma.cc/MXV6-XPQT] (discussing Unroll.me's sale of user data, such as the sale of Lyft receipts to Uber).

164. Amanda Hess, How Privacy Became a Commodity for the Rich and Powerful, N.Y. Times Mag. (May 9, 2017), http://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html (on file with the *Columbia Law Review*).

165. FTC Data Broker Report, supra note 143, at 46; Singer, supra note 9.

166. Wolfie Christl, Cracked Labs, Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade and Use Personal Data on Billions 47 (2017), http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf [http://perma.cc/K7MC-8XN5].

167. Michal Kosinski et al., Manifestations of User Personality in Website Choice and Behaviour on Online Social Networks, 95 Machine Learning J. 357, 378 (2014); see also Hess, supra note 164, at 2 (discussing the use of social media data to make inferences as well as the use of data analytics in elections).

168. See generally U.S. Gov't Accountability Office, GAO-17-75, Internet of Things: Status and Implications of an Increasingly Connected World 6 (2017) (discussing the impact of the IOT and the use of advanced data analytics to analyze IOT data to uncover "subtle, or hidden patterns, correlations and other insights").

technological offerings to limit tracking and data collection while accessing the Internet. This remains true even though PFP products are not completely immune from vulnerabilities and may not prevent the collection and disclosure of consumer data in all instances.

Advocates of PFP discount offerings in the broadband context contend that (1) different groups of consumers have distinct preferences for privacy; (2) most consumers are prepared to trade privacy for convenience and discounts and can make decisions about the issues associated with such plans; and (3) these plans can help consumers of various socioeconomic backgrounds.[169] Opponents of the FCC Rules, which would have addressed PFP discount programs, argued that the regulation unfairly targeted ISPs while leaving other online companies, who are the primary users of consumer information, to freely collect and use this data, thereby confusing consumers.[170] Other commentators suggest that technological developments, such as encryption, may prevent ISPs from viewing and accessing consumers' data and activities.[171] However, despite encryption, ISPs may be able to see certain domains viewed by users.[172]

---

169. Notice of Proposed Rulemaking: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, at 142–47 (Apr. 1, 2016) (dissenting statement of O'Rielly, comm'r) [hereinafter O'Rielly Dissenting Statement], http://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf (on file with the *Columbia Law Review*) ("[The nature of the Internet economy] is a trade-off—consumers receive 'free' stuff offered by Internet companies while in return the companies receive other things . . . that consumers may or may not want . . . ."); Petition for Reconsideration by the United States Telecom Association at 6, Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., WC Docket No. 16-106 (FCC filed Jan. 3, 2017) [hereinafter Petition for Reconsideration], http://www.ustelecom.org/sites/default/files/documents/Privacy_PFR_01.03.17_lf_krs%20.pdf [http://perma.cc/7E7S-GFPC] ("Most consumers are happy to share information with online service providers in exchange for free or discounted services."); Doug Brake, Info. Tech. & Innovation Found., Why Broadband Discounts for Data Are Pro-Consumer 4 (2016) ("In considering the value to consumers of such a program, it is worth recognizing that consumer privacy preferences vary considerably."); see also Verizon, Comments on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services 4 (2016) [hereinafter Verizon Comments], http://ecfsapi.fcc.gov/file/60002078934.pdf [http://perma.cc/NBM3-XMPV] ("[Restricting discount programs] conflicts with the fundamental premise . . . that consumers are capable of making informed choices about the uses of their information.").

170. Verizon Comments, supra note 169, at 3–4.

171. Peter Swire et al., Online Privacy and ISPs: ISP Access to Consumer Data Is Limited and Often Less than Access by Others 3 (2016) (unpublished working paper), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf (on file with the *Columbia Law Review*); see also Maureen K. Ohlhausen, Acting Chairman, FTC, Remarks: Internet Privacy: Technology and Policy Developments 6 (May 1, 2017) [hereinafter Ohlhausen Remarks], http://www.ftc.gov/system/files/documents/public_statements/1213203/ohlhausen_-_internet_privacy_remarks_rayburn_hob_5-1-17.pdf [http://perma.cc/7T7Y-ZNLG] (supporting a privacy framework that is "technology neutral—that is, that ISPs be treated like any other large platform").

172. Opposition to Petitions for Reconsideration at 2–3, Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., WC Docket No. 16-106 (FCC filed Mar. 6, 2017), http://ecfsapi.fcc.gov/file/1030755074740/Coalition%20Opposition%20Final.pdf [http://

Privacy-discount plans may force consumers to make difficult choices between privacy and other necessities.[173] As the FCC notes, broadband Internet access service (BIAS) companies provide consumers with access to the Internet, a critical service in the digital age.[174] Through the Internet, consumers can access various opportunities and engage in commercial transactions—for instance by purchasing and selling goods and services.[175] One commentator has suggested that "for a struggling family, [the decision to pay to opt out of data sharing] could mean choosing between paying [an extra $29] for privacy and paying for groceries or the public transportation needed to get to work."[176] The FCC has acknowledged the potential negative impact of PFP plans on low-income consumers.[177] In a survey conducted by the Pew Research Center, fifty-five percent of respondents found it unacceptable for a company to collect data about activities in their homes in exchange for savings on their energy bills.[178] Research on consumer choices and privacy policies also suggests

---

perma.cc/Y2HZ-J876] ("But even with encryption (implemented at the discretion of the website operator, not the consumer), the ISP can still see the top-level and second-level domains accessed by its customers.").

173. See Warren Letter, supra note 16, at 2 (contending that companies should not transform privacy into a luxury good and such practices may harm low-income consumers); see also Electronic Privacy Information Center, Comment Letter on Proposed Rule on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services 25 (May 27, 2016) [hereinafter EPIC Comments], http://ecfsapi.fcc.gov/file/60002079241.pdf [http://perma.cc/U4MF-JSFB] (urging the FCC to prohibit PFP schemes as "[f]inancial pressures reduce the voluntariness of consumer consent").

174. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64), repealed by Act of Apr. 3, 2017, Pub. L. No. 115-22, 131 Stat. 88 (codifying a joint resolution disapproving of the FCC "Broadband and Telecommunications Services" privacy rules).

175. Id.; see also Olivier Sylvain, Network Equality, 67 Hastings L.J. 443, 447 (2016) ("The Internet has become the platform through which people learn about and seek jobs, health care, housing, and education.").

176. Sandra Fulton, Pay-for-Privacy Schemes Put the Most Vulnerable Americans at Risk, Free Press (May 10, 2016), http://www.freepress.net/blog/2016/05/10/pay-privacy-schemes-put-most-vulnerable-americans-risk [http://perma.cc/9FES-AM2L]; see also Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. at 87,274 ("Thirty-eight public interest organizations expressed concern that financial incentives can result in consumers paying up to $ 800 per year—$62 per month—for plans that protect their privacy.").

177. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. at 87,274 (noting that there are "legitimate concerns that financial incentive practices can also be harmful if presented in a coercive manner, mislead consumers into surrendering their privacy rights . . . [and have a] disproportionate effect on low income individuals").

178. Rainie & Duggan, Privacy Study, supra note 68, at 37. But see Greg Lindsay et al., Atl. Council, Smart Homes and the Internet of Things 3 (2016), http://www.atlanticcouncil.org/images/publications/Smart_Homes_0317_web.pdf [http://perma.cc/97EK-W499] (suggesting that "[f]orty percent of consumers are willing to share data from their wearable devices with retailers or brands in exchange for coupons, discounts or information" (internal

that consumers do not always make rational choices about their privacy or data collection.[179] Further, as Professors Nancy Kim and D.A. Jeremy Telman have noted, "[S]urvey data indicates that consumers would not willingly choose to sacrifice their privacy in exchange for targeted advertising."[180] A 2016 study of consumer preferences found that more than eighty percent of respondents had given data to companies online "when they wished that they did not have to do so."[181]

Opponents of PFP discount programs in the broadband setting have suggested that perhaps such programs could be improved by providing users with "fair value for their data" and an adequate discount rather than a "privacy penalty," and increasing consumer knowledge about how their data are used.[182] In some cases, PDE programs attempt to meet at least some of these goals, yet the danger of unequal access to privacy remains.

2. *PDE Models.* — In the PDE setting, consumers who are not economically disadvantaged may avoid participating in a PDE marketplace, while other consumers may sell their data at the first opportunity, particularly if companies elect to provide significant compensation for the data. Thus, under the data-transfer model, low-income consumers and those from other at-risk communities could dominate the personal data-selling market, thereby widening the gap between those who have privacy and those who do not. Of course, a wide range of consumers in different income brackets could use other PDE models that primarily provide insights to consumers about their data, and these consumers could refrain from using the monetization options provided by these companies. One could also contend that consumers who elect to engage in the PDE marketplace are more likely to be sophisticated and informed about the value of their data. PDE companies may have the potential to provide consumers with more options for extracting value from their data, but the monetization options these companies provide also raise concerns. Further, PDE companies on their own cannot remedy all ills associated with pervasive data collection and a lack of consumer privacy.

---

quotation marks omitted) (quoting The Internet of Things: The Future of Consumer Adoption, Accenture, http://www.accenture.com [http://perma.cc/3F9U-GZ85] (last visited Aug. 16, 2017))).

179. See generally Omri Ben-Shahar & Adam Chilton, Simplification of Privacy Disclosures: An Experimental Test, 45 J. Legal Stud. S41 (2016) (concluding the use of simpler disclosures does not significantly affect consumers' understanding of the disclosure, "willingness to share personal information," or "expectations about their rights").

180. Nancy S. Kim & D.A. Jeremy Telman, Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent, 80 Mo. L. Rev. 723, 729, 738–39 (2015) (discussing a 2013 survey by Consumer Action that showed sixty-nine percent of respondents would not be "willing to allow companies to track, collect, and share data with permission in exchange for a free product or service").

181. Kesan et al., supra note 70, at 267.

182. Fulton, supra note 176.

A collaborative effort by multiple stakeholders with a resulting shift towards comprehensive privacy protection for consumers is needed.

The danger of unequal access to privacy is also alarming when one considers the monetization of children's data. Companies could mine and analyze child data to predict or make "probabilistic inferences" about the current and expected adulthood preferences and activities of children. Imagine a scenario in which a PDE company offers to purchase the data of everyone in a consumer's household, and, in addition to personalized discounts and offers, the parent receives $100 a month for authorizing tracking and data collection. Luth Research has offered similar monthly payments to users who agree to the tracking and collection of their online activities.[183] In the data-as-payment setting, parents frequently disclose information (including pictures and videos) about their children.[184] Parents could intentionally (or unintentionally, such as when child-related data is combined with household data or when parents and children share devices) engage in the PDE marketplace using child data.[185]

There have been repeated instances of parents who have faced economic challenges and resorted to using their children's identities for financial gain or to provide their families with necessities.[186] Exploitation of child data may be exacerbated in the IOT setting as the quality and quantity of data about children increase. This data could be viewed as an asset that can generate tangible compensation. Parents could potentially enter into an agreement for the sale or license of their child's data to a PDE company. Such arrangements may be attractive to cash-strapped parents who are unable to pay for basic services, such as utilities. As noted earlier, it is also possible that parents may provide access to data about their children inadvertently simply by providing information about

---

183. Winston Ross, How Much Is Your Privacy Worth?, MIT Tech. Rev. (Aug. 26, 2014), http://www.technologyreview.com/s/529686/how-much-is-your-privacy-worth/ [http://perma.cc/9VJ5-MHB7] (noting as many as "20,000 PC users and 6,000 smartphone users" have participated in Luth Research's program and the information the company collects is sold to various companies that use the data to make advertising decisions).

184. Tara Haelle, Do Parents Invade Children's Privacy When They Post Photos Online?, NPR (Oct. 28, 2016), http://www.npr.org/sections/health-shots/2016/10/28/499595298/do-parents-invade-childrens-privacy-when-they-post-photos-online [http://perma.cc/L4Q9-LYFM].

185. But see Terms of Service, Datacoup, http://datacoup.com/docs#tos [http://perma.cc/BU4B-RUJ4] [hereinafter Datacoup, Terms of Service] (last updated Nov. 1, 2013) (noting users of the company's service agree not to "solicit personal information from minors").

186. Gerry Smith, Family Secrets: Parents Prey on Children's Identities as Victims Stay Silent, Huffington Post (Nov. 11, 2011), http://www.huffingtonpost.com/2011/11/11/child-identity-theft-parents-credit-fraud-debt_n_1010093.html [http://perma.cc/GX32-GQGA]; see also Blake Ellis, Financial Abuses of Deadbeat Parents, CNN Money (June 8, 2010), http://money.cnn.com/2010/06/08/pf/parents_financial_abuses/index.htm [http://perma.cc/A3G3-UQG9] (summarizing different methods and articulating examples of ways parents could use their children's identities for financial gain, such as "taking out loans," "opening credit cards," "creating new accounts," or "co-signing a lease").

their household. In either case, the level of privacy provided to a child depends on the parent's choice, with the result being that the children of parents who elect not to directly provide access to household data or their child's data to third parties may receive more privacy protections than children of parents who decide to accept PFP discounts or participate in the burgeoning PDE marketplace. Admittedly, this concern is prevalent regardless of whether parents participate in the PDE marketplace. However, increases in data volume and quality generated by the IOT as well as the new venues offered by PDE companies to aggregate and share data with unaffiliated parties in exchange for discounts and other deals could prove to be problematic. Eventually information about a child's behavioral status, preferences, experiences and other sorts of child-related data could be used to determine the types of opportunities that children receive during childhood as well as negatively impact their adulthood lives and prospects. Thus, rising data quality and quantity and increases in the digital footprints of children combined with new platforms for collecting and sharing household (and child) data may exacerbate privacy concerns for children.

Additional concerns arise in the landlord–tenant context. Landlords typically supply appliances in a rental unit. Soon, every household good will be connected to the Internet and will generate information about users.[187] Landlords could elect to sell or provide access to data generated from a renter's use of landlord IOT devices in the PDE marketplace.[188]

A nationwide report on the rental housing market published by the Joint Center for Housing Studies of Harvard University found that "[b]y income, the largest increase in renters—4.0 million—was among households earning less than $25,000 annually, both because low-income households are much more likely to rent and because their numbers had swelled following the recession."[189] The report also found that a signifi-

187. See Lee Rainie & Janna Anderson, The Internet of Things Connectivity Binge: What Are the Implications?, Pew Research Ctr., (June 6, 2017), http://www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/ [http://perma.cc/4V87-RNPF] [hereinafter Rainie & Anderson, IOT Connectivity Binge] (discussing results from a canvassing of IOT experts and noting IOT "connection is inevitable" as more manufacturers will begin to "add the internet" to devices).

188. Other commentators have expressed similar concerns with respect to the rise of smart home technology. See Kaveh Waddell, Would You Let Companies Monitor You for Money?, Atlantic (Apr. 1, 2016), http://www.theatlantic.com/technology/archive/2016/04/would-you-let-companies-monitor-you-for-money/476298/ [http://perma.cc/PVW4-LTXT] (expressing concerns regarding the rise of smart home technology and the willingness of surveyed individuals to sell their personal data for cash). See generally A. Michael Froomkin & P. Zak Colangelo, Self-Defense Against Robots and Drones, 48 Conn. L. Rev. 1, 32–33 (2015) (noting surreptitious installation of monitoring devices may lead to landlord liability under tort theories).

189. Joint Ctr. for Hous. Studies of Harvard Univ., America's Rental Housing: Expanding Options for Diverse and Growing Demand 2 (2015), http://www.jchs.harvard.edu/sites/jchs.harvard.edu/files/americas_rental_housing_2015_web.pdf [http://perma.cc/6TH9-6VP4].

cant segment of Hispanic and African American households that rent are "severely cost burdened."[190]

To the extent that renters elect to directly participate in the PDE marketplace, landlords could require renters to consent to sharing insights produced by PDE companies. Some renters may object to such arrangements, but if such provisions become widely used, a tenant may have no option but to consent to such terms to obtain housing.

Landlords may have valid reasons for requiring data collection. IOT appliances could be manufactured to not only provide notices to landlords about when the device needs to be serviced but also lead to energy savings.[191] The appliance may also need to receive software updates from the manufacturer to continue to function. Monitoring could also allow landlords to know whether an appliance has malfunctioned because of ordinary wear and tear or because of tenant misuse. Tenants may also benefit from access to IOT devices. For instance, a device may be able to continually measure and record the temperature in a tenant's home and provide evidence of safety issues in the home that have not been corrected by the landlord.[192] Data collection in the tenancy context may become more prevalent as more "smart buildings" are constructed and IOT devices begin to replace static devices. Whether tenants will be provided with notice of this or understand the implications of their use of IOT devices provided by landlords is unclear.

Landlords could use renter data to obtain insights about renters and to make housing determinations. Most landlords already use "tenant-screening companies" to generate reports on prospective tenants, and tenants typically bear the costs of these reports.[193] Companies that provide services to landlords could directly obtain data about renters by engaging in PDE marketplaces, or they could obtain the information from other companies that are allowed to participate in PDE marketplaces. The costs of PDE data insights could be passed on to renters.

---

190. Id. at 5. The study defines cost-burdened as "paying more than 30 percent of income for housing" and severely cost-burdened as "paying more than half of income for housing." Id. at 4.

191. See Surabhi Kejriwal & Saurabh Mahajan, Deloitte Ctr. for Fin. Servs., Smart Buildings: How IOT Technology Aims to Add Value for Real Estate Companies 9 (2016), http://www2.deloitte.com/content/dam/Deloitte/nl/Documents/real-estate/deloitte-nl-fsi-real-estate-smart-buildings-how-iot-technology-aims-to-add-value-for-real-estate-companies.pdf [http://perma.cc/RW4J-PKTZ]; see also Matt Power, The Green Landlord: 5 New Technologies that Save Energy and Money, Green Builder Media (June 9, 2014), http://www.greenbuildermedia.com/internet-of-things/blog/the-green-landlord-five-new-technologies-that-save-energy-and-money [http://perma.cc/7RF2-Y8B6].

192. Klint Finley, How to Use the Internet of Things to Fight Slumlords, Wired (Aug. 28, 2014), http://www.wired.com/2014/08/heat-seek-nyc/ [http://perma.cc/X5VK-P7SK].

193. See Eric Dunn & Marina Grabchuk, Background Checks and Social Effects: Contemporary Residential Tenant-Screening Problems in Washington State, 9 Seattle J. Soc. Just. 319, 323 (2010) (explaining that the entire cost of tenant-screening reports is "generally passed along to the applicant").

Tenant-screening reports could become more expensive as a result. Groups that already face significant barriers accessing housing are particularly vulnerable as they are generally required to pay for new screening reports for each application to a landlord prior to obtaining housing.[194] Not only is a lack of privacy a concern, but the danger for such renters and their families is possible homelessness if they are unable to bear the costs of multiple screening reports during their search for housing.

Consider that a UK company, Tenant Assured, has developed a program to permit landlords to analyze the social media data of renters.[195] The program scans renters' social media conversations and posts for "information about the user's personality, life events (like giving birth or getting married), and even their 'financial stress level'—a measure of how easy it is for them to pay their rent, based on the frequency with which keywords like 'no money,' 'poor,' and 'staying in'" appeared in their posts.[196]

Naborly, another start-up company, touts that it "goes beyond the basics" of credit reports,[197] which the Fair Credit Reporting Act (FCRA) may regulate,[198] and utilizes artificial intelligence to compile and scrutinize tenant information for landlords.[199] As Professor Daniel Solove has observed, "Not only are our digital biographies reductive, but they are often inaccurate."[200] Companies such as Naborly could qualify as consumer reporting agencies.[201] To the extent that these reports are

194. Id. at 333.

195. James Vincent, Startup Lets Landlords Scan Tenants' Facebook to Check if They Can Pay Rent, Verge (June 10, 2016), http://www.theverge.com/2016/6/10/11903082/landlord-social-media-credit-check [http://perma.cc/9GWM-MKDR].

196. Id.

197. We Let You Know Exactly Who You're Renting to, Before They Move In, Naborly.Co, http://naborly.com [http://perma.cc/3JVS-EQGZ] [hereinafter Naborly] (last visited July 28, 2017).

198. See 15 U.S.C. § 1681a(d)(1) (2012) (defining "consumer report" as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living"); Daniel J. Solove & Paul M. Schwartz, Privacy Law Fundamentals 86 (1st ed. 2011) [hereinafter Solove & Schwartz, Privacy Law Fundamentals] (noting the FCRA "applies to 'any consumer reporting agency' that furnishes 'a consumer report'" (quoting 15 U.S.C. § 1681b (2006))).

199. Naborly, supra note 197.

200. Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 46 (2004).

201. See 15 U.S.C. § 1681a(f) (defining "consumer reporting agency" as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages . . . in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties"); Chris J. Hoofnagle, Federal Trade Commission Privacy Law and Policy 277 (2016) [hereinafter Hoofnagle, FTC Privacy Law and Policy] ("Companies selling data that are aware that they are being used for credit, insurance, employment, or tenancy screening are

being used "in a covered circumstance," one could contend that the company producing and transferring such a report is a covered entity and should comply with the FCRA requirements.[202] If these companies are not viewed as consumer reporting agencies or the FCRA does not cover the artificial intelligence reports they generate, it is not entirely clear whether consumers will have access to such reports or have an opportunity to dispute inaccuracies in these reports.[203]

Professor Hoofnagle contends that if "companies merge non-FCRA information with FCRA data it is all subject to the act."[204] It could be possible, however, for companies to separate artificial intelligence, social media, and PDE reports from traditional credit reports. An FTC staff letter evaluating a business that transferred background reports that con-

---

[consumer reporting agencies]."). The FTC explains that "tenant background-screening companies" are considered "consumer reporting agencies" under the FCRA when they "sell or provide" reports that "serve as a factor in determining . . . eligibility for housing, employment, credit, insurance, or other purposes and they include information 'bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.'" What Tenant Background Screening Companies Need to Know About the Fair Credit Reporting Act, FTC (quoting 15 U.S.C. § 1681a(d)(1)), http://www.ftc.gov/tips-advice/business-center/guidance/what-tenant-background-screening-companies-need-know-about-fair [http://perma.cc/8BW9-DMN4] (last visited July 28, 2017).

202. Letter From Maneesha Mithal, Assoc. Dir., FTC, to Renee Jackson, Nixon Peabody LLP 1 (May 9, 2011) [hereinafter FTC Social Intelligence Letter], http://www.ftc.gov/sites/default/files/documents/closing_letters/social-intelligence-corporation/110509socialintelligenceletter.pdf [http://perma.cc/R256-RNVE] (finding that a company that provided "Internet and social media background screening service used by employers . . . [is] a consumer reporting agency because it assembles or evaluates consumer report information that is furnished to third parties that use such information as a factor in establishing a consumer's eligibility for employment"); see also Alexander Reicher, The Background of Our Being: Internet Background Checks in the Hiring Process, 28 Berkeley Tech. L.J. 115, 131–33 (2013) (discussing the FTC's conclusion that Social Intelligence is a consumer reporting agency under the FCRA).

203. See A Summary of Your Rights Under the Fair Credit Reporting Act, CFPB, http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf [http://perma.cc/859V-A853] (last visited Sept. 25, 2017) (describing the right to view and contest information in consumer reports under the FCRA); Disputing Errors on Credit Reports, FTC, http://www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports [http://perma.cc/VXV2-A6P8] (last visited July 28, 2017) ("Under the FCRA, both the credit reporting company and the information provider (that is, the person, company, or organization that provides information about you to a credit reporting company) are responsible for correcting inaccurate or incomplete information in your report."); Using Consumer Reports: What Landlords Need to Know, FTC, http://www.ftc.gov/tips-advice/business-center/guidance/using-consumer-reports-what-landlords-need-know [http://perma.cc/9VJR-G9ZF] (last visited July 28, 2017) (stating that when landlords "use consumer reports to make tenant decisions, [they] must comply with the Fair Credit Reporting Act").

204. Hoofnagle, FTC Privacy Law and Policy, supra note 201.

tained social media information suggests that even when companies produce social media reports, the FCRA rules may still apply.[205]

Renter data could also be used in contexts that are not directly connected to rental determinations. In theory, a landlord could enter into an arrangement with a PDE company to provide all data generated by IOT devices the landlord owns and provides in a building. While there may be practical and technological obstacles to such an arrangement (for instance, the tenant may have supplied the IOT appliances), the landlord could provide the information to receive personalized services, discounts, or monetary compensation. Such an arrangement may not have a direct connection to housing determinations, yet the privacy and data of renters would still be at issue. Given the studies that suggest that economically vulnerable and minority consumers are more likely to rent,[206] and the possible unequal bargaining power between landlords and renters, particularly when housing supply is low, monetization by landlords may also exacerbate concerns about unequal access to privacy.

The National Conference of State Legislators reports that only one state has adopted a "social media privacy" statute applicable to landlords.[207] The Wisconsin statute prohibits landlords from requiring tenants to provide access to their Internet accounts as a "condition of tenancy."[208] The statute defines a personal Internet account as an "[i]nternet-based account that is created and used by an individual exclusively for purposes of personal communications."[209] While personal Internet accounts likely include social media accounts, it is not entirely

---

205. FTC Social Intelligence Letter, supra note 202; see also Lesley Fair, The Fair Credit Reporting Act and Social Media: What Businesses Should Know, FTC: Bus. Blog (June 23, 2011), http://www.ftc.gov/news-events/blogs/business-blog/2011/06/fair-credit-reporting-act-social-media-what-businesses [http://perma.cc/GX4M-F466]. PDE and social media reports could also simply be viewed as data about an individual's reputation. Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 276 (contending that information about someone's reputation is not a consumer report under the FCRA). But see 15 U.S.C. § 1681a(d)(1) (defining "consumer report" as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's . . . character, general reputation, [or] personal characteristics").

206. See supra note 189 and accompanying text.

207. State Social Media Privacy Laws, Nat'l Conference of State Legislators (May 5, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx [http://perma.cc/D2HL-VK6Q] (noting that twenty-five states have adopted social media privacy laws applicable to employers, sixteen of which have enacted similar laws that are applicable to educational institutions, but that Wisconsin is the only state to have adopted legislation that is applicable to landlords).

208. Wis. Stat. § 995.55 (2014) (stating that no landlord may "[r]equest or require a tenant or prospective tenant, as a condition of tenancy, to disclose access information for the personal Internet account of the tenant or prospective tenant or to otherwise grant access to or allow observation of that account").

209. Id.

clear whether accounts with PDE companies or the data insights such companies provide will be protected by the statute.

The Wisconsin statute also does not prevent landlords from reviewing or utilizing data about tenants that a landlord can acquire without the tenant's user name, password, or other security data.[210] This suggests that to the extent that the data are public or prospective tenants engage in the PDE marketplace, the information they provide could still be used or perhaps obtained by landlords if landlords do not require the tenants to disclose their passwords and other related information. Consider that Datacoup provides users with a "public link" of their data profiles that can be shared with potential data buyers.[211] Once a user distributes the link to encourage interest by data buyers, one could argue that the user's PDE data profile is now "available in the public domain" and therefore a landlord is not prohibited from using the data profile under the statute.

Landlords frequently obtain criminal background checks as part of the tenancy-application process, which may have a discriminatory impact on groups that have a "disproportionate rate of incarceration."[212] Commentators have highlighted the risks that may flow from protecting information privacy in the landlord–tenant context, such as when a landlord fails to notify tenants of the criminal history or tendencies of another tenant when there is a foreseeable risk.[213] However, the dangers associated with unequal access to privacy should not be ignored, and an appropriate balance between allowing disclosures to ensure the physical safety of co-tenants and providing baseline privacy rights to citizens on an equal basis is necessary. Careful consideration must be given to the ways in which the perceived and supposed criminality of certain groups may be used to justify data disclosures.

B. *Illusory Control and Choice*

1. *PDE Models.* — PDE companies suggest that their products offer consumers more choice and control over what happens to their data.[214] In some instances, what may be provided to consumers is the illusion of

---

210. Id. The statute defines defines "access information" as "a user name and password or any other security information that protects access to a personal Internet account" and explains that the statute "does not prohibit a landlord from viewing, accessing, or using information about a tenant or prospective tenant that can be obtained without access information or that is available in the public domain." Id.

211. MEF White Paper, supra note 23, at 27.

212. Carol Necole Brown, Experiencing Housing Law, 1323, 1409–10 (2016). Professor Brown contends that, except for a small number of local ordinances, "presently, there are no fair housing protections at the state or federal levels for individuals with criminal backgrounds." Id. at 1409.

213. E.g., Eugene Volokh, Tort Law vs. Privacy, 114 Colum. L. Rev. 879, 928 (2014).

214. See supra section III.A.2.

control and choice. A review of the terms and conditions and privacy policies of these companies indicates that some PDE companies could still monetize or disclose data once the consumer transfers or provides access to their data.[215]

Transferees of user data in Datacoup's marketplace "have access to a large pool of aggregated, de-identified, anonymous Datacoup user data."[216] Datacoup's terms and conditions state that by using the data consolidation, importation, and aggregation features of their service, a user grants the company a "non-exclusive, perpetual, irrevocable, royalty-free, sublicensable, transferable right" to aggregate, utilize, and divulge the data "for any purpose."[217] Datacoup could not only transfer this data to data buyers but also subsequently provide this information to third parties, such as advertisers and the company's analytics affiliates.[218] This subsequent potential disclosure of anonymized and aggregated data may be no different from the de-identified data disclosures and transfers made by conventional companies, except that Datacoup suggests that the company's primary goal is to empower individuals to reacquire control of their data.[219] Moreover, Datacoup's privacy policy also notes that "[u]nless expressly stated otherwise," once the company transfers consumer data to a data buyer, the information is subject only to the privacy protections that the buyer has agreed to, and "absent express limitations," the data buyer may subsequently "resell [the user's] personal information or use it in other ways that are not described in [Datacoup's] Privacy Policy."[220] Similar provisions exist in the privacy policies of other PDE-like companies.[221]

---

215. See Abraham & Oneto, supra note 28, at 3.

216. Datacoup, How Datacoup Works, supra note 135.

217. Datacoup, Terms of Service, supra note 185. Additionally, the company's terms and conditions note that users retain all intellectual property rights in their data. Id.

218. Datacoup, Privacy Policy, supra note 135 ("We may disclose aggregated or de-identified data derived from information about you to any third party. By registering for or using our Services you consent to the collection, use and sharing of such aggregated data and/or or de-identified information as Datacoup deems appropriate."). The company's privacy policy notes that the company may "analyze and draw conclusions" from a user's personal information and use the data to target users with special offers from unaffiliated parties. Id. As to personal information (defined by the company as information that can be used to identify a user), the company promises not to share this data without the user's consent, but personal information is defined to exclude aggregated or de-identified data. Id.

219. Datacoup, About Us, supra note 134 ("We are building for a future where individuals like you are in control of your data and are the chief beneficiaries of its value."); see also Datacoup, Privacy Policy, supra note 135 ("Datacoup empowers you to take control of your data . . . .").

220. Datacoup, Privacy Policy, supra note 135.

221. See, e.g., Privacy Policy, Beagli, http://www.beagli.com/legal/ (click "Privacy Policy" tab) [http://perma.cc/NH8W-3DAM] (last visited July 28, 2017) ("Beagli can share aggregated level information based on your data with third parties (any third parties). When creating this report/analysis Beagli will not allow third parties to identify you

Companies often use anonymization to justify disclosures of consumer data.[222] Overreliance on anonymization to protect consumers presumes to some extent that consumers are primarily bothered by the possibility that their names could be attached to their data.[223] However, individuals may have various reasons for objecting to the commercial use of their data.[224] As is the case in the non-PDE setting, disclosures of aggregated and de-identified data are a cause for concern in light of evidence suggesting that anonymized data could be de-anonymized or re-identified.[225] Companies may be able to make inferences and estimates about users from anonymized data and combine PDE data with information obtained from other sources to identify users.[226] Consumers have no control over how companies that make "probabilistic inferences" and identify patterns from anonymized data will treat them.[227] Hence, the artifice of consumer control. In addition to the potential harms to individual consumers, one must also consider that privacy "is also a pub-

based on your data and will not pass on any contact information to third parties."); Privacy, Cozy, http://forum.cozy.io/privacy [http://perma.cc/8YUK-YMRT?type=image] (last visited July 28, 2017) ("We do not sell, trade, or otherwise transfer to outside parties your personally identifiable information. . . . However, non-personally identifiable visitor information may be provided to other parties for marketing, advertising, or other uses.").

222. See Schwartz & Solove, The PII Problem, supra note 32, at 1836–47.

223. Bonnie Kaplan, Selling Health Data: De-Identification, Privacy, and Speech 8 (Yale Inst. for Soc. & Policy Studies, Bioethics Working Paper No. 14-024, 2014), http://bioethics.yale.edu/sites/default/files/files/ISPS14-024.pdf [http://perma.cc/G586-X2XP].

224. Id.

225. See Sharona Hoffman, Electronic Health Records and Medical Big Data: Law and Policy 136 (2016) [hereinafter Hoffman, Electronic Health] (discussing the possible re-identification of de-identified electronic health records through "nonmedical data, such as voter registration records" as well as "records of patients' medication purchases, media stories about accidents and illnesses, Facebook, and other sources"); Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701, 1701 (2010) (contending that computer "scientists have demonstrated that they can often 'reidentify' or 'deanonymize' individuals hidden in anonymized data with astonishing ease"); Ira S. Rubinstein & Woodrow Hartzog, Anonymization and Risk, 91 Wash. L. Rev. 703, 705 (2016) (contending that "the failure of anonymization has identified a weakness in the focus of the law surrounding data releases"). Professor Sharona Hoffman suggests that even though the risk of re-identification may appear small, re-identification could impact "tens of thousands or even hundreds of thousands of records." Hoffman, Electronic Health, supra, at 225. For a discussion of how medical records might be de-anonymized, see Kaplan, supra note 223, at 8–9 (contending that as "the information kept in medical records grows to include patients' genomes and other genetic information as well as data on social and behavioral determinants of health . . . it will be easier to identify patients from their records").

226. Solon Barocas & Helen Nissenbaum, Big Data's End Run Around Procedural Privacy Protections, Comm. ACM, Nov. 2014, at 31, 32–33 (contending that anonymization practices make it harder for third parties to discover "embarrassing, discrediting, or incriminating facts, but they do nothing to limit the ability of these companies to draw upon this information in shaping a growing share of everyday experiences that take place on these companies' platforms.").

227. Id.

lic value (of value to the democratic political system) and it is a collective value."[228]

By going directly to the source of the data—the consumer—PDE companies can obtain access to consumer data without having to rely on established data brokers. However, some PDE companies are arguably also data brokers to the extent that they compile and share user data. The FTC describes data brokers as "companies that collect consumers' personal information and resell or share that information with others" for several purposes.[229] PDE companies could also purchase information about consumers from various sources and then sell or provide access to the data to third parties.

Absent explicit restrictions imposed on the types of transferees that are permitted to participate in PDE marketplaces, established data brokers may be able to obtain consumer data in the PDE marketplace. A company that has entered into an agreement with a data broker could obtain access to PDE data and subsequently provide this information to the data broker. Thus, consumer data may simply move from one data broker to another with the difference being that there is now direct (or seemingly more active) consumer interaction enabling this process.

Admittedly, some PDE data-insight companies have taken a seemingly more proactive approach to addressing consumer-privacy and data-protection concerns. Digi.me's privacy summary notes that it does not track consumer activity, and it does not store or see social media account information or any associated personal data.[230] As a result, it cannot sell or use user data. Digi.me collects certain "anonymized statistics" about users, but the company's terms of service indicate that users can opt out of this process.[231] Meeco's privacy policy indicates that it does not mone-

---

228. Kirsty Hughes, The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse, *in* Social Dimensions of Privacy: Interdisciplinary Perspectives 225, 225 (Beate Roessler & Dorota Mokrosinska eds., 2015); see also Priscilla M. Regan, Legislating Privacy: Technology, Social Values, and Public Policy 220–43 (1995).

229. FTC Data Broker Report, supra note 143, at i.

230. See Digi.me Is Free . . . so How Do We Make Money?, Digi.me, http://www.digi.me/business-model [http://perma.cc/D9FA-AJCU] (last visited July 28, 2017) ("We never see, touch or hold your personal data so we couldn't use or sell it even if we wanted to. And we don't."); Your Privacy Is Paramount, Digi.me, http://docs.wixstatic.com/ugd/03cafa_cf269cf4470a45d0b226cca73edb0263.pdf [http://perma.cc/9ZVJ-BZJW] [hereinafter Digi.me, Paramount] (last visited Sep. 7, 2017) ("We do not: 1. Store any personal data on you except your name & email address, your country of residence and the language you are using in the application . . . 3. Track your activity except for checking that your license is valid when you use the application."). The company's website also indicates that, even when a user accepts a company's data request via a consent contract, "digi.me makes the agreed data available to the company for a limited time via a secure connection, encrypted so only they can see it." A Better Way to Share, Digi.me, http://www.digi.me/sharing [http://perma.cc/8Z5F-MC8F] (last visited July 28, 2017).

231. Digi.me End User Terms, Digi.me, http://www.digi.me/terms [http://perma.cc/L2N8-E5WW] (last visited July 28, 2017) (noting that the company collects anonymized statistics "including but not limited to version numbers of software, the features within the

tize consumer data, and the company's website acknowledges that consumers should have the "right to be free from surveillance [and] targeted and intrusive advertising."[232] However, the company's terms and conditions also note that if a user grants a third party access to their information, the user is subject to that third party's terms and conditions.[233]

Even if consumers have the option to control which companies can obtain access to their data profiles, issues similar to those prevalent in previously discussed data-business models (such as the data-as-payment and freemium models) may also arise.[234] These issues include a lack of consumer understanding of the potential implications of providing consent to data collection and disclosure. For instance, although consumers may be provided with consent terms and information about potential data buyers before agreeing to transfer or provide access to their data and may be given the ability to deny data access or sale requests, it is unclear whether consumers engaging in the PDE marketplace will review and understand any such disclosures or rights before agreeing to the transfer or disclosure. The lure of compensation and discounts (even if minor) may outweigh considerations regarding potential purchasers of consumer data and subsequent data usage. Consumers who choose to participate in the PDE marketplace may not grasp the extent to which their data can be subsequently monetized once it is disclosed or transferred and how the data can be used by companies to make inferences about their lives and impact the opportunities they receive. Consumers may be unlikely to impose use restrictions on data transferees, such as prohibiting data analytics and generating inferences or review the terms and conditions and privacy policies of a company accessing their data to determine what will happen to their data after

---

digi.me app being used and information on which services are being synced," but users have the ability to opt out of the anonymous data collection process). The company's website suggests that the information collected is fully anonymized so it cannot identify users and does not have any access to user data through the anonymization process. Id.; Digi.me, Paramount, supra note 230.

232. Meeco, How It Works, supra note 122; see also Abraham & Oneto, supra note 28, at 3; Meeco, Introduction to Meeco, supra note 122 ("Unlike other services, Meeco does not mine or sell your data."); Meeco, Privacy Policy, supra note 129. Meeco's privacy policy states that the company may disclose aggregated data by, for instance, publishing reports on "trends in the usage of [the company's] website or anonymous intentions" and users may opt out of direct marketing from the company. Id. As to licenses, Meeco's privacy policy notes that "to facilitate the Meeco Services on Your behalf, You hereby grant to Meeco a non-exclusive, royalty-free license to store, reproduce and display Your Data solely as reasonably necessary to provide the Meeco Services at Your direction and on Your behalf, and subject to this Agreement and our Privacy Policy." Id.

233. General Terms and Conditions for Meeco & Mecast Users, Meeco, http://www.meeco.me/meeco-terms.pdf [http://perma.cc/DGY8-L5FW] [hereinafter Meeco, Terms and Conditions] (last updated Sept. 15, 2015).

234. See supra section III.A.

transfer or disclosure. Thus, problems associated with notice and choice in older business models may continue under PDE models.

Additionally, it is not entirely clear whether consumers will be able to consistently negotiate contract terms to exert sufficient control over how data buyers or companies that gain access to their data will use the data once it is obtained. These companies may simply provide their terms and conditions and privacy policies on a take-it-or-leave-it basis. PDE companies may not always provide users with the ability to negotiate such terms. At least one PDE company touts that it allows users to control third-party access to their data as well as issue their own terms and conditions and notes,[235] but the company's terms and conditions indicate that a user-generated term can be treated as a mere request and may be unenforceable.[236]

Companies' earlier efforts to provide consumers with more control over their data have not been widely successful for various reasons, especially because other companies have been able to simultaneously obtain access to consumer data.[237] Professor Eric Goldman contends that the "infomediaries" of the dot-com era may have failed because of "marketer disincentives to pay to participate, consumer reluctance to invest, and operation costs."[238] Although PDE companies may give consumers the

---

235. Meeco, http://meeco.me [http://perma.cc/535Y-RFEQ] [hereinafter Meeco, Homepage] (last visited July 28, 2017) (describing Meeco's "sharing on your terms" policy and Consent Manager).

236. Meeco, Terms and Conditions, supra note 233. The company's terms and conditions provide that "Sharing Permissions will default to 'do not share with Third Parties or make Public without my permission' and 'do not sell or trade without my permission.'" Id. This suggests that users may have the ability in some instances to limit disclosures of their data, but this ability may not extend to other forms of monetization or inferences that can be made once user data are accessed or obtained by third parties.

237. See Hoofnagle & Whittington, Unpacking Privacy's Price, supra note 135, at 1347 (describing how the "diffusion of personal information in the marketplace" allows others to easily access consumer data). For discussions of "infomediaries" and their failures, see Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 Vand. L. Rev. 1609, 1686 (1999) ("Taken by themselves, however, infomediaries are unlikely to turn fair information practices into cyberspace's predominant norms. Infomediaries negotiating around a default of *maximum* disclosure of personal information will be incapable of shifting the customs of the Web through their practices."); Bethany L. Leickly, Intermediaries in Information Economies (Apr. 30, 2004) (unpublished M.A. thesis, Georgetown University), http://extrafancy.net/bethany/intermediaries.pdf [http://perma.cc/V35Y-3DR8] (providing a case study of earlier generations of infomediaries and identifying various reasons for their failures).

238. Goldman, Coasean Analysis, supra note 128, at 1198–99; see also Net Worth: Shaping Markets when Customers Make the Rules, Harv. Bus. Sch. Press (Oct. 12, 1999), http://hbswk.hbs.edu/archive/812.html [http://perma.cc/LV3Z-DRW9] (describing an infomediary as a "trusted third party to act as the custodian, agent, and broker of [consumer] information, marketing it to businesses on the consumer's behalf while at the same time protecting consumer privacy"). PDE companies share some characteristics with the "infomediaries" proposed by John Hagel III and Marc Singer and discussed by Professor Goldman, such as protecting consumer privacy. See Goldman, Coasean Analysis, supra note 128, at 1198 (describing the characteristics of the "infomediaries" proposed by Hagel

ability to decide with whom to share their data, tracking by other companies that use a data-as-payment or a freemium model may undermine these efforts. These other companies may have access to the exact same information that consumers provide to PDE companies and, as a result, may continue to monetize and disclose consumer data.

2. *PFP Models.* — The privacy-as-a-luxury model may provide more options for consumers to protect their privacy. Yet it is not entirely clear whether all companies using this model will refrain from monetizing consumer data. Of course, given the fact that the primium model is based on providing privacy controls and protection to consumers, one can only assume that selling or providing access to consumer data to advertisers or data brokers is contrary to the essence of the product that is provided to the primium user.

Privacy-conscious consumers who elect to pay for and use VPN services may also be misled into believing that their online activities will be completely anonymized.[239] Some VPN providers may "advertise an 'anonymous service' on their website but the fine print in their privacy policy suggests they log a significant amount of customer data."[240] In some instances non-VPN companies may prevent consumers from accessing their websites and services while using VPNs and may prevent

---

and Singer); see also John Hagel III & Jeffrey F. Rayport, The Coming Battle for Customer Information, Harv. Bus. Rev., Jan.–Feb. 1997, at 53, 54 (proposing and discussing the role of "infomediaries"). However, some PDE companies do not appear to "actively seek out the lowest price for a desired good or service," one of the characteristics or objectives of "infomediaries." Goldman, Coasean Analysis, supra note 128, at 1198; see also John Hagel III & Marc Singer, Net Worth: Shaping Markets when Customers Make the Rules 19, 35 (1999) (discussing the role of infomediaries in targeted marketing and obtaining the best prices for users). Some PDE companies have acknowledged that users should have a right to be free from targeted advertising in contrast to an "infomediary" that "anticipate[s] its clients' purchasing behavior and suggest[s] products and services before the client begins to search for them." Allison B. Smith, Net Worth: Shaping Markets when Customers Make the Rules, 18 J. Pub. Pol'y & Marketing 275, 276 (1999) (book review); see also Meeco, How It Works, supra note 122 (discussing users' right to be free from "targeted and intrusive advertising"). While PDE companies share some characteristics with "infomediaries," to the extent that PDE companies adopt an approach to data and privacy that focuses on the best interests of consumers rather than primarily "facilitating targeted advertisements," they may be more akin to the professional Personal Data Guardian (PDG) proposed by Professor Jerry Kang and others. See Jerry Kang et al., Self-Surveillance Privacy, 97 Iowa L. Rev. 809, 837 (2012) ("[T]he goal of the PDG is not to minimize transaction costs of online shopping by facilitating targeted advertisements. Instead, the role ideology . . . is to intentionally and mindfully slow down data flows, advise the individual of unexpected consequences, and adopt default best practices . . . in the individual's best interests.").

239. See I Am Anonymous When I Use a VPN—10 Myths Debunked, Golden Frog: Blog (July 28, 2015), http://www.goldenfrog.com/blog/myths-about-vpn-logging-and-anonymity [http://perma.cc/39UZ-7Y4U] (describing the "disturbing trend" of VPN providers promising "anonymous service" without detailing how exactly data are handled).

240. Id.

their payment platforms from being used in VPN-related transactions.[241] In such an event, the consumer may need to temporarily disconnect from the VPN in order to access unaffiliated websites and services. Thus, the privacy and control promised by a VPN company may not always be absolute.

As to PFP discount programs in the broadband context, there is also an illusion of control and choice. Even customers who elected not to take the discount previously offered by one ISP to entice consent to its data collection practices may have had some of their activities monitored. These consumers paid higher monthly fees (thereby paying for privacy) in order to avoid data collection. The FCC has noted that the ISP company mentioned above previously acknowledged "that it nonetheless 'may collect and use web browsing information for other purposes, as described in [the company's] Privacy Policy, even [for customers who] do not participate in the Internet Preferences program.'"[242]

C. *The PDE and New Monetization Techniques*

Currently, PDE companies utilize two main monetization options: (1) providing data insights, control, customized deals, and personalized experiences in exchange for access to consumer data; and (2) providing monetary compensation in exchange for purchasing or obtaining rights in consumer data and transferring that data to third parties or the PDE company. Given the expected volume of IOT data, additional monetization schemes may also be offered to users. However, concerns may arise when new monetization schemes are used.

If the value, velocity, and quantity of consumer data increase with the rise of the IOT, both lenders and consumers could eventually view consumer data as an attractive asset for use in routine secured transactions.[243]

---

241. Klint Finley, VPNs Won't Save You from Congress' Internet Privacy Giveaway, Wired (Mar. 28, 2017), http://www.wired.com/2017/03/vpns-wont-save-congress-internet-privacy-giveaway/ [http://perma.cc/5LS6-VHTS] [hereinafter Finley, VPNs Won't Save You]; see also Julia Greenberg, For Netflix, Discontent over Blocked VPNs Is Boiling, Wired (Mar. 7, 2016), http://www.wired.com/2016/03/netflix-discontent-blocked-vpns-boiling/ [http://perma.cc/CVM4-ASYQ] (describing Netflix's blocking of VPNs); Matt Kamen, Paypal Bans VPN and DNS Services, Wired (Feb. 5, 2016), http://www.wired.co.uk/article/paypal-bans-vpn-and-dns-services [http://perma.cc/9UQ7-H7PS] (describing PayPal's blocking of VPNs).

242. Notice of Proposed Rulemaking, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 31 FCC Rcd. 2500, 2582 n.402 (2016). AT&T recently indicated that it will end its PFP offerings, but given the repeal of the FCC Rules other ISPs may begin to offer such plans and AT&T could elect to reinstate its program. See Aaron Pressman, Here's Why AT&T Internet Customers Won't Pay Extra for Privacy Anymore, Fortune (Sept. 30, 2016), http://fortune.com/2016/09/30/att-internet-fees-privacy/ [http://perma.cc/PSF7-XX9P] (quoting AT&T as stating that it "plan[s] to end the optional Internet Preferences advertising program").

243. Bos. Consulting Grp., The Value of Our Digital Identity 2, 22 (2012), http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf [http://

Consumer data could be viewed as a general intangible under Article 9 of the UCC. A consumer could then elect to use her data as collateral to obtain financing from a lender who retains a security interest in the collateral. This would provide an alternative source of financing for consumers. Companies may be able to use their intangible assets, such as customer lists, to obtain financing from lenders, and consumer databases are valuable assets that can be transferred to third parties during bankruptcy proceedings.[244] Thus, if companies can monetize consumer data and lists for financing schemes, perhaps consumers should be permitted to do the same. However, consumers may be more adequately protected if transfer and assignment restrictions are imposed on certain types of data.[245]

The largest obstacle to such a monetization method is the perceived value of a consumer's individual data, which may be worth significantly less than the vast quantities of aggregated data and customer lists companies hold.[246] In evaluating whether such a monetization method should

---

perma.cc/BF7C-8MNN] (suggesting that "as the volume and variety of data grows, so does its value" and the value created through digital identity has a twenty-two percent annual growth rate); FTC, Big Data: A Tool for Inclusion or Exclusion? 2 (2016), http://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [http://perma.cc/V7FA-7MH4] (describing the velocity of data as "the speed with which companies can accumulate, analyze, and use new data"); Terrell McSweeny, Comm'r, FTC, Remarks to the U.S. Chamber of Commerce at TecNation 8 (Sept. 20, 2016), http://www.ftc.gov/system/files/documents/public_statements/985773/mcsweeny_-_tecnation_2016_9-20-16.pdf [http://perma.cc/VEJ3-L68H] ("What is changing in the digital economy is the volume, velocity, variety and value of data—or the four Vs."); The Increasing Value of Data, Future Agenda, http://www.futureagenda.org/insight/the-increasing-value-of-data [http://perma.cc/8WT4-5W9A] (last visited July 28, 2017) (suggesting that by 2020 "the sum of all the digitally available information about [individuals] will be worth €1 trillion"); see also Schwartz, Property, Privacy, and Personal Data, supra note 30, at 2056 ("The monetary value of personal data is large and still growing . . . ."); Omer Tene, Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws, 74 Ohio St. L.J. 1217, 1228 (2013) (contending that there has been a "surge in the value of personal data for governments, businesses, and individuals").

244. Xuan-Thao N. Nguyen, Collateralizing Privacy, 78 Tul. L. Rev. 553, 576–77 (2004) (describing consumer databases as intangible assets that can be used as collateral). See generally Walter W. Miller, Jr. & Maureen A. O'Rourke, Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?, 38 Hous. L. Rev. 777 (2001) (discussing the use of customer databases in bankruptcy proceedings).

245. Elvy, Commodifying Consumer Data, supra note 11, at 75 (discussing the imposition of transfer and assignment restrictions on companies' use of certain consumer data); Miller & O'Rourke, supra note 244, at 847 ("[T]here may be some information that should be inalienable because of its highly personal nature."); see also Helen Nissenbaum, Privacy as Contextual Integrity, 79 Wash. L. Rev. 119, 121, 154–55 (2004) (arguing for the adoption of a contextual-integrity approach to protecting privacy that can consider "the nature of the information," among other things).

246. Additionally, Article 9 of the UCC excludes certain assignments in consumer transactions from its scope. More specifically, Article 9 does not apply to "assignment[s] of . . . deposit account[s] in . . . consumer transaction[s]." U.C.C. § 9-109(d)(13) (Am. Law Inst. & Nat'l Conference of Comm'rs on Unif. State Laws 2014) (stating that Article 9 does not

be permissible, the policy reasons associated with a historical federal approach that frowns upon non-purchase money security interests in certain consumer items with minimal resale value must also be considered.[247] Digi.me suggests that its product will allow users to create "rich, deep datasets" that will be attractive to companies.[248] Cozy anticipates that users will use its platform as a "personal data hub" to aggregate data from multiple aspects of their lives.[249] The company has created an app that allows users to "import data" from their Google accounts.[250] Once a PDE company aggregates and processes an individual's data, it could be viewed as an attractive valuable asset on an individual level.

While permitting consumers to use their data for financing transactions under Article 9 is a promising idea, there are possible negative consequences that may result from allowing such transactions to occur. For example, Article 9 permits secured parties to foreclose on collateral in the event of a default as defined by the security agreement.[251] Failure to make timely payments is a common event of default. After default, the secured party may dispose of the collateral, including by selling it to third parties.[252] Data brokers and entities that prey on financially struggling consumers would of course be prime potential purchasers of this type of

---

apply to "an assignment of a deposit account in a consumer transaction, but Sections 9-315 and 9-322 apply with respect to proceeds and priorities in proceeds"). The official comments to Article 9 state that the aim of the exclusion of deposit accounts "as original collateral in consumer transactions" is to ensure that such transactions are left to "law other than" Article 9. Id. § 9-109 cmt. 16. One could contend that assignments of data in consumer transactions should not be subject to Article 9.

247. See, e.g., Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 301–02 (discussing 16 C.F.R. pt. 444 and the policy concerns associated with a "blanket security interest in household goods," such as the imposition of "psychological discomfort on debtors"); see also 16 C.F.R. § 444.1 (2011) (defining household goods as used within § 444.2); id. § 444.2 ("[I]t is an unfair act or practice . . . for a lender or retail installment seller directly or indirectly to take or receive from a consumer an obligation that . . . [c]onstitutes or contains a nonpossessory security interest in household goods other than a purchase money security interest.").

248. Firth, The Digi.me Story, supra note 121 (stating that the company's product will "allow businesses, who want access to these rich, deep datasets that our users will soon hold, to approach them directly and offer them personalised offers in exchange for seeing some slices of that data").

249. Make Sense of Your Data, Cozy, http://cozy.io/en/make-sense-of-your-data/ [http://perma.cc/8P57-SYH6] (last visited July 28, 2017) ("Health data coming from a fitness tracker, information flowing from sensors and appliances in your home, your travel itineraries and hotel bookings, bank transactions and financial information—there is a wealth of data pouring in from multiple sources.").

250. Applications, Cozy, http://cozy.io/en/apps/ [http://perma.cc/N22L-U3YC] (last visited July 28, 2017).

251. U.C.C. § 9-601(a); id. § 9-610 (providing rules for foreclosure via a "disposition of the collateral"); id. § 9-620 (providing rules for foreclosure via "acceptance of collateral in full or partial satisfaction of the obligation"). Article 9 also provides that "in a consumer transaction, a secured party may not accept collateral in partial satisfaction of the obligation it supports." Id. § 9-620(g).

252. Id. § 9-610.

collateral (assuming that they do not already have access to the same information contained in a user's PDE data profile).

Consumer-data monetizations under Article 9's financing scheme may also exacerbate concerns about unequal access to privacy. If secured-financing monetization methods become viable, economically vulnerable consumers may be more likely to grant security interests in their data, thereby monetizing their privacy. Even if user data are not viewed as a desirable standalone asset, they could be combined with other consumer assets to form a valuable asset package. Additionally, if consumer data are viewed as a common asset to be used for financing transactions, the market may eventually require all consumers (even those who would desire more privacy) to provide their PDE data profiles to obtain financing. Therefore, if a market develops for consumers to monetize their data for secured financing purposes and such transactions are covered by the UCC, the application of Article 9 to consumer-data transactions must be closely monitored to ensure that its provisions, including default and enforcement rules, do not consistently harm consumer interests.[253]

D. *Predatory and Discriminatory Behavior*

After collecting consumer data, data brokers have generated categories and labels to describe consumers, such as "Retiring on Empty: Singles," "Rural and Barely Making It," "Tough Start: Young Single Parents," and "Credit Crunched: City Families."[254] Data brokers use these labels in providing consumer information to data buyers.[255] Some companies have used consumer data to identify low-income and vulnerable consumers for predatory marketing campaigns.[256] During the housing bubble preceding the most recent financial crisis, companies used data about consumers to engage in predatory lending and discriminatory

253. Other laws regulating debt collection may also need to be considered. The Consumer Financial Protection Bureau (CFPB), which has "overlapping jurisdiction" with the FTC, may also play a role in protecting consumers in such transactions. Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 269. Additionally, the Gramm-Leach Bliley Act (and similar state laws), which regulates data collection, disclosures, and transfer of "nonpublic personal information" by financial institutions and uses a notice-and-choice framework could also be applicable to any such transactions. Id. at 292–94; Daniel J. Solove & Paul M. Schwartz, Consumer Privacy and Data Protection 88–92 (2015) [hereinafter Solove & Schwartz, Consumer Privacy] (contending that under the Gramm-Leach Bliley Act "[f]inancial institutions can share personal information with nonaffiliated companies only if they first provide individuals with the ability to opt out of the disclosure" and discussing confidentiality and use restrictions imposed on data transfers to third parties and similar state laws); see also 15 U.S.C. § 6802 (2012).

254. Staff of S. Comm. on Commerce, Sci. & Transp., Review of the Data Broker Industry, supra note 7, at ii.

255. Id.

256. See Amy J. Schmitz, Secret Consumer Scores and Segmentations: Separating "Haves" from "Have-Nots," 2014 Mich. St. L. Rev. 1411, 1413; see also Fulton, supra note 176.

behavior to the detriment of marginalized communities.[257] The IOT and the use of PFP and PDE models may provide opportunities to further enable this type of behavior.

1. *PFP Models.* — Recall from section III.A that consumers from vulnerable communities may be more willing to accept discounts offered under PFP discount models.[258] IOT devices often rely on a Wi-Fi connection provided by ISPs to function and access the Internet.[259] In theory, even consumers that rely primarily on their smartphones to access the Internet could use their smartphones as Wi-Fi hotspots to enable their IOT devices to function. In the IOT setting, in which consumers are generating more data than ever before, privacy-discount models could enable companies to stockpile increasingly intimate details about marginalized consumers who are more willing to accept privacy-invasive discounts. As Professor Scott Peppet notes, with the IOT "everything reveals everything," and IOT data could be combined "in unexpected ways, giving rise to powerful inferences from seemingly innocuous data sources."[260] Once consumers accept a privacy-invasive

---

257. See andré douglas pond cummings, Racial Coding and the Financial Market Crisis, 2011 Utah L. Rev. 141, 159; see also Carol Necole Brown, Intent and Empirics: Race to the Subprime, 93 Marq. L. Rev. 907, 908–12 (2010) (discussing housing discrimination and subprime lending); Pamela Foohey, Lender Discrimination, Black Churches, and Bankruptcy, 54 Hous. L. Rev. 1079, 1102–14 (2017) (discussing discrimination in lending to African American churches); Jim Hawkins, Are Bigger Companies Better for Low-Income Borrowers?: Evidence from Payday and Title Loan Advertisements, 11 J.L. Econ. & Pol'y 303, 324 (2015) (discussing how payday and title lenders target minorities); Creola Johnson, America's First Consumer Financial Watchdog Is on a Leash: Can the CFPB Use Its Authority to Declare Payday-Loan Practices Unfair, Abusive, and Deceptive?, 61 Cath. U. L. Rev. 381, 419 (2012) (discussing the impact of advertisement by payday lenders on consumer choice); Kristin Johnson, Steven Ramirez & Cary Martin Shelby, Diversifying to Mitigate Risk: Can Dodd-Frank Section 342 Help Stabilize the Financial Sector?, 73 Wash. & Lee L. Rev. 1795, 1813 (2016) (exploring the causes of the 2007–2009 financial crisis); Steven A. Ramirez, The Virtues of Private Securities Litigation: An Historic and Macroeconomic Perspective, 45 Loy. U. Chi. L.J. 669, 708 (2014) (discussing predatory lending practices).

258. See supra section III.A; see also Fulton, supra note 176.

259. Press Release, Gartner, Gartner Says Organizations Must Update Their Network Access Policy to Address Attack of IoT Devices (Sept. 8, 2016), http://www.gartner.com/newsroom/id/3436717 [http://perma.cc/Q45P-S2VL] ("[M]any IoT devices will be connected via Wi-Fi . . . ."); Verizon Wi-Fi, Verizon, http://www.verizon.com/home/wifi-wireless-internet-service/ [http://perma.cc/7GWE-BR2X] (last visited Sept. 9, 2017) (discussing Verizon's Wi-Fi service).

260. Peppet, Regulating the Internet, supra note 38, at 117–40 (discussing concerns regarding discrimination, privacy, and security on the IOT). Professor Hoffman discusses the implications in the medical industry:

> [O]pen data may enable discrimination by employers, financial institutions, and anyone with a stake in people's health. These entities may attempt to re-identify publicly available health records that belong to applicants or to employees. In the alternative, they may mine medical data to find statistical associations between particular attributes, habits, or behaviors (for example, obesity or smoking) and

discount, companies that obtain consumer data through this model can deploy "predictive data devices to discriminate against consumers they deem less valuable or too risky."[261] The chief executive officer of one cable company has openly discussed the use of consumer lifestyle data and data analytics in making choices about services offered to consumers and suggested that the "company's technicians [were not] going to 'spend 15 minutes setting up an iPhone app' for a customer who has a low FICO score."[262]

Some mobile carriers have allegedly packaged and transferred to third parties data generated from consumers' use of their products.[263] In some instances, purchasers of this data do not disclose which companies

---

> health risks. Then, based on their findings, entities could formulate discriminatory policies that exclude from employment, financial, or other opportunities individuals they perceive as high-risk.

Sharona Hoffman, Citizen Science: The Law and Ethics of Public Access to Medical Big Data, 30 Berkeley Tech. L.J. 1741, 1746 (2015).

261. Schmitz, supra note 256, at 1414; see also Solon Barocas & Andrew D. Selbst, Big Data's Disparate Impact, 104 Calif. L. Rev. 671, 677 (2016) (discussing how data mining has the potential to be used in a discriminatory manner); Mary Madden et al., Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans, 95 Wash. L. Rev. (forthcoming 2017) (manuscript at 53), http://ssrn.com/abstract=2930247 (on file with the *Columbia Law Review*) (discussing the negative impact of big data in "employment screening," "predictive policing," and "access to higher education" on poor communities). See generally Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy (2016) (discussing big data and discrimination).

262. Daniel Frankel, Cable One Using FICO Scores to Qualify Video Customers, Might Says, Fierce Cable (May 23, 2016) (quoting Thomas Might, CEO, Cable One), http://www.fiercecable.com/cable/cable-one-using-fico-scores-to-qualify-video-customers-might-says [http://perma.cc/N8Z4-L4DC]. Cable One later attempted to clarify these comments. Daniel Frankel, Cable One Clarifies FICO Score Usage with FCC, Says It Has Its Own System for Determining Customer Value, Fierce Cable (June 28, 2016), http://www.fiercecable.com/cable/cable-one-clarifies-fico-score-usage-fcc-says-it-has-its-own-system-for-determining-customer [http://perma.cc/77LK-QYWW]; see also Warren Letter, supra note 16 (discussing statements made by Cable One's CEO and urging the FCC to scrutinize PFP models in the broadband setting).

263. David Goldman, Your Phone Company Is Selling Your Personal Data, CNN Money (Nov. 1, 2011), http://money.cnn.com/2011/11/01/technology/verizon_att_sprint_tmobile_privacy/index.htm [http://perma.cc/V6KZ-HZ3N] (describing AT&T's and Sprint's use of consumer data and changes in Verizon's privacy policy that allowed the company to "record customers' location data and Web browsing history, combine it with other personal information . . . , aggregate it with millions of other customers' data, and sell it on an anonymous basis"); Kate Kaye, The $24 Billion Data Business that Telcos Don't Want to Talk About, AdvertisingAge (Oct. 26, 2015), http://adage.com/article/datadriven-marketing/24-billion-data-business-telcos-discuss/301058/ [http://perma.cc/HMA6-PVA3] (describing how mobile carriers are working with partners to sell data); Jay Stanley, Why Broadband Carriers Are a Menace to Privacy, ACLU: Free Future (Aug. 1, 2016), http://www.aclu.org/blog/free-future/why-broadband-carriers-are-menace-privacy [http://perma.cc/WJZ2-KG43] (suggesting that broadband companies "eavesdrop[] on . . . communications to sell targeted advertising").

are transferring the information.[264] The Electronic Frontier Foundation reports that ISPs have previously hijacked "consumers' search queries" (the process of redirecting queries to third party websites that may record the traffic and provide search results primarily from companies that have paid for increased traffic), snooped through consumer browsing traffic and subsequently placed targeted advertisements in consumer web traffic, and preinstalled software on smartphones to view and record applications and websites that consumers access.[265] Companies could engage in predatory behavior to encourage or coerce consumers to consent to PFP discount plans that further these practices, while pretending to provide consumers with the choice of accepting a discount or paying a higher price for products and services. They may also use consumer data to engage in discriminatory behavior to the detriment of vulnerable communities and cities in which low-income consumers are concentrated. This concern may also be present in the PFP luxury model as well as in the non-PFP context. However, use of PFP models may deceive consumers into believing that their data and privacy will be completely protected if they can pay enough for privacy, while simultaneously providing companies with the opportunity to collect more data from the financially disadvantaged as well as some information about those who pay higher fees. Thus, PFP models provide a vehicle through which companies can obtain consumer data that can be used to target specific groups of consumers as well as further facilitate predatory and discriminatory behavior.

2. *PDE Models.* — PDE models can also facilitate predatory behavior. Some PDE companies may have access to social media accounts and other information about consumers, and these companies could permit advertisers and other third parties to access consumer data profiles or aggregated data based on those profiles. The quantity and variety of consumer data may increase as consumers begin integrating their IOT devices with the data compilation platforms offered by PDE companies. This creates additional avenues for the disclosure of new types of consumer data. Admittedly, consumer data could be used in ways that are beneficial to consumers, and this may in fact be the goal of some PDE

264. Kaye, supra note 263; see also Jeremy Gillula, Five Creepy Things Your ISP Could Do if Congress Repeals the FCC's Privacy Protections, Elec. Frontier Found. (Mar. 19, 2017), http://www.eff.org/deeplinks/2017/03/five-creepy-things-your-isp-could-do-if-congress-repeals-fccs-privacy-protections [http://perma.cc/2PUP-BGJG].

265. Gillula, supra note 264; see also Finley, VPNs Won't Save You, supra note 241 (explaining AT&T, Sprint, and T-Mobile "all sold smartphones with preinstalled tracking software"); John Stephens, Repeal of FCC Privacy Rules Leaves America Vulnerable, Law360 (Apr. 26, 2017), http://www.law360.com/articles/917279/repeal-of-fcc-privacy-rules-leaves-america-vulnerable [http://perma.cc/443M-6CX8] (discussing ISP's "insertion of adware and spyware" into consumers' "browsers and mobile phones" to facilitate targeted advertising and contending that the repealed "FCC privacy rules would have ended this practice").

companies. However, once access to the data is granted to third parties, these companies could use the information for purposes that are detrimental to vulnerable consumers.[266] There are numerous examples of such behavior in the non-PDE context.[267] One retailer has allegedly used data about consumers to provide individuals living in neighborhoods with higher average incomes with discounted prices while individuals living in areas with lower average incomes "tended to see higher prices."[268] Datacoup's terms of service suggest that retailers and other third parties may use their products to provide targeted offers to specific types of users.[269] Companies that obtain access to consumer data from PDE companies should not be allowed to subsequently monetize the data in ways that are harmful to consumers.

In the tenancy context, the use of PDE-renter insights or data obtained by tenant screening companies or landlords could also engender discriminatory behavior. Federal and state legislation prohibiting discrimination in housing may alleviate some of these concerns. These statutes generally restrict the ability of parties to discriminate on the basis of race and sex, among other things.[270] Wisconsin's social media statute, discussed in section III.A above, and other housing regulation prohibit landlords from engaging in discriminatory behavior on similar grounds.[271] Rather than

---

266. See Cohen, Examined Lives, supra note 150, at 1398 ("A perverse consequence of a purely market-based approach to data privacy rights, then, may be more discounts for the rich. If so, then the poor will lose twice over. They will have less privacy, and they will also pay more for goods and services than more desirable customers.").

267. See generally Rory Van Loo, Helping Buyers Beware: The Need for Supervision of Big Retail, 163 U. Pa. L. Rev. 1311, 1311 (2015) (contending that empirical data suggests that the "behavioral economics-related practices" of various retailers that rely on data analytics and consumer data "in the aggregate may significantly harm all households, costing even a family at the poverty line hundreds of dollars annually").

268. Jennifer Valentino-Devries, Jeremy Singer-Vine & Ashkan Soltani, Websites Vary Prices, Deals Based on User's Information, Wall St. J. (Dec. 24, 2012), http://www.wsj.com/articles/SB10001424127887323777204578189391813881534 (on file with the *Columbia Law Review*).

269. Datacoup, Terms of Service, supra note 185 ("Retailers, online companies, and other third parties may use our Services to target offers to certain types of users based on parameters that they provide to us.").

270. 42 U.S.C. § 3604(b) (2012) (stating it is unlawful "[t]o discriminate against any person in the terms, conditions, or privileges of sale or rental of a dwelling, or in the provision of services or facilities in connection therewith, because of race, color, religion, sex, familial status, or national origin"); Wis. Stat. § 106.50 (2017) (prohibiting discrimination in housing on the basis of "sex, race, color, sexual orientation, disability, religion, national origin, marital status, family status, status as a victim of domestic abuse, sexual assault, or stalking, lawful source of income, age, or ancestry"); Fair Housing—It's Your Right, U.S. Dep't of Hous. & Urban Dev., http://portal.hud.gov/hudportal/HUD?src=/program_offices/fair_housing_equal_opp/FHLaws/yourrights [http://perma.cc/F8V9-DF9H] (last visited July 28, 2017) (noting the Fair Housing Act protects individuals from discrimination in housing on the basis of "race, color, national origin, religion, sex, disability, and the presence of children").

271. See supra section III.A. The Wisconsin statute states that no landlord may:

electing to discriminate explicitly based on traditionally prohibited reasons, such as race or sex, landlords could use PDE data insights to make rental decisions in new ways that are detrimental to specific groups or types of renters. As Professors Kate Crawford and Jason Schultz have noted, "correlative attributes" isolated by data analytics could be used as a "proxy for traits such as race or gender," and this could permit landlords and the companies that provide related services to more easily avoid accusations of overt discrimination.[272] Scholars have frequently highlighted the potential discriminatory impacts of "big data," but the quantity and variety of data are expected to increase exponentially with the expansion of the IOT, as previously noted. Therefore, any resulting discriminatory effects may become more prevalent in the IOT setting.

IV. EXISTING FRAMEWORKS AND RESPONSES

As discussed in Part III above, there are certain challenges and concerns associated with the use of PFP and PDE models. Existing regulatory frameworks and calls to reinstate the FCC Rules are unlikely to sufficiently meet these challenges for several reasons. First, litigation challenging the jurisdiction of a federal agency to regulate the activities of certain companies exposes issues associated with a sectoral approach to privacy. Second, in some instances the scope of existing and proposed regulation leaves segments of the consumer population unprotected or does not apply to all companies. Third, existing rules and proposals do not effectively recognize the limitations associated with relying on contractual consumer consent and notice and choice.

A. *FTC*

In *FTC v. AT&T* the Ninth Circuit held that common carriers were exempt from Section 5 liability under the Federal Trade Commission Act (FTCA).[273] The court reasoned that the common-carrier exemption

> [d]iscriminate in a manner described in [Wis. Stat. § 106.50] against a tenant or prospective tenant for exercising the right under subd. 1. to refuse to disclose access information for, grant access to, or allow observation of the personal Internet account of the tenant or prospective tenant, opposing a practice prohibited under subd. 1., filing a complaint or attempting to enforce any right under subd. 1., or testifying or assisting in any action or proceeding to enforce any right under subd. 1.

Wis. Stat. § 995.55(4)(a)(2) (2017).

272. Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 B.C. L. Rev. 93, 100 (2014). But see Tex. Dep't of Hous. & Cmty. Affairs v. Inclusive Cmtys. Project, Inc., 135 S. Ct. 2507, 2525 (2015) (addressing disparate impact and housing discrimination).

273. FTC v. AT&T Mobility LLC, 835 F.3d 993, 995 (9th Cir. 2016), reh'g en banc granted, 864 F.3d 995 (9th Cir. 2017). But see FTC v. Verity Int'l, Ltd., 443 F.3d 48, 60 (2d Cir. 2006) (finding "none of ACL's activities gave it the status of a common carrier subject

under the FTCA is a "status-based" rather than an "activity-based" exemption.[274] The FTC alleged that disclosures related to AT&T's "data throttling program" were inadequate.[275] This decision appears to limit the ability of the FTC to regulate common carriers who engage in "non-common-carrier activities" that are unfair and deceptive. The court's decision is troubling when one considers that various Internet companies could begin to perform common-carrier functions or activities to negatively impact the FTC's jurisdictional reach, and existing common carriers have acquired Internet companies that the FTC traditionally regulates.[276] The FTC petitioned for a rehearing en banc of the court's decision,[277] and the Ninth Circuit recently agreed to rehear the case.[278]

Regardless of the outcome of the rehearing, the case highlights the potential for jurisdictional gaps in existing regulatory frameworks.[279] One should not ignore the role that the American sectoral approach to privacy may play in contributing to these gaps. Under the sectoral approach, various laws and regulatory bodies govern "different industries."[280] If the

---

to the Communications Act of 1934, and accordingly, the FTC Act common-carrier exception would not apply"); FTC v. Am. eVoice, Ltd., No. CV 13-03-M-DLC, 2017 U.S. Dist. LEXIS 36388, at *12–13 (D. Mont. Mar. 14, 2017) (distinguishing *AT&T Mobility LLC* and finding that defendants were not common carriers); FTC v. Verity Int'l, Ltd., 194 F. Supp. 2d 270, 275 (S.D.N.Y. 2002) (finding that "whether an entity is a common carrier for regulatory purposes depends on the particular activity at issue" or, in other words, that "an entity may be a common carrier . . . for some purposes and not for others").

274. *AT&T Mobility LLC*, 835 F.3d at 999.

275. Id. at 995; see also Brief of the FCC as Amicus Curiae in Support of Plaintiff-Appellee at *4, FTC v. AT&T Mobility LLC, No. 15-16585 (9th Cir. filed May 30, 2017), 2017 WL 2398744 [hereinafter, FCC AT&T Brief] (stating that the FTC brought suit prior to the FCC's reclassification of broadband as a common carrier telecommunications service).

276. See Anthony Ha, Verizon Reportedly Closes In on a Yahoo Acquisition with a $250M Discount, TechCrunch (Feb. 15, 2017), http://techcrunch.com/2017/02/15/verizon-yahoo-250-million/ [http://perma.cc/4Z6Q-TVYM]; see also Brief of Amici Curiae Data Privacy and Security Law Professors in Support of FTC's Petition For Rehearing En Banc at 12–13, *AT&T Mobility LLC*, 864 F.3d 995 (9th Cir. 2017) (No. 15-16585) (discussing the impact of the court's decision and contending that under the court's rationale the FTC may no longer have jurisdiction over Yahoo if Verizon acquires Yahoo).

277. Petition of the FTC for Rehearing En Banc, *AT&T Mobility LLC*, 864 F.3d 995 (No. 15-16585).

278. *AT&T Mobility LLC*, 864 F.3d 995 (9th Cir. 2017) (order granting rehearing en banc).

279. FCC AT&T Brief, supra note 275, at 5 ("If the en banc Court were to adopt AT&T's position . . . the fact that AT&T provides traditional common-carrier voice telephone service could potentially immunize the company from any FTC oversight of its non-common-carrier offerings, even when the FCC lacks authority over those offerings . . . .").

280. See Woodrow Hartzog & Daniel J. Solove, The Scope and Potential of FTC Data Protection, 83 Geo. Wash. L. Rev. 2230, 2267 (2015) [hereinafter Hartzog & Solove, FTC Data Protection] (describing the role of the FTC in the regulation of privacy); see also What Information Do Data Brokers Have on Consumers, and How Do They Use It?: Hearing Before the S. Comm. on Commerce, Sci. & Transp., 113th Cong. 28 (2013) (explaining that the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Federal

jurisdiction of one agency is questioned, regulatory holes may result when the ability of other agencies to effectively regulate that space is undermined. The FCC has indicated that it intends to reverse the classification of "broadband as a common carrier service."[281] The FTC has called on Congress to amend the FTCA to remove the common-carrier exemption.[282]

Trade Commission Act, the Health Insurance Portability and Accountability Act of 1996, and the Children's Online Privacy Protection Act all regulate "the collection and use of consumer information").

281. Restoring Internet Freedom, 82 Fed. Reg. 25,568, 25,570 (proposed June 2, 2017) (to be codified at 47 C.F.R. pts. 8, 20) (proposing to "reinstate the information service classification of broadband Internet access service and return to the light-touch regulatory framework first established on a bipartisan basis during the Clinton Administration"); Jenna Ebersole, FCC's Net Neutrality Plan Sets Up Repeal Without Replace, Law360 (Apr. 28, 2017), http://www.law360.com/articles/918488/fcc-s-net-neutrality-plan-sets-up-repeal-without-replace [http://perma.cc/8BAM-RZ92]. But see Press Release, FCC, FTC, Joint Statement of FCC Commissioner Mignon Clyburn and FTC Commissioner Terrell McSweeny on Leaving Broadband Consumers and Competition Unprotected (Apr. 27, 2017) [hereinafter McSweeny & Clyburn Joint Statement], http://apps.fcc.gov/edocs_public/attachmatch/DOC-344627A1.pdf (on file with the *Columbia Law Review*) (critiquing the proposal to dismantle the Open Internet Order and suggesting that doing so "would also create an environment where neither the FCC nor FTC could protect the privacy of the customers of some of our largest broadband companies"). The FCC contends that its proposal to reclassify broadband as a "non–common carrier 'information service,'" even if adopted, may not sufficiently address the issues posed in *AT&T Mobility* because "in addition to the broadband services at issue in the FCC's proceeding, AT&T also provides traditional wireline and wireless voice telephone service, which are (and always have been) Title II common-carrier services." FCC AT&T Brief, supra note 275, at 4–5; see also U.S. Telecom Ass'n v. FCC, 855 F.3d 381, 382 (D.C. Cir. 2017) (per curiam) (denying en banc review of a decision upholding the FCC's Open Internet Order in light of the FCC's notice of proposed rulemaking that would "dismantle or reduce the Open Internet Order rules"); id. (Srinivasan, J., concurring) (noting, with the other concurring judges, that the denial was made).

282. Ohlhausen Remarks, supra note 171, at 7 (calling on Congress to amend the FTCA to remove the common carrier exemption because the "current exemption no longer makes sense in today's environment where the lines between telecommunications and other services are increasingly becoming blurred"); see also H.R. 2520, 115th Cong. (2017) (proposing to grant the FTC the power to regulate broadband providers and require opt-in approval for sensitive information and opt-out approval for non-sensitive information). The bill is similar to the repealed FCC Rules in that it would prohibit providers from terminating services if a user fails to "waive privacy rights guaranteed by law." Id. § 4; see also Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274, (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64), repealed by Act of Apr. 3, 2017, Pub. L. No. 115-22, 131 Stat. 88 (codifying a joint resolution disapproving of the FCC "Broadband and Telecommunications Services" privacy rules). But see Jenna Ebersole, GOP Plan Revives, Expands Part of Nixed FCC Privacy Rules, Law360 (June 1, 2017), http://www.law360.com/articles/930296/gop-plan-revives-expands-part-of-nixed-fcc-privacy-rules [http://perma.cc/78MH-YWTZ] (contending that the bill "would have the FTC use the FCC's opt-in approach to consumer consent, and it would also extend the rules beyond ISPs to content companies—so-called edge providers like Google and Facebook").

As to data brokers, the FTC has encouraged Congress to adopt legislation to "make data broker practices more visible to consumers and to give consumers greater control over the immense amounts of personal information about them collected and shared by data brokers."[283] Companies that adopt PFP or PDE models but do not qualify as common carriers—or otherwise fall into one of the exemptions under the FTCA—are likely subject to FTC supervision.[284]

Professors Solove and Schwartz contend that "[t]he FTC lacks practical rulemaking authority."[285] The FTC's self-regulatory method of evaluating privacy- and security-related matters under the FTCA has been

---

283. Press Release, FTC, FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control over Their Personal Information (May 27, 2014), http://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more [http://perma.cc/CM7V-LA5L]; see also FTC, Protecting Consumer Privacy in an Era of Rapid Change 11–12 (2012) [hereinafter FTC Rapid Change Report], http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [http://perma.cc/H68N-BEK4] (discussing data brokers and acknowledging that "self-regulation has not gone far enough").

284. Meeco, Digi.me, Cozy, and Beagli appear to be foreign rather than domestic entities. MEF White Paper, supra note 23. The FTC has pursued foreign companies for FTCA violations. See, e.g., ASUTeK Comput., Inc., FTC File No. 142 3156, No. C-4587, at 1–2 (F.T.C. July 28, 2016), http://www.ftc.gov/system/files/documents/cases/1607asustekdo.pdf [http://perma.cc/75BR-SVXU] (deciding an action against a Taiwan-based company); Andrew F. Popper, In Personam and Beyond the Grasp: In Search of Jurisdiction and Accountability for Foreign Defendants, 63 Cath. U. L. Rev. 155, 188–89 (2013) (suggesting that Section 5 of the FTCA gives the FTC the ability to pursue both domestic and foreign entities and "the enforcement power of the FTC extends beyond domestic borders if the foreign action 'ha[s] a direct, substantial, and reasonably foreseeable effect' on U.S. markets" (alteration in original) (quoting 15 U.S.C. § 45(a)(3)(A) (2012))); Letter from Edith Ramirez, Chairwoman, FTC, to Johann N. Schneider-Ammann, Head of the Dep't of Econ. Affairs, Educ. & Research, Swiss Fed. Council 3 (Jan. 9, 2017), http://www.ftc.gov/system/files/documents/public_statements/1049563/ramirez_swiss_privacy_shield_letter.pdf [http://perma.cc/FP52-VBS6] ("[FTC] enforcement actions . . . have a global impact. The FTC Act's prohibition on unfair or deceptive acts or practices . . . includes those practices that (1) cause or are likely to cause reasonably foreseeable injury in the United States, or (2) involve material conduct in the United States."); A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, FTC, http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [http://perma.cc/H3MW-CCGJ] (last visited July 28, 2017) (explaining that under Section 5(a) of the FTC Act, the FTC's jurisdiction includes "acts or practices involving foreign commerce that cause or are likely to cause reasonably foreseeable injury within the United States or involve material conduct occurring within the United States").

285. Solove & Schwartz, Consumer Privacy, supra note 253, at 161; see also Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 334 ("[T]he Magnuson-Moss Warranty Act stripped the FTC of ordinary rule-making procedures, putting in its place a system for promulgating rules that is unwieldy and time consuming."); Justin (Gus) Hurwitz, Data Security and the FTC's UnCommon Law, 101 Iowa L. Rev. 955, 964 (2016) (contending that legislation has "imposed heightened procedural requirements on the Commission's unfairness-related rulemaking and prohibited the Commission from regulating certain industries").

described as "too measured and conservative."[286] The FTCA prohibits "unfair or deceptive acts or practices in or affecting commerce."[287] According to a policy statement issued by the FTC, the following elements are central to deception cases: (a) the existence of "a representation, omission, or practice that is likely to mislead consumers;" (b) the materiality of the activity (whether it is "likely to affect the consumer's conduct or decision with regard to a product or service"); and (c) the point of view of a reasonable consumer or the group impacted by the activity.[288] Deception cases include "broken promises of privacy and data security, deceptive actions to induce the disclosure of information and failure to give sufficient notice of privacy invasive practices."[289] In determining whether a practice is deceptive, the FTC considers the extent to which representations are clear and unambiguous, the importance of any absent information, as well as the conspicuousness of "qualifying information."[290] This approach relies excessively on a notice-and-choice model and promises made by companies regarding privacy and security. As a result, it may not consistently protect the interests of consumers.[291]

The FTC has broad unfairness authority.[292] Professors Daniel Solove and Woodrow Hartzog have identified five theories of unfair practices

---

286. Hartzog & Solove, FTC Data Protection, supra note 280, at 2234.

287. 15 U.S.C. § 45(a)(1).

288. Letter from James C. Miller III, Chairman, FTC, to John D. Dingell, Chairman, House Comm. on Energy & Commerce (Oct. 14, 1983) [hereinafter FTC Policy Statement on Deception], http://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf [http://perma.cc/G4BF-4CEX]; see also Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 123 (contending that "[a]t any time, the Commission could abandon the Deception Statement formally as it is a self-imposed and voluntary restriction on the FTC's powers").

289. Hartzog & Solove, FTC Data Protection, supra note 280, at 2234.

290. FTC Policy Statement on Deception, supra note 288; see also Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 125.

291. See Elvy, Commodifying Consumer Data, supra note 11, at 51–53; see also Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583, 628 (2014) [hereinafter Solove & Hartzog, New Common Law] (contending that although "[m]uch of the FTC's privacy jurisprudence is based upon a deception theory of broken promises," the FTC now "considers the entirety of a company's dealings with the consumer, not just the specific promises made in the company's privacy policy").

292. Hartzog & Solove, FTC Data Protection, supra note 280, at 2247 ("The FTC's unfairness authority is . . . comprehensive [and] . . . the FTC can find a practice unfair even when it is otherwise legally permissible."); see also Letter from Michael Pertschuk, Chairman, FTC, et al., to Wendell H. Ford, Chairman, Senate Consumer Subcomm. on Commerce, Sci. & Transp., and John C. Danforth, Ranking Minority Member, Senate Consumer Subcomm. on Commerce, Sci. & Transp. (Dec. 17, 1980) [hereinafter FTC Policy Statement on Unfairness], http://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [http://perma.cc/79E2-KEY9] (identifying "three factors" to evaluate whether a practice is unfair: "(1) whether the practice injures consumers, (2) whether it violates established public policy, and (3) whether the conduct is unethical or unscrupulous").

that may be subject to FTC scrutiny: "(1) retroactive policy changes, (2) deceitful data collection, (3) improper use of data, (4) unfair design, and (5) unfair information security practices."[293] The FTC's policy statement on unfair practices suggests that the extent to which a practice violates recognized public policy, is "unethical or unscrupulous," as well as whether consumers suffer substantial injury that is not "outweighed by any offsetting consumer or competitive benefits" and "which consumers could not reasonably have avoided" are all relevant in assessing the unfairness of a practice.[294]

To the extent that consumers consent to the terms of PFP or PDE products or plans that businesses offer and the company provides adequate notice of its terms (during its course of dealing with consumers, including in its privacy policies, user-interface, email communications, and other materials), keeps its implicit and express promises, makes no material omissions, uses data in compliance with its promises, and does not otherwise engage in deceptive or deceitful practices, there may be no grounds for FTC intervention in the absence of lax or non-existent data security practices. Of course, if a PDE company made explicit or implied statements promising not to track consumers or view social media account information and the company violated those promises, this activity may be viewed as deceptive. Similarly, if the design or default settings of PDE companies do not provide consumers with sufficient control over their data as promised or sufficient notice regarding data sharing and collection practices, such actions may be viewed as unfair or deceptive. The FTC has also attempted to protect certain vulnerable consumers, such as the elderly.[295]

While protecting consumers from unfair and deceptive practices is an important regulatory goal, issues related to unequal access to privacy and its negative impact on low-income consumers may not fit neatly into current theories "of what constitutes an unfair [or deceptive] trade practice."[296] For instance, claims related to broken promises, retroactive changes to privacy policies, or settings that were implemented without providing notice and obtaining consent or claims related to a failure to implement reasonable security procedures do not completely address

---

293. Solove & Hartzog, New Common Law, supra note 291, at 640; see also 15 U.S.C. § 45(n) (2012) (delineating the FTC's authority to declare acts or practices unlawful on the grounds that "such act or practice is unfair"); Solove & Schwartz, Privacy Law Fundamentals, supra note 198, at 165 (contending that the following "privacy practices will trigger FTC complaints (1) inadequate security, (2) security gaffes and failure to train, (3) broken promises, (4) retroactive privacy policy changes, (5) deceptive data collection and (6) inadequate disclosure of extent of data gathering").

294. FTC Policy Statement on Unfairness, supra note 292; see also Solove & Hartzog, New Common Law, supra note 291, at 639. Professor Hoofnagle suggests that whether an activity violates public policy cannot "independently support a claim of unfairness." Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 131.

295. Hartzog & Solove, FTC Data Protection, supra note 280, at 2282.

296. Solove & Hartzog, New Common Law, supra note 291, at 640.

one of the main concerns associated with unequal access to privacy: that certain consumers by the nature of their social and economic circumstances are less likely to receive the same level of privacy as other consumers. This likely remains true even if companies provide low-income consumers with notice and choice not only via a company's privacy policy but also in other communications with the company, such as website design or icons.

Concerns about unequal access to privacy could be viewed as abstract and "speculative" rather than "substantial," or alternatively, the benefits that PDE and PFP companies and their products provide to "consumers or competition" could outweigh the harms of unequal access to privacy.[297] One could also contend that issues associated with unequal access to privacy are not the primary concern or objective of the FTC. The FTC has stated that "[a]n injury may be sufficiently substantial . . . if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm."[298] One could contend that unequal access to privacy is a significant societal harm that could impact large numbers of consumers and that societal harm should constitute a substantial injury for purposes of evaluating whether a practice is unfair.[299] However, one may also posit that low-income consumers could avoid harms associated with PDE and PFP offerings simply by electing not to participate in PDE marketplaces and PFP discount programs or choosing not to use the services and products PFP luxury companies provide.[300] Thus, it is not entirely clear whether concerns about unequal access to privacy and subsequent monetization by companies, discussed in Part III, will be consistently and effectively addressed.

Finally, one may argue that the conduct of low-income consumers who are not specifically targeted by a practice—and who nevertheless elect to engage in the PDE marketplace without first acquiring sufficient knowledge of the implications of directly trading data—is "arguably not reasonable," which may impact the extent to which a practice is viewed as deceptive.[301] As Professor Hoofnagle notes, however, "unreasonable

---

297. Id. at 639 ("In evaluating whether a trade practice is unfair, the FTC focuses largely on substantial injury to consumers. Monetary, health, and safety risks are common injuries considered 'substantial' but trivial, speculative, emotional and other 'more subjective harm' are usually not considered substantial for unfairness purposes." (quoting FTC Policy Statement on Unfairness, supra note 292)).

298. FTC Policy Statement on Unfairness, supra note 292, at n.12.

299. Hartzog & Solove, FTC Data Protection, supra note 280, at 2283 ("In determining whether an injury is outweighed by any countervailing benefits to consumers or competition, the FTC considers not only the consumer's cost to remedy the alleged injury, but also the cost to society in general.").

300. See Solove & Hartzog, New Common Law, supra note 291, at 639 ("If consumers could have reasonably avoided the alleged injury, the FTC will not consider a trade practice unfair.").

301. Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 128.

consumers are likely to be the most in need of protection."[302] Further, in light of evidence that suggests that companies can significantly impact the privacy expectations of consumers,[303] even a strong focus on the reasonable expectations of consumers may not be sufficient to protect consumer privacy.

B. *Children's Online Privacy Protection Act*

COPPA governs websites and online services, including mobile applications, that obtain personal information, such as voice and geolocation data, from children under the age of thirteen.[304] The operator of the online service or website must direct its website or services to children or have "actual knowledge" that it is obtaining information from a user under the age of thirteen.[305] The FTC has recently announced that businesses that offer child IOT devices, such as connected toys, are subject to COPPA.[306] IOT data and social media information may qualify as personal information.[307] Companies subject to COPPA must provide adequate notice about their data collection practices, among other things.[308] Businesses are required to provide direct notices to parents and post policies on their websites describing the types of information that the company collects from children and how the company will use and

---

302. Id.

303. Kim & Telman, supra note 180, at 736 (discussing techniques by large Internet giants to shape consumer actions and perceptions); see also Jim Hawkins, Exploiting Advertising, 80 Law & Contemp. Probs., no. 3, 2017, at 43, 43–45 (describing behavioral advertisement and its impact on consumers).

304. 15 U.S.C. § 6502(a)(1) (2012); 16 C.F.R. § 312.12 (2012) (defining child, Internet, personal information, and "[w]eb site or online service directed to children" under COPPA). Additionally, "the collection of personal information under COPPA also includes passive tracking of a child online." 16 C.F.R. § 312.2; see also, Solove & Schwartz, Consumer Privacy, supra note 253, at 202.

305. 15 U.S.C. § 6502(a)(1); Solove & Schwartz, Consumer Privacy, supra note 253, at 204 (contending that "COPPA only applies when a website has actual knowledge that a user is under [thirteen] or operates a website specifically targeted to children"); Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 200 ("To trigger the COPPA obligations, a website or service must be directed at children, or have actual knowledge that it has collected information from children.").

306. Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business, FTC, http://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance [http://perma.cc/M8X8-HQ45] (last visited July 28, 2017); see also Behnam Dayanim & Mary-Elizabeth Hadley, After FTC's Update, A Refresher on Complying with COPPA, Law360 (June 26, 2017), http://www.law360.com/articles/937897/after-ftc-s-update-a-refresher-on-complying-with-coppa [http://perma.cc/8V6B-4XXU] (noting that the FTC's 2017 updated six-step compliance plan for businesses to comply with COPPA "makes clear that companies providing 'connected toys or other internet of things (IoT) devices' are covered by COPPA").

307. 16 C.F.R. § 312.2.

308. 16 C.F.R. § 312.4; Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 203.

disclose the information.[309] Companies should obtain "verifiable parental consent" to collect, use, or disclose the data of children.[310]

COPPA has several limitations. First, data collected from minors over the age of thirteen are arguably not subject to the statute.[311] Professor Anupam Chander contends that "COPPA was designed [in part] to protect children from prying adults, but not from themselves . . . [and the statute's age restriction] leaves youth precisely when they enter that time in their lives where they need it most."[312] If companies using PFP or PDE models obtain data from children over the age of thirteen, the statute's protections are likely not applicable.

Second, the statute likely does not apply to data adults supply about children, as its coverage is limited to information supplied directly by children.[313] Thus, to the extent that a parent submits child-related data for the purpose of participating in a PDE monetization program as discussed in section III.A above, COPPA's protections may not be applicable. Third, COPPA also relies on notice and parental consent to justify data-collection practices.[314] Consumers frequently do not read or understand

309. See 15 U.S.C. § 6502(b)(1)(A)(i) (requiring notice on website); 16 C.F.R. §§ 312.4(b)–(c) (providing rules for direct parental notice); 16 C.F.R. § 312.4(d) (providing rules for posting website or service notices); Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 203 ("COPPA's notice requirements include a duty to provide a general privacy notice as well as special, direct notices to parents before the service collects information from children.").

310. 15 U.S.C. § 6502(b)(1)(A)(ii); 16 C.F.R. § 312.5 (discussing parental consent and exceptions); see also Children's Online Privacy Protection Rule, 16 C.F.R. § 312.8 (2013) (noting that operators "must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children").

311. In contrast, a related California statute that applies to minors is not limited to children under thirteen. Cal. Bus. & Prof. Code § 22580(d) (2015); see also 1 Raymond T. Nimmer & Holly K. Towle, Data Privacy, Protection, and Security Law § 2.08(10)(a)(i), LexisNexis (2017) (stating that the California "statute concerns 'minors' as opposed to the COPPA subset of children under the age of 13 [and] [u]nder the CA statute, a minor is a natural person under 18 years who resides in CA"). Previous attempts to expand COPPA's coverage have stalled. See Summary: H.R. 2734—114th Congress (2015-2016), Congress.gov, http://www.congress.gov/bill/114th-congress/house-bill/2734 [http://perma.cc/Y4LU-5QKK] (last visited July 28, 2017) (indicating the last action on the bill occurred on June 12, 2015); see also 114 Legislative Outlook H.R. 2734, LexisNexis (database updated 2017) (available in full on LexisAdvance and on file with the *Columbia Law Review*) (indicating the bill failed).

312. Anupam Chander, Youthful Indiscretion in an Internet Age, *in* The Offensive Internet 124, 128 (Saul Levmore & Martha C. Nussbaum eds., 2010).

313. Solove & Schwartz, Consumer Privacy, supra note 253, at 203; Complying with COPPA: Frequently Asked Questions, FTC, http://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions [http://perma.cc/RT2T-PKHS] [hereinafter FTC, Complying with COPPA] (last updated Mar. 20, 2015) ("Does COPPA apply to information *about* children collected online from parents or other adults? No. COPPA only applies to personal information collected online from children, including personal information about themselves, their parents, friends, or other persons.").

314. Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 202–08 (discussing COPPA's notice-and-choice framework). The FTC's enforcement of COPPA has also been

privacy policies, and this practice may continue even though parental consent is received.[315] Lastly, as Professor Angela Campbell has noted, in many instances it is unclear whether a company's website or service targets children and the "multifactor test employed by the FTC leaves room for subjective interpretation."[316] Since the COPPA rule "does not require operators of general audience sites to investigate the ages of visitors to their sites or services," complications may arise when attempting to determine whether an operator of a website or service has "actual knowledge" that children are using their service.[317]

C. *Proposals to Restore the FCC Rules*

As of the date of writing, members of Congress opposed to the repeal of the FCC Rules have proposed various legislation to restore the rules.[318] The recently repealed FCC Rules required BIAS companies that offer "financial incentives," such as discounts, "in exchange for a customer's approval to use, disclose, and/or permit access to the customer's

---

criticized. See generally Angela J. Campbell, Rethinking Children's Advertising Policies for the Digital Age, 29 Loy. Consumer L. Rev. 1, 21–35 (2016).

315. Under the COPPA framework, the mechanism used to obtain parental consent should be "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent." 16 C.F.R. § 312.5(b); see also Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 203–04 (discussing various ways to obtain parental consent).

316. Campbell, supra note 314, at 27.

317. Id. (contending that children may be untruthful about their birthdates and "the FTC does not require operators to investigate the ages of their users"); FTC, Complying with COPPA, supra note 313.

318. Restoring American Privacy Act of 2017, H.R. 1868, 115th Cong. § 2 (2017) ("Notwithstanding any other provision of law [BIAS providers] shall be subject to . . . the [FCC] Report and Order in the matter of protecting the privacy of customers of broadband and other telecommunications services that was adopted by the Federal Communications Commission on October 27, 2016 (FCC 16–148) . . . ."); see also S. 878, 115th Cong. (2017) (proposing to direct the FCC to adopt regulation similar to the recently repealed FCC Rules); Press Release, Senator Ed Markey, Senator Markey Leads Senators in Legislation to Fully Restore Broadband Privacy Protections (Apr. 6, 2017), http://www.markey.senate.gov/news/press-releases/senator-markey-leads-senators-in-legislation-to-fully-restore-broadband-privacy-protections [http://perma.cc/GG3E-35YC] ("The [proposed] legislation reinstates the Federal Communications Commission (FCC) rules which require internet service providers to obtain consent before sharing their subscribers' sensitive information and adopt reasonable data security protections."); Press Release, Congresswoman Jackie Rosen, Rosen Introduces Bill to Restore Americans' Internet Privacy Protections (Apr. 4, 2017), http://rosen.house.gov/media/press-releases/rosen-introduces-bill-restore-americans-internet-privacy-protections [http://perma.cc/5FTV-2FMQ] ("H.R. 1868, the Restoring American Privacy Act of 2017, . . . will reverse the Congressional resolution signed by President Trump allowing internet providers to sell their customers' personal information without their knowledge or consent."). The S. 878 bill would authorize the FCC to adopt rules to prohibit a "telecommunications carrier from refusing to serve a customer who doesn't consent to the use and sharing of his or her customer proprietary information for commercial purposes (commonly known as 'take-it-or-leave-it offers')." S. 878 § 1(3)(e).

proprietary information" to provide information about the terms of the PFP discount plan to consumers using clear, noticeable, understandable, and non-deceptive language.[319] The FCC Rules would have required BIAS providers to explain what information the BIAS companies will collect, how they will use and share that information, and "that the program requires opt-in approval."[320] In addition, BIAS providers would have needed to provide consumers with information about equivalent non-PFP discount plans as well as the ability to withdraw from the plan.[321]

In the wake of the recent repeal of the FCC Rules, some ISPs have attempted to reassure consumers by suggesting that "they do not and will not sell customers' sensitive web browsing history to third parties without consumers' knowledge or consent."[322] Other providers have expressly noted that they do not sell consumer "web browsing history" but have also indicated that they may use aggregated and de-identified information for targeted advertising.[323] One ISP drew the attention of the FCC after using behavior-tracking mechanisms to monitor consumers' online activities without sufficiently informing consumers and allowing opt outs.[324]

---

319. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64), repealed by Act of Apr. 3, 2017, Pub. L. No. 115-22, 131 Stat. 88 (codifying a joint resolution disapproving of the FCC "Broadband and Telecommunications Services" privacy rules). The term "customer proprietary information" means "information that BIAS providers and other telecommunications carriers acquire in connection with their provision of service, which customers have an interest in protecting from disclosure." Id. at 87,824.

320. Id. at 87,346.

321. Id.

322. Suevon Lee, Senate Dems Float Bill to Revive Nixed FCC Privacy Rules, Law360 (Apr. 7, 2017), http://www.law360.com/articles/911118/senate-dems-float-bill-to-revive-nixed-fcc-privacy-rules (on file with the *Columbia Law Review*); see also Gerard Lewis, Our Commitment to Consumer Privacy, Comcast: Consumer Voices (Mar. 31, 2017), http://corporate.comcast.com/comcast-voices/our-commitment-to-consumer-privacy [http://perma.cc/N4D3-GBBJ] (explaining that Comcast has never sold its customers' web-browsing history and does not intend to do so); Bob Quinn, Reversing Obama's FCC Regulations, AT&T Pub. Pol'y (Mar. 31, 2017), http://www.attpublicpolicy.com/privacy/reversing-obamas-fcc-regulations-a-path-to-consumer-friendly-privacy-protections/ [http://perma.cc/4A2D-QMVK] (explaining that the company is still subject to section 222 of the Communications Act, even though Congress eliminated the FCC privacy rules).

323. See, e.g., Karen Zacharia, Verizon Is Committed to Your Privacy, Verizon (Mar. 31, 2017), http://www.verizon.com/about/news/verizon-committed-your-privacy [http://perma.cc/QTR5-QA84] (explaining Verizon does not sell the web-browsing data of its customers but does provide optional services that use aggregated and de-identified customer information for personalized or targeted advertising).

324. Karl Bode, Verizon May Soon Get to Enjoy a Lawsuit Over Its Sneaky Use of Perma-Cookies, Techdirt (Nov. 7, 2014), http://www.techdirt.com/articles/20141105/11315029057/verizon-may-soon-get-to-enjoy-lawsuit-over-their-sneaky-use-perma-cookies.shtml [http://perma.cc/THP2-PZDR] (describing the Verizon Select and Relevant Mobile Ad system as well as Verizon's use of stealth cookies that covertly track user activities "without users being able to disable them via browser settings"); see also Karl Bode, Two and a Half Years Later, Verizon Finally Lets People Opt Out of Its Stealth Zombie Cookie, Techdirt (Apr. 6, 2015), http://www.techdirt.com/articles/20150402/06110930520/t%20.%20.%20.%20later-

User data obtained through these methods could ultimately be processed, disclosed and transferred to third parties.[325]

Critics of the FCC Rules argued that consumers would pay higher broadband prices if the rules were implemented and that the opt-in provisions of the FCC Rules "would stop the modern digital economy in its tracks and transform many 'free' Internet services into smaller, subscription-based enterprises."[326] Opponents also criticized the rules for their supposed potential to "undermin[e] protection for sensitive data and chill[] innovative uses for nonsensitive data."[327]

Despite criticisms from the common-carrier industry, some provisions of the FCC Rules would certainly benefit consumers, such as the prohibition on "take-it-or-leave-it offers" that are "contingent on surrendering privacy rights."[328] However, restoring the FCC Rules without considering their shortcomings is problematic. First, the FCC Rules would not have applied to all companies implementing PFP discount programs, such as mobile applications or websites governed by the FTC.[329] Thus, the rules had a limited reach. This is likely due to the limited jurisdiction of the FCC.

---

verizon-finally-lets-people-opt-out-stealth-zombie-cookie.shtml [http://perma.cc/B2CP-66VG] (noting after public outcry Verizon now allows consumers to opt out of its stealth tracking); Press Release, FCC, FCC Settles Verizon Supercookie Probe, Requires Consumer Opt-In for Third Parties (Mar. 7, 2016) (on file with the *Columbia Law Review*) (discussing Verizon's settlement with FCC over "supercookies").

325. See Finley, VPNs Won't Save You, supra note 241; Stephens, supra note 265.

326. Petition for Reconsideration, supra note 169, at 7; see also O'Rielly Dissenting Statement, supra note 169 ("Heightening the limitations on the use of information, as contemplated by [the FCC Rules], will impact every other pricing component of Internet access and eventually edge providers.").

327. Michael Macagnone, FTC Commissioner Continues Attack on FCC Data Rules, Law360 (June 28, 2016), http://www.law360.com/articles/811995/ftc-commissioner-continues-attack-on-fcc-data-rules [http://perma.cc/QCC5-7NR2]; see also Jenna Ebersole, FCC's Halt Of Privacy Rule Signals Net Neutrality Reversal, Law 360 (Mar. 2, 2017), http://www.law360.com/articles/897486/fcc-s-halt-of-privacy-rule-signals-net-neutrality-reversal [http://perma.cc/HH37-B76U] [hereinafter Ebersole, FCC's Halt of Privacy Rules] (suggesting that under the Obama Administration the FTC and the FCC "'appeared to have a more adversarial relationship' on questions of jurisdiction"). See generally FTC, Internet of Things: Privacy and Security in a Connected World 18 (2015), http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [http://perma.cc/2A6P-G7YH] ("[P]erceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption.").

328. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274, 87,276 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64), repealed by Act of Apr. 3, 2017, Pub. L. No. 115-22, 131 Stat. 88 (codifying a joint resolution disapproving of the FCC "Broadband and Telecommunications Services" privacy rules).

329. FCC Fact Sheet, supra note 19, at 4 (stating the FCC Privacy Rules "[d]o not regulate the privacy practices of websites or apps, like Twitter or Facebook, over which the Federal Trade Commission has authority").

Second, proposals to restore the FCC Rules must adequately address PFP discount plans.[330] The FCC Rules did not prohibit PFP discount plans but rather relied on a notice-and-choice model and required opt-in consumer consent as noted above.[331] Under the rules, notices about PFP discount plans would have been provided separately from a company's privacy policy, and the FCC indicated that it would assess the validity of such programs on a "case-by-case basis."[332] Opt-in consent is likely better than opt-out consent, since consumers may be unaware of how to opt out of data collection and the implications of their failure to opt out of such programs. It may also be time-consuming for consumers to locate opt-out mechanisms on a company's website.

The FCC has previously indicated that the goal of imposing "heightened disclosure and consent requirements" for PFP plans offered by BIAS providers was to ensure that consumers' decisions about such plans "are based on informed consent."[333] Research has challenged the notion of informed consent in the consumer context, and various theories have been offered to explain the failure of consumers to review form contracts.[334] This may hold true even when opt-in consent is required. Research on consumers' understanding of privacy policies has also consistently found that a significant number of consumers do not under-

330. The Restoring American Privacy Act of 2017 would restore the FCC Rules as is. See Restoring American Privacy Act of 2017, H.R. 1868, 115th Cong. § 2 (2017). The S. 878 bill does not clearly address PFP discount programs, and a grant of authority to the FCC to reinstate the repealed FCC Rules could possibly lead to the adoption of similar rules that would have been applicable to PFP discount programs. S. 878, 115th Cong. (2017).

331. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. at 87,275.

332. Id. at 87,346; see also id. at 87,317 ("Mindful of the potential benefits and harms associated with financial incentive practices, we adopt heightened disclosure and choice requirements [and] . . . BIAS providers must make financial incentive notices easily accessible and separate from any other privacy notifications . . . .").

333. Id. at 87,317 ("We therefore find that that heightened disclosure and affirmative customer consent requirements will help to ensure that customers' decisions to share their proprietary information in exchange for financial incentives are based on informed consent.").

334. See Florencia Marotta-Wurgler, Does Contract Disclosure Matter?, 168 J. Institutional & Theoretical Econ. 94, 110 (2012) (discussing a study of "the twenty-five most trafficked sites likely to have information about [end-user license agreement] terms . . . [which found] that shoppers accessed EULA information in consumer review sites in only three out of 148,552 sessions with at least two pages accessed"); see also Wayne R. Barnes, Toward a Fairer Model of Consumer Assent to Standard Form Contracts: In Defense of Restatement Subsection 211(3), 82 Wash. L. Rev. 227, 257–58 (2007) ("[P]eople evaluate data based on factors immediately available to them, often giving disproportionate value to such factors . . . [and] make erroneous decisions based on statistically unsound samplings of data they nevertheless judge to be sufficiently representative."). Professor Wayne Barnes further explains that individuals may also "value present and immediate benefits and expenditures disproportionately more than they value benefits or expenditures which may occur in the future . . . [while] systematically underestimating the risks that they undertake." Id. at 258.

stand the meaning of the term "privacy policy," and many mistakenly believe that the existence of a privacy policy means that their data will not be disclosed or shared with third parties.[335] One study found that "if all American Internet users were to annually read the online privacy policies word-for-word each time they visited a new site, the nation would spend about 54 billion hours reading privacy policies . . . [and] lose the value of about $781 billion from the opportunity cost value of the time."[336] Consumers may want more privacy and control over their data as noted in Part I, but they may not know how to achieve this result, and many unwittingly consent to data collection practices that undermine these goals. A recent empirical study of privacy policies found that the "average policy complies with only 39% of the FTC guidelines,"[337] and "most firms do not follow FTC recommendations to adopt short, streamlined, and standardized privacy policies."[338]

Consumers are already overwhelmed with the wealth of disclosures that they must review when they engage in daily transactions. In a single transaction, companies provide consumers with separate privacy policies, terms and conditions, end-user license agreements, and warranty information for their products.[339] Imposing an additional disclosure requirement that consumers must attempt to read and understand before opting in is unlikely to sufficiently protect consumers. The imposition of a clear and conspicuous language requirement would likely not have

335. Pew Research Ctr., What Internet Users Know About Technology and the Web 7 (2014), http://www.pewinternet.org/files/2014/11/PI_Web-IQ_112514_PDF.pdf [http://perma.cc/2LGY-B83L] (finding that fifty-two percent of survey respondents incorrectly believed that "when a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users"); Joseph Turow, Lauren Feldman & Kimberly Meltzer, Annenberg Pub. Policy Ctr. of the Univ. of Pa., Open to Exploitation: American Shoppers Online and Offline 20 (2005) (unpublished working paper), http://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers [http://perma.cc/9JUF-ZYWH] (finding that fifty-nine percent of survey respondents said the statement "[w]hen a web site has a privacy policy, I know that the site will not share my information with other websites or companies" was true).

336. Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J.L. & Pol'y for the Info. Soc. 543, 563–64 (2008); see also MEF 2017 Consumer Report, supra note 63, at 19 (noting that only thirty-four percent of surveyed consumers in ten countries indicated that they "always read" a company's "privacy policy or terms and conditions first"); Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts, 43 J. Legal Stud. 1, 6 (2014) (discussing theories arguing that not reading form contracts may be rational); Ben-Shahar & Chilton, supra note 179, at S42 (contending that "the average person encounters so many privacy disclosures every year . . . that it would take 76 days to read them").

337. Florencia Marotta-Wurgler, Understanding Privacy Policies: Content, Self-Regulation and Markets 1 (N.Y. Univ. Law & Econ. Working Paper No. 435, 2016), http://lsr.nellco.org/cgi/viewcontent.cgi?article=1439&context=nyu_lewp [http://perma.cc/XH5H-96CZ].

338. Id. at 4.

339. Elvy, Hybrid Transactions, supra note 67, at 95–96.

adequately alleviated this concern. As to the issue of subsequent monetization, if the company's PFP discount notice complied with the FCC Rules, and a consumer consented, the company would likely have been free under the FCC Rules to monetize the data in whatever manner it chose, including potentially disclosing the data to data brokers.[340]

V. THE PATH FORWARD

Given the limitations of existing legal frameworks in remedying the concerns associated with the rise of PFP and PDE models, discourse about various approaches to regulating these nascent business programs is necessary. This Part offers five potential points to consider with the goal of alleviating or preventing the concerns and inadequacies discussed in Parts III and IV. First, PDE companies must consistently implement measures to ensure that consumers have sufficient control over their data, acknowledge the limitations of the notice-and-choice model, and address issues that contributed to the failure of earlier generations of infomediaries. In addition, cooperation by non-PDE companies may be necessary in order for PDE companies to significantly change the data industry. Second, in industries that provide necessities in the digital age, PFP discount programs could be prohibited. Third, as the primary regulator of data-security and privacy issues, the FTC's approach in this area must consider (and address when possible) the concerns highlighted in this Article. Ambiguities in the FTC's jurisdiction and potential jurisdictional gaps must be resolved, and existing regulation that may be beneficial to consumers should not be dismantled. Increased regulation of the activities of data brokers is long overdue, and there should be rigorous oversight of PDE markets. Fourth, it may be necessary to impose restrictions on the monetization of certain types of data, including data that children or renters generate. Fifth, guidance on the best ways to structure PDE arrangements to protect consumers is necessary.

A. *The Promise of the PDE*

PDE companies are attempting to provide consumers with more control over their data, which is a laudable endeavor. However, to effectuate a comprehensive change in the structure of the existing industry,

340. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274, 87,344 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64) (prescribing that "a telecommunications carrier may not use, disclose, or permit access to customer proprietary information except with the opt-out or opt-in approval of a customer"), repealed by Act of Apr. 3, 2017, Pub. L. No. 115-22, 131 Stat. 88 (codifying a joint resolution disapproving of the FCC "Broadband and Telecommunications Services" privacy rules); see also id. at 87,346 ("A BIAS provider that offers a financial incentive . . . must do all of the following: . . . Obtain customer opt-in approval in accordance with § 64.2004(c) for participation in any financial incentive program.").

PDE companies must overcome several challenges. Data brokers and established companies can obtain consumer information from multiple sources and may have no incentive to change their current approaches. The data in a consumer's PDE profile may be more accurate and current given the fact that consumers play an active role in logging their data. In contrast, information about consumers obtained by data brokers may not always be correct and could be out of date. This could make PDE data more desirable to data brokers and other companies. PDE marketplaces may provide additional venues for established companies to access or purchase data. Absent valid and effective restrictions, third parties that obtain access to user data from PDE companies could potentially transfer this information to conventional data brokers and other companies, as well as use the data to make inferences about users in ways that may negatively impact the opportunities they receive.

To address the foregoing concerns, PDE companies could consistently prescreen third parties interested in participating in their marketplaces to determine whether such companies are data brokers. Companies interested in accessing or obtaining consumer PDE data could be explicitly prohibited from engaging in PDE marketplaces if they are unwilling to refrain from subsequently monetizing, transferring, or disclosing consumer data or are not amenable to negotiating data access and disclosure terms with consumers. This, of course, assumes that consumers will become more educated about data-transfer terms and the risks and benefits associated with monetizing their data.

In some instances, PDE companies duplicate data that are generated from a user's interaction with companies that adopt a data-as-payment model.[341] These non-PDE companies will continue to have access to the duplicated streams of consumer-generated data held by PDE companies, may assert ownership of specific rights in such data, and could use them in whatever manner they choose, even if a PDE company provides users with more control over this data once the consumer uses the PDE company's platforms. Questions about data ownership or rights in data are increasingly complex as various entities (as well as consumers) may claim an interest in consumer-generated data. PDE companies' ability to provide consumers with adequate control over this data may be limited to the service and products they provide. Stated differently, consumers may have more privacy and control over their data when interacting with certain PDE companies, but these benefits may not be available when the consumer interacts with other companies that do not adopt a PDE approach. As noted earlier, a similar problem also arises in the PFP-subscription setting, as the activities of other companies may undermine the effectiveness of the data and privacy protection service offered by a VPN company.

---

341. See Firth, The Digi.me Story, supra note 121.

The long-term success of existing pro-consumer PDE companies and the ability of these companies to effectuate true change across the data market depend in part on the willingness of other established companies to either adopt an approach to consumer privacy and data collection that facilitates the goals of PDE companies or at the very least ensure that their activities do not undermine the efforts of companies using consumer-friendly PDE models. Regulatory and legislative responses may influence this result.

With respect to data that are not duplicative of information that is already held by non-PDE companies, PDE companies can serve as data vaults that provide limited access to data on consumers' terms. However, consumer consent should not be used to validate PDE data transfers and disclosures that are detrimental to consumer interests. PDE companies must recognize the failure of the notice-and-choice model and implement effective mechanisms to avoid the pitfalls associated with relying primarily on disclosures in their terms and conditions and privacy policies and consumer consent to justify data disclosures and transfers to third parties in PDE marketplaces.

Additionally, regardless of the activities of non-PDE companies, one must consider that, even though some PDE companies may offer consumers more monetization and data-control options when compared to conventional companies,[342] as new PDE companies enter the market the policies of these companies may not always provide consumers with sufficient control over their data. This, of course, means that consumers would not truly have the ability to protect their own privacy even when interacting with PDE companies.

Other explanations scholars offer for the failure of earlier entities that have attempted to provide consumers with control over their data must also be considered.[343] For example, Professor Peter Swire contends that two of the biggest obstacles "infomediaries" historically face include a lack of consumer trust and an inability to provide sufficient value to users.[344] Thus, the choices consumers make can also impact whether changes will be seen across the data industry. PDE companies must convince consumers to trust them with their information. Additional concerns related to trust and security could also arise if PDE companies

342. See Meeco, Homepage, supra note 235 (explaining that Meeco provides users with a "personal web to browse . . . without leaving a data trail or being tracked by cookies").

343. See, e,g., Goldman, Coasean Analysis, supra note 128, at 1198–99.

344. Peter P. Swire, Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy, 54 Hastings L.J. 847, 859–60 (2003) ("[W]hy should consumers trust one company to manage all their personal information when the business model is based on consumer distrust of how companies handle their data? . . . Infomediaries and the many dot-bombs have failed the market test when they did not offer enough value to consumers.").

permit consumers to store PDE data in unaffiliated cloud platforms offered by other companies.[345]

The rise of the IOT and the prevalence of data-leak scandals may foster consumer interest in PDE offerings and consumer distrust in established companies. One could posit that data volume and variety have increased consistently over several decades. Yet this persistent rise in the quantity of data has not led to significant changes in data practices or consumer interest in data and privacy-related issues. Following that line of argument, consumer apathy and existing data practices will likely continue in the IOT setting. However, for the first time, routine daily activities will be transformed into online activity by the IOT. The Pew Research Center reports that leading experts have acknowledged that "[u]nplugging [from the Internet] is nearly impossible now [but with the IOT] by 2026 it will be even tougher."[346] Even those that would like to refrain from using IOT devices may not have the "will or means to disconnect."[347]

Further, recall that results from various studies and surveys indicate that increasingly more consumers are concerned about their data and privacy.[348] A survey conducted by Consumer Reports in April 2017 of 1,007 adults found that seventy percent of respondents "lack confidence that their personal data is private and safe from distribution without their knowledge."[349] The survey found a five percentage-point increase in the percent of consumers that are concerned about their data when compared to a similar survey conducted by Consumer Reports in January 2017.[350] The widespread attention given to the implications of the repeal of the FCC Rules, combined with a political setting in which parties in power have publicly expressed their goal of dismantling various consumer-friendly regulations, may also lead consumers to view PDE companies as attractive alternatives. Consider that ninety-two percent of respondents to the Consumer Reports survey mentioned above believe

345. See Sync, Privacy White Paper 1 (2015), http://www.sync.com/pdf/sync-privacy.pdf [http://perma.cc/D2WU-KHZK] (discussing Dropbox and Google Drive privacy policies); Digi.me, Security, supra note 128 (discussing storing user data on Dropbox, Google, Drive and other platforms); see also Nilay Patel, Is Google Drive Worse for Privacy than iCloud, Skydrive, and Dropbox?, Verge (Apr. 25, 2012), http://www.theverge.com/2012/4/25/2973849/google-drive-terms-privacy-data-skydrive-dropbox-icloud [http://perma.cc/8G78-GSLM].

346. Rainie & Anderson, IOT Connectivity Binge, supra note 187, at 7.

347. Id. at 4.

348. See supra Part I.

349. Bree Fowler, Americans Want More Say in the Privacy of Personal Data, Consumer Reports (May 18, 2017), http://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data/ [http://perma.cc/7H2V-4RQH].

350. Id.

that "consumers should have the right to request a complete list of the data an internet service provider or website has collected about them."[351]

In this environment, it is entirely possible that PDE companies will succeed where earlier generations of similar entities have failed. The FTC has recommended that legislation be adopted to obligate data brokers to "provide consumers with access to their data" and "allow consumers to suppress the use of [their] information."[352] A 2017 report on consumer attitudes in several countries (including the United States) found that when consumers were asked "what they wanted in exchange for their personal data . . . the response that most people gave was that personal information could be returned or deleted at a time of their choosing . . . ."[353] The report found that consumers valued "personal data privacy-protection and access to their data" more than "financial rewards" and "discounts."[354] As more companies begin providing users with copies of their data, consumers will need platforms to store and understand these data. PDE companies could fulfill this growing demand, and they can provide products for consumers to easily compile, access, and obtain insights from all of their data, thereby generating value for consumers. Consider that recent updates to Twitter's privacy policy allow users to request and receive an email containing all data linked to their account.[355]

Other initiatives and projects aimed at providing consumers with easy access to their data or information about themselves that may be generated by others could also contribute to an environment in which consumers expect to view and receive copies of their data and information connected to them. The OpenNotes initiative, which allows patients

---

351. Id.

352. FTC Data Broker Report, supra note 143, at 50–53.

353. MEF 2017 Consumer Report, supra note 63, at 28.

354. Emma Firth, MEF Global Consumer Trust Study 2017: All Hail the Rise of the Savvy User, Digi.me: Blog (June 29, 2017), http://blog.digi.me/2017/06/29/mef-global-consumer-trust-study-2017-all-hail-the-rise-of-the-savvy-user/ [http://perma.cc/C3KQ-GDQ3]; see also MEF 2017 Consumer Report, supra note 63, at 8.

355. Jon Fingas, Twitter Gives You More Control over How It Uses Your Data, Engadget (May 17, 2017), http://www.engadget.com/2017/05/17/twitter-gives-more-control-over-your-data/ [http://perma.cc/7WVS-QXBY] (noting that the updates to Twitter's privacy policy are likely a result of expansions in how the company uses and shares user data). The updates coincide with revisions to the company's privacy policy that permit the company to retain user data for a longer period, among other things. See id.; Ian Paul, Twitter Rolls Out New Privacy Tools as It Ditches Do Not Track and Expands Data Sharing, PC World (May 18, 2017), http://www.pcworld.com/article/3197343/internet/twitter-rolls-out-new-privacy-tools-as-it-ditches-do-not-track-and-expands-data-sharing.html [http://perma.cc/L28K-YTNM]; Twitter Privacy Policy, Twitter, http://twitter.com/en/privacy [http://perma.cc/BY5Y-6ZBU] (last visited July 28, 2017).

to access their doctors' visits notes and has millions of participants, is one such example.[356]

The European General Data Protection Regulation (GDPR) may also create conditions favorable to the success of PDE companies.[357] The GDPR provides individuals with a "right to be forgotten" and a "right to data portability."[358] The "right to data portability" allows individuals to obtain data they have provided to a company "in a structured, commonly used and machine-readable . . . format" and to transfer their data to third parties.[359] Companies could amend their privacy policies and data practices not only to ensure GDPR compliance when dealing with European users but also to provide similar portability options to American users. PDE companies could also begin coordinating with non-PDE companies (on behalf of consumers) regarding the use and transfer of user data.

The continued expansion and seeming success of existing PDE companies may also encourage movement toward consumer use of PDE products.[360] Digi.me reportedly has more than "400,000 users in 140 countries," and, through its local partners, the company is working with the government of Iceland to provide citizens with copies of their health data.[361] Additionally, Digi.me recently merged with Personal—an American company that "focuse[s] on secure, collaborative creation and management of reusable data."[362] Meeco has launched a "global expansion" of its

356. Notes & You, Open Notes, http://www.opennotes.org/notes-you/ [http://perma.cc/RL3A-ZEVP] (last visited July 28, 2017).

357. Commission Regulation 2016/679, 2016 O.J. (L 119) 1, 60–62.

358. Id. arts. 17, 20.

359. Id. art. 20; see also Linda V. Priebe, How EU Data Privacy Reform Will Impact U.S. Telecoms, Law360 (Mar. 21, 2017), http://www.law360.com/articles/903685 [http://perma.cc/AN7B-U9HQ] ("The portability right includes two separate rights: For data subjects to get their data back; and to transfer their data to another service provider."). But see Peter Swire & Yianni Lagos, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, 72 Md. L. Rev. 335, 338 (2013) (contending that data portability "is a bad fit with U.S. antitrust and E.U. competition law").

360. Natasha Lomas, Digi.me Bags $6.1M to Put Users in the Driving Seat for Sharing Personal Data, TechCrunch (June 30, 2016), http://techcrunch.com/2016/06/30/digi-me-bags-6-1m-to-put-users-in-the-driving-seat-for-sharing-personal-data/ [http://perma.cc/9VNC-J76H] (discussing investments in Digi.me).

361. Emma Firth, Digi.me Allowing Icelandic Citizens to Download Their Own Health Data in World First, Digi.me: Blog (May 31, 2017), http://blog.digi.me/2017/05/31/digi-me-allowing-icelandic-citizens-to-download-their-own-health-data-in-world-first/ [http://perma.cc/F5NM-6C5S]; Emma Firth, Digi.me Raises £4.2M ($6.1M) in Series A Funding Round, Digi.Me: Blog (Jun. 30, 2016), http://blog.digi.me/2016/06/30/digi-me-raises-4-2m-6-1m-in-series-a-funding-round/ [http://perma.cc/EP5T-TAMR]; see also MEF White Paper, supra note 23, at 12.

362. Emma Firth, Digi.me Merges with Personal to Create Global Personal Data Control Powerhouse, Digi.Me: Blog (Aug. 17, 2017), http://blog.digi.me/2017/08/17/digi-me-merges-with-personal-to-create-global-personal-data-control-powerhouse/ [http://perma.cc/7NGC-LJXF].

offerings.[363] These companies are indicative of the market-wide growth that may attract consumer use of PDE products.

B. *Restrictions on PFP Discount Programs*

To the extent that PFP discount programs permit a company to collect, mine, disclose, sell, transfer, or provide third-party companies with access to consumer data, such programs could be prohibited in industries that provide products necessary to ensure full participation of citizens in the digital economy.[364] The broadband industry is one such example. Although AT&T ceased offering its PFP plan, ISPs may begin to widely offer such plans, as suggested by their staunch defense of PFP plans in response to the FCC Rules.[365] In fact, Forrester, a research and consulting company, predicts that the repeal of the FCC Rules will spell a "return of 'pay-for-privacy.'"[366] Consumers should be provided with basic privacy protections to secure their data and privacy in such industries.

---

363. David Swan, Start-Up Meeco in Global Push, The Australian (Mar. 31, 2016), http://www.theaustralian.com.au/business/technology/startup-meeco-in-global-push/news-story/e4ae320082fd15407980340a2f9168e9 (on file with the *Columbia Law Review*) (discussing Meeco's European and American expansion).

364. Supporters of a prohibition on such programs in the broadband context have also made similar arguments and highlighted possible dangers for low-income consumers. Brake, supra note 169, at 6 ("[C]ritics of these sorts of deals argue that broadband is special, because it is an 'essential service' . . . ."). Opponents of the FCC Rules have also contended that the restrictions imposed by the rules implicate free speech concerns, as "[t]he creation, analysis, and transfer of consumer data for marketing purposes constitute speech." Petition for Reconsideration at 9, Protecting the Privacy of Broadband & Other Telecomms. Servs., WC Docket No. 16-106, (FCC filed Jan. 3, 2017), http://ecfsapi.fcc.gov/file/1010300614650/Petition%20for%20Reconsideration%201.3.2017_2.pdf [http://perma.cc/B3Q6-3WCL] (citing U.S. West, Inc. v. FCC, 182 F.3d 1224, 1232 (10th Cir. 1999)). However, a detailed discussion of these issues is beyond the scope of this Article and is left to future scholarship.

365. Jack Derricourt, Five Things to Know About the ISP Privacy Decision in the Senate, Digital J. (Mar. 24, 2017), http://www.digitaljournal.com/internet/five-things-to-know-about-the-isp-privacy-decision-in-the-senate/article/488725 [http://perma.cc/7LWN-LEPZ] (discussing AT&T's PFP plan and stating "we could see similar pay for privacy plans rolling out from other service providers in the near future"); Jeff Dunn, Trump Just Killed Obama's Internet-Privacy Rules—Here's What that Means for You, Bus. Insider (Apr. 4, 2017), http://www.businessinsider.com/trump-fcc-privacy-rules-repeal-explained-2017-4/#-27 [http://perma.cc/L8W6-Z7YV] (noting that AT&T no longer offers its PFP discount plan but the "lack of clear legal barriers" prohibiting such plans opens the door for the future adoption of similar plans by ISPs); see also Letter from Francis M. Buono, Senior VP, Comcast Corp., to Marlene H. Dortch, Sec'y, FCC (Aug. 1, 2016), http://ecfsapi.fcc.gov/file/10802205606782/Comcast%20Ex%20Parte%20–%20WC%20Dkt%20No%2016-106%20–%207-28%20WCB%20Meeting.pdf [http://perma.cc/Y6FC-2H62] ("We also urged that the Commission allow business models offering discounts or other value to consumers in exchange for allowing ISPs to use their data. As Comcast and others have argued, the FCC has no authority to prohibit or limit these types of programs."); Verizon Comments, supra note 169, at 6–23.

366. Dunn, supra note 365 (discussing communications with a principal analyst at Forrester).

Admittedly, in light of the current political climate, it is unlikely that proposals to reinstate the FCC Rules—or for that matter the prohibitions on PFP plans proposed herein—will be implemented. However, given the crucial role ISPs play, this Article joins previous calls for prohibiting these programs.[367]

A possible critique of this approach is that some consumers may not be opposed to paying more for privacy options, and that such a prohibition requires BIAS companies to provide the same level of privacy to everyone even if certain consumers may demand more privacy. One potential response to this critique is that restricting the use of discount plans in certain settings does not automatically prevent companies from offering additional privacy options to consumers that are willing to pay for them while simultaneously providing a baseline level of privacy to all consumers that does not depend on a trade-off between privacy and a discount. Of course, such an approach by a company may generate concerns about unequal access to privacy, particularly if adopted baseline privacy levels are inadequate.

Another related objection is that consumers willingly accept discounts and rewards in other settings in which companies use discounts to collect information about users.[368] A Pew Research Center survey on store loyalty cards found that thirty-two percent of respondents objected to a "free loyalty card" that allowed a company to monitor user shopping habits and sell the data to unaffiliated parties, but fifty-six percent of low-income respondents indicated that the practice "would be acceptable."[369] The willingness of respondents in low-income households to accept such programs highlights concerns about unequal access to privacy. The survey also found that even users who currently use discount cards are worried "about how and under what circumstances their data are passed along to third parties."[370] These concerns included fears about data security, anonymization, telemarketers, and a lack of control over subsequent interactions with companies.[371] Scholars and commentators have highlighted various consumer concerns related to the use of loyalty cards in

367. Brake, supra note 169, at 5–7 (describing proposals to prohibit the use of PFP discount plans in the broadband setting); EPIC Comments, supra note 173; Fulton, supra note 176; see also Letter from Senators Edward Markey, Richard Blumenthal, Al Franken, Elizabeth Warren, Patrick Leahy, Bernie Sanders, Tammy Baldwin, to Tom Wheeler, Chairman, FCC 2 (July 7, 2016), http://www.dslreports.com/r0/download/2276489~9c8eadeef46a724ca4d98bd97565ce17/Letter%20–%20FCC%20Privacy%20%207-7-16.pdf [http://perma.cc/3CAC-JDX3] (urging the FCC to prohibit ISP use of PFP plans given potential harms to "low-income consumers, the elderly and other vulnerable populations").

368. Brake, supra note 169, at 3–4.

369. Maeve Duggan & Lee Rainie, Privacy and Information Sharing, Pew Research Ctr. (Jan 14. 2016), http://www.pewinternet.org/2016/01/14/scenario-consumer-loyalty-cards-and-profiling/ [http://perma.cc/E7E2-DMLG].

370. Id.

371. Id.

the retail and supermarket context.[372] In some instances, a user may be required to sign up for or use a rewards card in order to view or receive discounted prices.[373] The fact that companies in other settings have used discount programs to collect information about users does not mean that consumers have received adequate privacy and data-control protections, and it certainly should not automatically mean that such practices should be permissible in the broadband context. Consumers may not limit their in-store shopping activities to a single store or use discount cards during every purchase. In contrast, many consumers access the Internet daily, which may provide more opportunities to track the activities of users. To adequately address the concerns noted in this Article, restrictions on discount programs in other online settings may also need to be implemented.

C. *The FTC as the Main Regulator*

The FTC's regulatory authority "covers nearly any for-profit entity that handles personal data."[374] However, broadband has been classified as a common carrier service.[375] The FTC's jurisdictional authority over broadband companies is questionable.[376] Professor Hoofnagle suggests that the FTC "cannot police privacy on its own" and that other agencies, such as the FCC and the Consumer Financial Protection Bureau (CFPB),

---

372. Alessandro Acquisti, Leslie K. John & George Loewenstein, What Is Privacy Worth?, 42 J. Legal Stud. 249, 259 (2013) (stating that users are "typically given binary choices, including take-it-or-leave it options" like "choosing to use a grocery loyalty card (which tracks individual purchases but offers a discount the consumers cannot negotiate) or not"); Katherine Albrecht, Supermarket Cards: The Tip of the Retail Surveillance Iceberg, 79 Denv. U. L. Rev. 534, 536–39 (2002) (discussing privacy concerns associated with supermarket rewards cards); Van Loo, supra note 267, at 1331 (discussing the use of "loyalty card data" and "pricing practices").

373. Robert H. Flashman & Alex Lesueur, Univ. of Ky. Coll. of Agric., Privacy: A Balancing Act 1 (2009), http://fcs-hes.ca.uky.edu/sites/fcs-hes.ca.uky.edu/files/frm-rhf-130.pdf [http://perma.cc/RJF5-L9K4] ("[M]any supermarket chains now require their customers to get special cards in order to receive sale prices on certain items. As part of the sign-up process, consumers are asked for personal information, including their name, address, phone number, and Social Security number.").

374. Hartzog & Solove, FTC Data Protection, supra note 280, at 2236.

375. Protecting and Promoting the Open Internet, 30 FCC Rcd. 5601 (2015) (reclassifying broadband Internet service providers as common carriers under Title II of the Communications Act).

376. See Terrell McSweeny, Comm'r, FTC, The Future of Broadband Privacy and the Open Internet: Who Will Protect Consumers? 2 (Apr. 17, 2017) [hereinafter McSweeny Remarks], http://www.ftc.gov/system/files/documents/public_statements/1210663/mcsweeny_-_new_americas_open_technology_institute_4-17-17.pdf [http://perma.cc/J8ML-JSFN] ("[The FTC] does not currently have jurisdiction over the security and privacy practices of broadband, cable and wireless carriers."); Ohlhausen Remarks, supra note 171 ("[T]he FCC's action in 2015 to reclassify broadband shoved the FTC out because [the FTC's] statute exempts common carriers from [its] general jurisdiction."); supra section IV.A (discussing the potential for jurisdictional gaps in existing privacy regulatory frameworks).

are also suited to address privacy concerns in specific industries.[377] The FCC and the CFPB must also play a critical role in protecting consumers. However, the recent repeal of the FCC Rules calls into question the ability of the FCC to effectively protect consumers.[378] Moreover, parties currently wielding political power have expressed an intent to accelerate the undoing of various existing regulatory frameworks (including the classification of "broadband as a common-carrier service").[379] The FTC and the FCC have indicated that they will attempt to collaborate and harmonize their approaches to related privacy and data-security issues.[380] As other commentators have noted, it "isn't so simple to create mirrored regulations at the FCC and FTC given their different frameworks,

377. Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 337. The CFPB also has some regulatory oversight of these privacy issues to the extent that they arise in transactions and companies within the agency's jurisdiction. See, e.g., Press Release, CFPB, CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices (Mar. 2, 2016), http://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/ [http://perma.cc/6QH8-P6VM] (describing a CFPB enforcement action against a company for ineffective data security practices).

378. See David Shepardson, Trump Signs Repeal of U.S. Broadband Privacy Rules, Reuters (Apr. 3, 2017), http://www.reuters.com/article/us-usa-internet-trump-idUSKBN1752PR [http://perma.cc/9NN3-5QGH] (describing the narrow passage of the repeal of the FCC Rules over "strong objections of privacy advocates"); Stephens, supra note 265 (arguing that the "negative security implications of the repeal of the FCC rules are far-reaching and have long-lasting implications for personal privacy and national security").

379. Jenna Ebersole, FCC Will Undo Obama-Era Open Internet Framework, Pai Says, Law360 (Apr. 26, 2017), http://www.law360.com/articles/917465/fcc-will-undo-obama-era-open-internet-framework-pai-says [http://perma.cc/VA3B-H3PY] (reporting on the FCC Commissioner's remarks pledging to undo "the reclassification of broadband as a common carrier service" in 2017); Kelcee Griffis, FCC to Move Forward on Net Neutrality Rollback, Law360 (May 18, 2017), http://www.law360.com/articles/925438/fcc-to-move-forward-on-net-neutrality-rollback [http://perma.cc/6NAC-9D7G] ("FCC commissioners voted 2-1 Thursday to move forward with a process that would reverse Title II broadband classification, the legal footing for the commission's 2015 net neutrality rules."); see also Restoring Internet Freedom, 82 Fed. Reg. 25,568, 25,577 (proposed June 2, 2017) (to be codified at 47 C.F.R. pts. 8, 20) (proposing "to respect the jurisdictional lines drawn by Congress whereby the FTC oversees Internet service providers' privacy practices"). But see McSweeny & Clyburn Joint Statement, supra note 281, at 12 (contending that reversal of the Open Internet rules would permit broadband providers to "shape the future of internet content, mine and sell sensitive personal information, and limit consumer access to the internet in whatever manner they think will bring them the most profit"); McSweeny Remarks, supra note 376, at 6 (suggesting that the FTC lacks expertise in "network engineering" in contrast to the FCC and that it may be best to "continue to rely on" the FCC's expertise in this area); Gregory Roberts, Republican Threat to CFPB Rules May Mean Enforcement Boost, BNA (May 12, 2017), http://www.bna.com/republican-threat-cfpb-n73014450852/ [http://perma.cc/9MYJ-5R58] (discussing threats to dismantle CFPB rules).

380. See Ebersole, FCC's Halt of Privacy Rules, supra note 327 (reporting that the FTC Chair and the FCC Chairman "promised to 'work together' to harmonize FCC rules with FTC standards").

underscoring the complexity of the various agency jurisdictions on privacy protections that the public broadly supports."[381]

Questions about the FTC's jurisdiction and the privacy and data-protection guidelines applicable to specific industries must be resolved. The FTC has recently announced work on a project that will provide clarification on the types of substantial consumer injuries that are actionable for "privacy and data-security claims."[382] The FTC's regulatory approach must effectively address the concerns discussed in Part III, including considering intangible harms to consumers.[383] If necessary, congressional intervention should enable this process, although there may be practical obstacles and significant challenges in the current political environment.

The use of consumer information by existing data brokers may be beneficial to consumers in certain instances, such as the creation of "risk-mitigation products" to avoid fraud and identity theft.[384] However, the FTC has acknowledged that this process also generates serious risks for consumers. These concerns include making "sensitive inferences" about consumers' lives[385] and creating cybersecurity risks.[386] Similar concerns abound in the PDE setting.

As discussed in section III.B above, some PDE companies may arguably be data brokers even though they interact extensively and directly with consumers. The result is that new data brokers are entering a market that is notoriously opaque about which data aggregators hold consumer data, how consumer data are collected, and how the data are used.[387] PDE companies have the potential to mitigate some of these concerns. For example, these companies may clearly identify to whom the company will transfer or give access to consumer data and provide

---

381. Id.

382. See Allison Grande, FTC Head Says Privacy Harm Lines Will Soon Be Clearer, Law360 (Apr. 19, 2017), http://www.law360.com/articles/914825/ftc-head-says-privacy-harm-lines-will-soon-be-clearer [http://perma.cc/S859-DAU5] (noting that the FTC will complete a project to determine which "types of consumer injuries are sufficient to support privacy and security claims" by the end of 2017); see also Bryan Koenig, FTC's Definition of Cyber Injury Getting Broader, Chief Says, Law360 (May 17, 2017), http://www.law360.com/articles/925071/ftc-s-definition-of-cyber-injury-getting-broader-chief-says [http://perma.cc/4K3X-RNUZ] (noting that acting FTC Chair Maureen K. Ohlhausen has stated that the "[d]isclosure of sensitive medical information" and "health and safety risks" could both be considered "substantial injur[ies]" to consumers (internal quotation marks omitted)).

383. Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 344–45 (suggesting that the FTC's "harms-based approach" is a "historical red herring" and that harm should not be limited to "physical and economic injuries").

384. FTC Data Broker Report, supra note 143, at v (noting that data brokers use consumer information to generate "people-search products," "risk-mitigation products," and "marketing products").

385. Id. at iv–v.

386. Id. at vi.

387. Id.

consumers with access to their own data. PDE companies have a direct relationship with consumers and are potentially accountable to consumers, unlike regular data brokers. However, as previously noted, it is possible that PDE data buyers and PDE companies may use aggregated or de-identified consumer data in the same manner as existing data brokers and other companies.[388] Thus, new developments call for increased regulatory scrutiny of PDE companies and existing data brokers. While some companies provide information about their relationships with data brokers,[389] consumers need more clarity with respect to what established data brokers and new PDE data companies are doing with their data. Given the FTC's previous calls for legislation to oversee data brokers,[390] these new changes to the data market reflect a growing need for further legislative intervention in this area. Laws that require companies to provide information to consumers about the type of information they collect, disclose, and transfer, the identity of the specific parties to whom such data are provided, and when such transfers are made could mitigate transparency concerns.[391] However, in imposing such requirements, consideration must be given to the limitations and failures of the notice-and-choice model.

There may also be concerns about adequate compensation for data sales, disclosures, and access to consumer data. Currently, the terms of some PDE arrangements and the price for consumer data appear to be determined solely by PDE companies; thus, it is questionable whether consumers will have the opportunity to negotiate compensation terms for their data or terms regarding subsequent disclosures of their data.[392] If the consumer is the party directly supplying the product in the PDE marketplace, should the consumer not be the one to establish the initial price? Consumers who offer goods for sale on eBay frequently determine the price of the products that they intend to sell.[393] At least one PDE-like company touts that it permits users to determine the price for third par-

388. See supra notes 214–234 and accompanying text.

389. See, e.g., Appended & Matched Data, Yahoo!, http://policies.yahoo.com/us/en/yahoo/privacy/topics/appenddata/index.htm [http://perma.cc/S7Z8-DPDE] (last visited July 28, 2017) (stating that Yahoo! may obtain information from a list of various data brokers and combine that information with data provided by customers who use their services).

390. See FTC Data Broker Report, supra note 143, at 49–56.

391. A statute giving consumers similar rights was proposed in Illinois. See Hannah Meisel, Data-Selling 'Right to Know' Bill Clears Hurdle in Ill., Law360 (Mar. 14, 2017), http://www.law360.com/articles/901936 [http://perma.cc/7HZ4-RBDG] (describing the proposed Right to Know Act).

392. See supra section II.C.

393. See Create Effective eBay Listings, eBay, http://pages.ebay.com/seller-center/listing/create-effective-listings.html [http://perma.cc/AW3U-7A57] (last visited Aug. 19, 2017).

ties to contact them.[394] Of course, one could contend that consumers are not in the best position to determine the value of their data, or alternatively that, as in other consumer transactions, form contracts with preestablished prices and terms are more efficient. In either case, given the expected growth in the variety and volume of data generated by consumers' use of IOT devices, there should be increased governmental oversight of PDE markets and consumer complaints related to unauthorized use of their data.

To the extent that it is authorized to do so, the FTC must rigorously pursue PDE companies that fail to live up to their promises of providing consumers with increased privacy or control over their data and information about potential data buyers. If PDE companies commit to imposing restrictions on subsequent monetizations by third-party companies that access consumer data via PDE marketplaces, these promises should be kept and enforced. Nevertheless, a company's failure to meet express and implied promises is not the only concern in the PDE context. The FTC must move away from an overreliance on misrepresentations made by companies and its deception authority and begin to more widely use its unfairness authority.[395] In fact, the FTC has recognized the limits of self-regulation.[396] To the extent that the FTC's unfairness or deception authority is inadequate to effectively address the concerns noted in this Article, a legislative response may be necessary. The possible development of new monetization schemes, such as the use of consumer data for financing purposes as discussed in section III.C, must also be actively monitored given related concerns.

---

394. See About Nextio, Nextio, http://www.nextio.com/n/about [http://perma.cc/LK8J-37EU] [hereinafter Nextio, About Nextio] (last visited July 28, 2017) ("As Nextio members, you establish the guidelines for who you're open to being contacted by, what you're open to being contacted about, and how much it will cost anyone else to contact you about anything else."). Companies adopting an attention payment model provide users with a venue to be compensated for their attention. For instance, Nextio describes consumer attention as "the new currency." Nextio, http://www.nextio.com/ [http://perma.cc/GNJ8-PSM7] (last visited July 28, 2017). Nextio's website states, "It's Your Data, You can take it with you at any time." About Nextio, supra. This model is similar to the compensated telemarketing scenario Professor Ian Ayres and Matthew Funk proposed. See Ayres & Funk, supra note 30, at 80 ("Households should be allowed to decide how much they will be compensated for receiving telemarketing calls."). But see Goldman, Coasean Analysis, supra note 128, at 1195–96 (contending that while a small number of companies "have carved out small niches . . . attention markets collectively play a negligible role in marketer-consumer matchmaking" in part because "consumer response to attempted attention markets has been underwhelming"). See generally Tim Wu, The Attention Merchants: The Epic Scramble to Get Inside Our Heads 3–7 (2016) (discussing the rise of the attention industry).

395. Hoofnagle, FTC Privacy Law and Policy, supra note 201, at 345–47.

396. FTC Rapid Change Report, supra note 283.

D. *Monetization Restrictions*

Legislation has long been used to impose use constraints on certain types of information, and these restrictions "rest on a social judgment that even if transacting parties both wish to reveal and use a particular piece of information, its use should be forbidden because of some social harm . . . that is greater than the social benefits."[397]

The harms associated with the potential monetization of child data in the PDE marketplace likely exceed the resulting benefits, and existing or new regulation must effectively account for this development. Consideration must be given to whether the ability of parents to monetize child data, as well as potential monetizations by children over the age of thirteen in the PDE context, should be permissible.

One could contend that the level of privacy afforded to minors should always be left to parents, who can be trusted to consistently act in the best interests of their children. However, as noted in Part III, parents are likely not immune from techniques used by companies to shape consumer perceptions, and parents—like most consumers—may not always review or understand the implications of a company's terms and conditions and privacy policy. Parental consent to data monetization should not be used to justify data collection and monetization practices that are harmful to the long-term interests of children.

Another potential objection to imposing restrictions on child data is that it is unlikely that parents will intentionally engage in PDE marketplaces using their children's data. Parental monetization of the experiences and activities of children is already taking place in some venues.[398] The plethora of family vlogs documenting the lives of children on YouTube is one such example. Parents can earn significant funds from the monetization of these videos.[399] It is not beyond the realm of possibility that child data may be used in PDE marketplaces.

The early age at which children begin accessing the Internet and leaving digital footprints, as well as the expected proliferation of IOT devices, may warrant a new approach to protecting child data and amendments to COPPA. Data analytics could provide insights about children that companies could use to shape the long-term (including adulthood) preferences of minors. As noted previously, PDE companies could attempt to address this concern by imposing contractual restrictions on the subsequent use of data as well as adopting mechanisms to minimize the use of child data in PDE marketplaces, but issues related to the supply side of the data must also be addressed.

---

397. Peppet, The Unraveling of Privacy, supra note 30, at 1200.

398. Rachel Bertsche, How This Family Made More than $1 Million from YouTube Videos of Their Kids Playing with Toys, Yahoo! (Mar. 16, 2015), http://www.yahoo.com/news/how-this-family-made-more-than-1-million-from-113525464417.html [http://perma.cc/S3QN-PHU4].

399. Id. A more thorough analysis of whether restrictions on the monetization of child data should be imposed in other settings is left to future scholarship.

Another possible critique of imposing explicit restrictions is that in some instances it may be difficult for parents who would like to monetize their household data to separate adult data from child data. Despite these concerns, when it is possible to clearly identify child data or IOT data generated from the use of IOT toys, monetization schemes using such data may need to be restricted to adequately protect children.

To the extent that child data are monetized or provided, minors could be provided with a right to delete that permits them to request that PDE companies erase their data regardless of who provided the data, whether consent or consideration was received, and whether the company targets minors or is aware that the data of minors are being provided.[400] Consideration must also be given to the age at which any such right should be triggered.[401] PDE companies must implement mechanisms to address child data that may be collected from shared family devices and accounts.

Monetizations by landlords of data generated by renters must also be adequately regulated. Additional legislation could be widely adopted to expressly prohibit landlords from requiring tenants to consent to providing access to data exchange accounts as a condition of tenancy. Any such legislation must be broadly drafted to ensure that it is not limited to social media accounts and will also cover PDE consumer arrangements, PDE insights, and data generated by IOT devices.

Although addressing the issues associated with renters and children is an important goal, remedying these issues without more is unlikely to be sufficient to resolve all concerns associated with PDE and PFP models, particularly for individuals who do not fall within these categories. Comprehensive responses to the issues detailed in this Article are necessary.

---

400. See, e.g., Cal. Bus. & Prof. Code § 22581 (2015) (providing minors with the ability to request that their information be deleted subject to certain exceptions). The statute gives limited protection for minors. For instance, one section provides that "an operator or a third party is not required to erase or otherwise eliminate, or to enable erasure or elimination of, content or information [in certain instances including when] the minor has received compensation or other consideration for providing the content." Id.; see also Michael J. Kelley & David Satola, The Right to Be Forgotten, 2017 U. Ill. L. Rev. 1, 44 (2017) (contending the California statute "gives minors who are registered users of an operator's Internet website the right 'to remove or, if the operator prefers, to request and obtain removal of, content or information posted on the operator's Internet websites, online service, online application, or mobile application by the user'" (quoting Cal. Bus. & Prof. Code § 22581(a)(1))). A right to delete or a right to be forgotten may also implicate freedom of expression concerns that may need to be considered. Jeffrey Rosen, The Right to Be Forgotten, 64 Stan. L. Rev. Online 88, 91 (2012), http://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/ [http://perma.cc/7SLR-7AZM] (suggesting that if a third party posts content about an individual, a right to delete "raises the most serious concerns about free expression").

401. Basic contract law principles relating to minors who enter into agreements may also be relevant. See E. Allen Farnsworth, Contracts 221–24 (4th ed. 2004) (discussing contracts voidable at the option of the minor and applicable state statutes).

E. *Structuring PDE Arrangements*

Guidance on the most effective ways to structure arrangements between PDE companies and consumers may be necessary to ensure sufficient protection for consumers. Courts, legislators, and entities that produce influential sources of law may play an important role in this process. Existing legal frameworks may need to be adjusted to ensure adequate consumer protection.

With respect to data-trade agreements, one scholar has proposed a "hybrid inalienability regime" in which individuals may transfer their data as long as they are provided with an opportunity to limit subsequent transfers of their data to unaffiliated entities.[402] Consumer interests may be more adequately protected if any proposed right to limit certain types of subsequent disclosures, transfers, and uses extends to both affiliated and unaffiliated entities.

Another potential option is a licensing approach to consumer PDE agreements. Existing frameworks applicable to software and computer information transactions, such as the American Law Institute's (ALI) Principles of the Law of Software Contracts and the Uniform Computer Information Transactions Act (UCITA), may be useful models.[403] Although UCITA contains specific provisions applicable to mass-market license transactions, such as rules related to the adoption of contract terms, consumer-protection advocates have criticized the uniform law.[404] To the extent that these frameworks are used as a model, they must be adapted to ensure that the interests of consumers are sufficiently protected.

---

402. Schwartz, Property, Privacy, and Personal Data, supra note 30, at 2060 (suggesting a hybrid inalienability regime that "permit[s] an initial transfer of personal data from the individual, but only if the concerned individual is granted an opportunity to block further transfers or uses by unaffiliated entities").

403. Nancy S. Kim, Expanding the Scope of the Principles of the Law of Software Contracts to Include Digital Content, 84 Tul. L. Rev. 1595, 1595 (2010) (discussing the ALI's Software Principles and contending that it excludes digital content); Samuelson, supra note 29, at 1129 (discussing alternative legal regimes for protecting personal information).

404. Unif. Comput. Info. Transactions Act § 209(a) (Nat'l Conference of Comm'rs on Unif. State Laws 2002); Robert L. Oakley, Fairness in Electronic Contracting: Minimum Standards for Non-Negotiated Contracts, 42 Hous. L. Rev. 1041, 1072–73 (2005) (discussing criticisms of UCITA and contending that the uniform law has not been widely adopted); see also Brian D. McDonald, The Uniform Computer Information Transactions Act, 16 Berkeley Tech. L.J. 461, 470–74 (2001) (discussing Maryland's version of UCITA); Juliet M. Moringiello & William L. Reynolds, What's Software Got to Do with It? The ALI Principles of the Law of Software Contracts, 84 Tul. L. Rev. 1541, 1542 (2010) (discussing "bomb-shelter" provisions adopted by states to prevent application of UCITA and stating that UCITA is "dead in the water"). Additionally, even in states that have adopted UCITA, revisions have been made to the statute. Compare Md. Code Ann., Com. Law § 22-209 (LexisNexis 2013), with Va. Code Ann. § 59.1-502.9 (2014), and Unif. Comput. Info. Transactions Act § 209(a).

Guidance on structuring PDE agreements must also consider whether such arrangements should be exclusive, which may impact the ability of consumers to simultaneously monetize their data with other PDE companies. PDE consumer agreements should also be revocable at the option of the consumer.[405] Overly broad, perpetual, royalty-free, transferable-rights provisions and authorizations that permit a PDE company to use consumer data in ways that go beyond what is generally required to provide the products offered should not be encouraged. Provisions that are common to form consumer contracts, which negatively impact consumers' remedies or ability to sue in the event of a breach, should not be widely used in PDE agreements.[406]

Issues surrounding the validity of privacy notices as contracts may also be relevant as may other sources of contract law applicable to consumers.[407] The ALI has announced work on the Restatement of the Law of Consumer Contracts (ALI Restatement).[408] If finalized and adopted, the ALI Restatement could provide guidance on the contract status of privacy policies and shed light on related case law trends, as well as other consumer contracting issues that may be relevant to structuring PDE agreements.[409]

---

405. Professor Paul Schwartz has suggested that "[c]onsent to data trade should imply not only an initial opportunity to refuse trade, but also a later chance to exit from an agreement to trade." Schwartz, Property, Privacy, and Personal Data, supra note 30, at 2106.

406. See, e.g., Datacoup, Terms of Service, supra note 185 (discussing an "agreement to arbitrate," class action waiver, and users' ability to opt out). A thorough discussion of the potential consumer causes of action and remedies for breach of PDE agreements is left to future scholarship.

407. Although one may argue that Article 2 of the UCC could apply to PDE-data trade agreements as a consumer's data could be viewed as a good under Article 2 to the extent that it is "movable at the time of identification to the contract for sale," there are several problems with such an argument. First, there may be challenges associated with labeling consumer data as "goods" under Article 2's current definition of goods. U.C.C. § 2-105 (Am. Law Inst. & Nat'l Conference of Comm'rs on Unif. State Laws 2014) ("'Goods' means all things (including specially manufactured goods) which are movable at the time of identification to the contract for sale other than the money in which the price is to be paid, investment securities (Article 8) and things in action."). At least one court has distinguished goods from data. See Burrows v. Purchasing Power, LLC, No. 1:12-cv-22800-UU, 2012 WL 9391827, at *3 (S.D. Fla. Oct. 18, 2012) ("Personal data does not have an apparent monetary value that fluctuates like the price of goods or services."). Section 2-102 provides that "[u]nless the context otherwise requires, this Article applies to transactions in goods." U.C.C. § 2-102. One might contend that a transaction involving consumer data is a context in which Article 2 should not apply by arguing that data associated with PDE agreements are more akin to general intangibles.

408. See Restatement of the Law, Consumer Contracts, ALI, http://www.ali.org/projects/show/consumer-contracts/ [http://perma.cc/X85D-LZ5F] (last visited Sept. 25, 2017).

409. See Project Feature, Restatement of the Law, Consumer Contracts, The ALI Advisor, http://www.thealiadviser.org/consumer-contracts/ [http://perma.cc/8A8M-CDV8] (last visited Sept. 25, 2017) (listing topics the potential Restatement may address).

CONCLUSION

PFP programs and the PDE marketplace are innovative offerings that have been provided to meet and exploit the growing demand for privacy and data controls and the ever-increasing variety and quantity of consumer data. However, these models present significant privacy and data-protection challenges, some of which are similar to the issues raised by earlier generations of data business models. PFP and PDE models generate substantial concerns for consumers, including the potential for exacerbating preexisting inequalities and unequal access to privacy. In some instances, consumers may be more adequately protected when the use of such programs is prohibited or when monetization is restricted. Guidance is also needed to evaluate pressing issues, such as how best to structure PDE agreements, and legal frameworks may need to be adjusted to account for new monetization schemes. Increased regulatory guidance and oversight of existing data aggregators and PDE companies are needed and jurisdictional ambiguities must be resolved. Despite the foregoing, if the concerns noted herein are effectively addressed, PDE companies may have the ability to influence how consumers and established companies view and use consumer data. New developments, such as the GDPR, may facilitate this process. Regulation in this area must meet the difficult goal of promoting innovation while simultaneously protecting consumer interests.