Cite as: Noam Kolt, *Return on Data*, 38 YALE LAW & POLICY REVIEW (forthcoming 2019)

RETURN ON DATA

Noam Kolt*

Consumers routinely supply personal data to technology companies in exchange for services. Yet, the relationship between the utility (U) consumers gain and the data (D) they supply — "return on data" (ROD) — remains largely unexplored. Expressed as a ratio, ROD = U / D. While lawmakers strongly advocate protecting consumer privacy, they tend to overlook ROD. Are the benefits of the services enjoyed by consumers, such as social networking and predictive search, commensurate with the value of the data extracted from them? How can consumers compare competing data-for-services deals? Currently, the legal frameworks regulating these transactions, including privacy law, aim primarily to protect personal data. They treat data protection as a standalone issue, distinct from the benefits which consumers receive. This article suggests that privacy concerns should not be viewed in isolation, but as part of ROD. Just as companies can quantify return on investment (ROI) to optimize investment decisions, consumers should be able to assess ROD in order to better spend and invest personal data. Making data-for-services transactions more transparent will enable consumers to evaluate the merits of these deals, negotiate their terms and make more informed decisions. Pivoting from the privacy paradigm to ROD will both incentivize data-driven service providers to offer consumers higher ROD, as well as create opportunities for new market entrants.

TABLE OF CONTENTS

I. INTRODUCTION

Many data-driven companies do not charge fees for the services they provide. They market their services as free.[1] But these arrangements can be misleading. The business models of the FANGs, BATs and other service providers rely on consumers trading personal data for services.[2] Consumers, in effect, pay for services with personal data.[3] The bargain is data *for* services. Although lawmakers have confronted the erosion of privacy, they have given little attention to this bargain, which is now at the core of the increasingly post-privacy economy.[4] Privacy and data protection continue to monopolize the debate.[5] Change is overdue. We need to begin to explore return on data (ROD)—*the relationship between the price consumers pay, in the form of data, and the utility of the services they receive*.

Skepticism around the prevailing privacy paradigm is growing. Brittany Kaiser, former Director of Business Development at Cambridge Analytica, provocatively declared that "[p]rivacy doesn't exist in a post-Facebook crisis era. . . . Just like with Airbnb, if somebody is going to come and use your physical assets, you would expect to agree a price and what they're going to do with it before you hand over the keys to your house. . . . Why isn't it the same with your data?"[6] Kaiser's remarks are revealing. They imply that perhaps we can no longer adequately protect personal data and that, consequently, we should consider what consumers *receive* in return for the data they supply. Lawmakers are also beginning to recognize the limitations of the privacy paradigm. In the Senate hearing before which Facebook CEO Mark Zuckerberg testified, Commerce Committee Chairman John Thune remarked that "whether you are using Facebook or Google or some other online services, we

---

* Noam Kolt is a corporate lawyer whose practice focuses on venture capital, M&A and technology regulation. Many thanks to Shaanan Cohney, Adi Deutsch, Reza Green, Teddy Lazebnik and the working group of Monash University Law Faculty alumni for reviewing earlier versions of this article.

[1] *See, e.g., Transcript of Mark Zuckerberg's Senate Hearing*, WASH. POST (Apr. 10, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/ ("There will always be a version of Facebook that is free.") *See also Zuckerberg's Appearance before House Committee*, WASH. POST (Apr. 11, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee/.

[2] Facebook, Amazon, Netflix and Alphabet, and Baidu, Alibaba and Tencent, respectively. *See, e.g.*, Jacky Wong, *BATs vs. FANGs: Why China's Tech Has Extra Risk*, WALL ST. J. (Oct. 13, 2017), https://www.wsj.com/articles/bats-vs-fangs-why-chinas-tech-has-extra-risk-1507870793.

[3] *See* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1420 (2017); MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY § 1.26 (2016); BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 1, 47 (2015). *See, e.g.,* Rachel Metz, *Google's New Tools Will Make Your Life More Convenient—For a Price,* MIT TECH. REV. (May 7, 2018), https://www.technologyreview.com/s/611079/googles-new-tools-will-make-your-life-more-convenientfor-a-price/; Mary Madden, *Need Medical Help? Sorry, Not Until You Sign Away Your Privacy*, MIT TECH. REV. (Oct. 23, 2018), https://www.technologyreview.com/s/612282/need-medical-help-sorry-not-until-you-sign-away-your-privacy/; Jason T. Voiovich, *Using Google Maps Costs More than You Think*, MEDIUM (Dec. 17, 2018), https://medium.com/swlh/using-google-maps-costs-more-than-you-think-d62c7d857b2d.

[4] *See* ANDREAS S. WEIGEND, DATA FOR THE PEOPLE: HOW TO MAKE OUR POST-PRIVACY ECONOMY WORK FOR YOU 969 [Kindle location] (2017); *The End of Privacy (Special Issue)*, 347 SCIENCE (2015). *Cf, e.g.,* R "Ray" Wang, *Beware Trading Privacy for Convenience*, HARV. BUS. REV. (June 10, 2013), https://hbr.org/2013/06/beware-trading-privacy-for-con (describing privacy as a "societal choice").

[5] *See, e.g.,* Natasha Singer, *Facebook's Push for Facial Recognition Prompts Privacy Alarms*, N.Y. TIMES (July 9, 2018), https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html; Complaint for Violations of the Consumer Protection Procedures Act, District of Columbia v. Facebook, Inc. (D.C. Super. Ct. Civ., filed Dec. 19, 2018).

[6] Michelle Jamrisko & Mark Miller, *If Privacy Is Dead, Some Argue People Should Sell Their Own Data*, BLOOMBERG (Sept. 6, 2018), https://www.bloomberg.com/news/articles/2018-09-06/if-privacy-is-dead-some-argue-people-should-sell-their-own-data.

are trading certain information about ourselves for free or low-cost services." Judiciary Committee Chairman Chuck Grassley stated that "[a]s we get more free or extremely low-cost services, the trade-off for the American consumer is to provide more personal data."[7]

Despite the growing recognition of data-for-services transactions, several important questions are not being addressed. What is the precise *data price* which consumers pay for a given service? Do all consumers pay the same data price for a given service? What exactly do consumers receive *in return* for the data they supply? Do all consumers enjoy the same benefits in exchange for sharing the equivalent quantity and quality of personal data? Which service providers offer consumers the best deals? Without a clear conceptual framework and granular insight into data-for-services transactions, it is difficult to answer these questions. At present, consumers cannot assess precisely how much they pay (in personal data) for the services they receive. Nor can they assess the specific utility they gain in return for the data they supply. ROD—*the relationship between the data price consumers pay and the benefits they receive*—is unknown.

To date, there are no legal frameworks which regulate ROD or data platforms which evaluate ROD. Existing legal frameworks and data platforms tend to overwhelmingly focus on privacy. The chief response to the many privacy scandals embroiling Facebook has been to demand greater protection for personal data.[8] Although privacy laws in the United States and in the EU have significantly developed in recent years,[9] they too focus on data protection. The EU's General Data Protection Regulation (GDPR), which came into effect in 2018, and California's Consumer Privacy Act, which is due to come into effect in 2020, do not scrutinize the benefits which consumers reap from data-for-services transactions or investigate how these benefits weigh up against the data price which consumers pay. Terms of service and privacy policies, which establish the parameters of data-for-services transactions, decouple the collection of personal data from the provision of services.[10]

Alongside these legal developments, the emerging field of privacy tech is flourishing.[11] There are scores of technologies which monitor data collection and facilitate data protection.[12] Some companies give consumers the option of paying a monetary premium to receive privacy-friendly versions of services which would otherwise collect vast amounts of personal data.[13] Privacy is also increasingly being integrated into the design of consumer products and services.[14] However, with few exceptions, privacy technologies aim to *protect*

---

[7] *Senate Hearing*, *supra* note 1.

[8] *See* Jessica Rich, *Beyond Facebook: It's High Time for Stronger Privacy Laws*, WIRED (Aug. 4, 2018), https://www.wired.com/story/beyond-facebook-its-high-time-for-stronger-privacy-laws/; Zack Whittaker, *In Senate Hearing, Tech Giants Push Lawmakers for Federal Privacy Rules*, TECHCRUNCH (Sept. 26, 2018), https://techcrunch.com/2018/09/26/in-senate-hearing-tech-giants-push-lawmakers-for-federal-privacy-rules/; James Vincent, *Tim Cook Warns of 'Data-Industrial Complex' in Call for Comprehensive US Privacy Laws*, VERGE (Oct. 24, 2018), https://www.theverge.com/2018/10/24/18017842/tim-cook-data-privacy-laws-us-speech-brussels; Michael LaForgia et al., *Facebook's Data Deals Are Under Criminal Investigation*, N.Y. TIMES (Mar. 13, 2019), https://www.nytimes.com/2019/03/13/technology/facebook-data-deals-investigation.html.

[9] *See infra* Part III.B. *See also, e.g.,* Adam Satariano, *Google Is Fined $57 Million Under Europe's Data Privacy Law*, N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

[10] *See infra* Part III.A. *But see infra* Part III.D.

[11] *See* Alyssa Newcomb, *At CES, Tech's Biggest Trade Show, Privacy Was the Buzzword*, NBC (Jan. 12, 2019), https://www.nbcnews.com/tech/security/ces-tech-s-biggest-trade-show-privacy-was-buzzword-n957826. *Cf* Pete Pachal, *CES 2019 Had Nothing to Say about the Biggest Conversation in Tech*, MASHABLE (Jan. 12, 2019), https://mashable.com/article/ces-2019-consumer-data-privacy/#T8CftbcriaqM.

[12] *See infra* Part IV.A.

[13] *See infra* Part IV.B.

[14] *See, e.g.,* Blake Morgan, *Apple Flaunts Privacy at CES: Why Other Companies Should Pay Attention*, FORBES (Jan. 7, 2019), https://www.forbes.com/sites/blakemorgan/2019/01/07/apple-flaunts-privacy-at-ces-

personal data.[15] They do not attempt to assess what consumers receive in exchange for the personal data they supply.

Although data protection and privacy are vital and fuel much of the techlash against data-driven companies, they are not the only issue confronting the data economy. The privacy paradigm and lack of engagement with ROD are question-begging. Regulators and developers seeking to tackle the collection, use and trade of personal data largely ignore the benefits which consumers receive in exchange for the personal data they share. *Privacy* law, *privacy* policies and *privacy* tech are partly to blame. By emphasizing data protection, they obscure the exchange that underpins the predominant business model of data-driven firms.

To engage more critically with data-for-services transactions, we need to pivot away from the prevailing privacy paradigm and transition towards a new analytical apparatus. The first step is to establish a conceptual framework for evaluating ROD. The second step is to develop practical tools for assessing ROD. The third step is to communicate ROD evaluations to consumers. The goal of making ROD more transparent is to help consumers understand the mechanics of data-for-services transactions and enable them to factor ROD into their decision making. If consumers were able to select services (even partly) on the basis of ROD, data-driven service providers would be unlikely to remain indifferent. In order to compete with firms providing comparable services, they would need to increase consumers' ROD, either by reducing the data price or providing additional benefits to consumers. In this way, ROD could bolster competition, stimulate innovation and, ultimately, offer consumers more favorable data-for-services deals.

The following four principles provide a basic conceptual roadmap for evaluating ROD:

1. *ROD gauges the relationship between the utility (U) consumers gain and the data (D) they supply in data-for-services transactions. Expressed as a ratio, ROD = U / D.*
2. *ROD evaluations need to be personalized and dynamic.*
3. *To assess ROD, you need to collect personal data.*
4. *ROD evaluations are most appropriate for comparing transactions in which similar services are provided.*

Part II of the article critically examines the phenomenon of data-for-services transactions. Aided by behavioral insights, it questions our preoccupation with privacy and advocates a transition to ROD. Part III considers the legal frameworks which regulate data-for-services transactions, including privacy policies, privacy law and the proposal that property rights attach to personal data. It depicts how these frameworks do not address the mutual exchange inherent in data-for-services transactions. The one exception is a recent EU proposal which recognizes that consumers routinely pay for services with personal data. Part IV canvasses a range of data platforms which aim to protect personal data or provide monetary and other benefits in exchange for personal data, but do not actually attempt to quantify or communicate ROD. Part V outlines four guiding principles for assessing ROD and making data-for-services transactions more transparent. It concludes that ROD has the potential to both empower individual consumers and incentivize data-driven service providers to carefully consider the relationship between the personal data they collect and the services they provide.

---

why-other-companies-should-pay-attention/#50675f0a10bf; Tripp Mickle, *Apple Exerts Power as Privacy Protector*, WALL ST. J. (Jan 31., 2019), https://www.wsj.com/articles/apple-exerts-power-as-privacy-protector-11548982840.

[15] *See infra* Part IV.C.

II. PIVOTING FROM PRIVACY TO RETURN ON DATA

A. Exchanging Personal Data for Services

Finja, a digital payments company, does not charge consumers transaction fees. Instead, it relies on selling consumers value-added services, such as credit and insurance, which it can effectively market with the assistance of data-driven technologies.[16] According to Finja's CEO, the real price which consumers pay is personal data.[17] This business model extends beyond fintech. Consumers in many contexts regularly use services provided by firms that collect personal data relating to them. These services often incur no monetary charge.[18] Consumers receive services in return for enabling service providers to collect personal data. These exchanges are a form of barter, a *quid pro quo*.[19]

Data-for-services transactions are usually mutually beneficial. The collection of data is not an externality imposed on consumers, a hidden cost which they must bear in order to receive nominally "free" services.[20] Data collection is simply the price of the services they consume.[21] Conversely, service providers do not receive personal data at no cost.[22] They provide services in exchange for personal data. Data-for-services transactions are a give-and-take which provides value to both parties. Consumers access personalized newsfeeds, crowd-sourced traffic updates and other valuable services.[23] Meanwhile, companies access personal data which enable them to glean consumer preferences and facilitate targeted advertising,[24] or provide (or on-sell) those data to firms which do.[25] Personal data can also help companies

---

[16] FINJA (last visited __), http://finja.pk/Index.

[17] *Money Talks: Don't Bank with Me Argentina*, ECONOMIST (May 8, 2018), https://soundcloud.com/theeconomist/money-talks-dont-bank-with-me.

[18] *But see, e.g.,* Elvy, *Paying for Privacy*, *supra* note 3, at 1387 (discussing freemium models). *See also infra* Part V.A (considering the role of monetary payments alongside data payments).

[19] *See* JARON LANIER, WHO OWNS THE FUTURE? 51 (2013); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 255 (2013); Jacob M. Victor, *Comment, The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513, 517 (2013). *See also* Timothy D. Sparapani, *Putting Consumers at the Heart of the Social Media Revolution: Toward a Personal Property Interest to Protection Privacy*, 90 N.C. L. REV. 1309, 1316 (2012) (describing these as trade-offs).

[20] *Cf* Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 609, 649 (2014) (treating data collection as an unforeseen transaction cost); CHRIS ANDERSON, FREE: THE FUTURE OF A RADICAL PRICE 18–20 (2009) (describing data-driven advertising revenue as a form of cross-subsidy).

[21] *But see infra* note 219 (discussing objections to commodifying personal data).

[22] *Cf* LANIER, *supra* note 19, at 49 (arguing that "siren servers" do not pay for the data they collect). *See also* ERIC POSNER & GLEN WEYL, RADICAL MARKETS: UPROOTING CAPITALISM AND DEMOCRACY FOR A JUST SOCIETY 234 (2018); *The Digital Proletariat: Should Internet Firms Pay for the Data Users Currently Give Away?*, ECONOMIST (Jan. 11, 2018), https://www.economist.com/finance-and-economics/2018/01/11/should-internet-firms-pay-for-the-data-users-currently-give-away (describing data-driven service providers as free-riders).

[23] *See, e.g.*, Jay R. Corrigan et al., *How Much Is Social Media Worth? Estimating the Value of Facebook by Paying Users to Stop Using It*, PLOS ONE (Dec. 19, 2018), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0207101 (using experimental auctions to discover the monetary value which users place on Facebook's services).

[24] *See, e.g.,* Lara O'Reilly & Laura Stevens, *Amazon, With Little Fanfare, Emerges as an Advertising Giant*, WALL ST. J. (Nov. 27, 2018), https://www.wsj.com/articles/amazon-with-little-fanfare-emerges-as-an-advertising-giant-1543248561. *See generally* David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, 23 J. ECON. PERSP. 37 (2009).

[25] *See, e.g.,* Gabriel J.X. Dance et al., *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html; Ava Kofman, *Google's Sidewalk Labs Plans to Package and Sell Location Data on Millions of Cellphones,*

train artificial intelligence (AI) and machine learning (ML) systems,[26] as well as perform A/B testing and other product analytics.[27] Importantly, payment—in the form of data collection—is not a one-off event. Nor is it comprised of several distinct installments, as is common in retail transactions. Rather, payment is ongoing.[28] In return for providing continuous access to certain services, service providers can capture personal data on an ongoing basis.

For many companies, the data-for-services business model is highly lucrative. A majority of the largest companies globally, namely Alphabet, Amazon, Tencent, Alibaba and Facebook and, increasingly, Apple and Microsoft, are, to varying degrees, data-driven.[29] Facebook, for example, does not charge users a monetary fee. Instead, it collects personal data which users generate, and uses these to power a targeted advertising platform.[30] From the consumers' perspective, the deal is data-*for*-services. In the case of Facebook, over 2 billion people accept this deal.[31] Similarly, Google does not charge users a monetary fee for many of the services it offers, including search, Gmail and Google Drive. Instead, Google collects personal data which users generate and uses these for a variety of purposes.[32] Billions of people, in practice, embrace this deal.[33]

But Google and Facebook are not alone. Data-for-services transactions are ubiquitous.[34] Many companies now have an intimate portrait of their customers' lives and the lives of the people with whom they interact.[35] Amazon, Netflix, Spotify and other data-driven

---

INTERCEPT (Jan. 28, 2019), https://theintercept.com/2019/01/28/google-alphabet-sidewalk-labs-replica-cellphone-data/. *But see* Hamza Shaban & Brian Fung, *AT&T Says It'll Stop Selling Your Location Data, Amid Calls for a Federal Investigation*, WASH. POST (Jan. 10, 2019), https://www.washingtonpost.com/technology/2019/01/10/phone-companies-are-selling-your-location-data-now-some-lawmakers-want-federal-investigation/.

[26] Imanol Arrieta-Ibarra et al., *Should We Treat Data as Labor? Moving Beyond "Free"*, 108 AM. ECON. ASSOC. PAPERS & PROC. 38, 40–41 (2018).

[27] *See, e.g.,* Ya Xu et al., *From Infrastructure to Culture: A/B Testing Challenges in Large Scale Social Networks*, PROC. ACM SIGKDD ON KNOWLEDGE DISCOVERY AND DATA MINING (2015).

[28] *See* Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, U. CHI. LEGAL F. 95, 131, 150 (2013).

[29] *See Global Top 100 Companies by Market Capitalisation*, PWC (Mar. 31, 2018), https://www.pwc.com/gx/en/audit-services/assets/pdf/global-top-100-companies-2018-report.pdf. *See also* Michael Sheetz, *Just Three Stocks Are Responsible for Most of the Market's Gain This Year*, CNBC (July 10, 2018), https://www.cnbc.com/2018/07/10/amazon-netflix-and-microsoft-hold-most-of-the-markets-gain-in-2018.html. *But see Big Tech's Sell-Off*, ECONOMIST (Nov. 1, 2018), https://www.economist.com/business/2018/11/01/big-techs-sell-off.

[30] *See* Felix Richter, *Facebook's Growth Is Fueled by Mobile Ads*, STATISTA (July 26, 2018), https://www.statista.com/chart/2496/facebook-revenue-by-segment/ (indicating that over 98% of Facebook's revenue is generated by advertising).

[31] *See Number of Monthly Active Facebook Users Worldwide as of 3rd Quarter 2018*, STATISTA (last visited __), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

[32] *But see* Alexandra Simon-Lewis, *Google Will No Longer Read Your Emails to Personalise Adverts*, WIRED UK (June 26, 2017), http://www.wired.co.uk/article/google-reading-personal-emails-privacy.

[33] *See* Frederic Lardinois, *Gmail Now Has More Than 1B Monthly Active Users*, TECHCRUNCH (Feb. 1, 2016), https://techcrunch.com/2016/02/01/gmail-now-has-more-than-1b-monthly-active-users/; Frederic Lardinois, *Google Drive Will Hit a Billion User This Week*, TECHCRUNCH (July 25, 2018), https://techcrunch.com/2018/07/25/google-drive-will-hit-a-billion-users-this-week/. *But see infra* Part III.A (challenging the notion of consumer consent to such transactions).

[34] Even government bodies, at times, enter into such transactions. *See, e.g.,* Nick Wingfield, *How Amazon Benefits From Losing Cities' HQ2 Bids*, N.Y. TIMES (Jan. 28, 2018), https://www.nytimes.com/2018/01/28/technology/side-benefit-to-amazons-headquarters-contest-local-expertise.html (discussing how municipalities supplied Amazon with vast quantities of data in exchange for the opportunity to bid to host the company's new headquarters).

[35] *See, e.g.,* Rory Cellan-Jones, *Facebook Explored Unpicking Personalities to Target Ads*, BBC NEWS (Apr. 24, 2018), http://www.bbc.com/news/technology-43869911; Youyou Wu et al., *Computer-Based Personality Judgments Are More Accurate than Those Made by Humans*, 112 PROC. NATL. ACAD. SCI. 1036 (2015).

companies can use ML to make personalized product recommendations.[36] As the Internet of Things (IoT) expands into new domains, such as autonomous vehicles and wearable tech, data-for-services transactions are likely to surge.[37] The scope of data collection is also expanding as major tech firms apply their data-driven business models to new industries.[38]

Despite privacy concerns, consumers have not, on average, reduced their consumption of services paid for with personal data.[39] Predictions that privacy breaches would discourage individuals from sharing personal data have proven false.[40] According to a Deloitte survey, while 81% of U.S. respondents felt that they had lost control over the handling of personal data relating to them, individuals' willingness to share personal data via social media has doubled in recent years.[41] These figures appear to suggest that consumers are content with data-for-services deals.[42] However, not all consumers are fully aware of the scope of data

---

[36] *See, e.g.,* Josef Adalian, *Inside the Binge Factory*, VULTURE (June 11, 2018), http://www.vulture.com/2018/06/how-netflix-swallowed-tv-industry.html (explaining how Netflix's access to viewer data has enabled it to better predict viewer habits and cater for niche viewer markets); Jesse Damiani, *Black Mirror: Bandersnatch Could Become Netflix's Secret Marketing Weapon*, VERGE (Jan. 2, 2019), https://www.theverge.com/2019/1/2/18165182/black-mirror-bandersnatch-netflix-interactive-strategy-marketing.

[37] *See, e.g.,* Kaitlyn Tiffany, *Amazon's Smart Microwave Is a Trojan Horse*, VOX (Sept. 21, 2018), https://www.vox.com/the-goods/2018/9/21/17886682/amazon-new-smart-home-microwave-speakers-internet-of-things; Jennings Brown, *Privacy Expert Resigns from Alphabet-Backed Smart City Project Over Surveillance Concerns*, GIZMODO (Oct. 23, 2018), https://gizmodo.com/privacy-expert-resigns-from-alphabet-backed-smart-city-1829934748; James Vlahos, *Smart Talking: Are Our Devices Threatening Our Privacy?*, GUARDIAN (Mar. 26, 2019), https://www.theguardian.com/technology/2019/mar/26/smart-talking-are-our-devices-threatening-our-privacy. *See also* FEDERAL TRADE COMMISSION, CROSS-DEVICE TRACKING: AN FTC STAFF REPORT (Jan. 2017), *available at* https://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 (discussing the pooling of data across different devices); Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. (2018) (discussing the legal issues facing the IoT). *See generally* BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD (2018).

[38] *See, e.g.,* Melanie Evans & Laura Stevens, *Big Tech Expands Footprint in Health*, WALL ST. J. (Nov. 27, 2018), https://www.wsj.com/articles/amazon-starts-selling-software-to-mine-patient-health-records-1543352136; Emily Glazer et al., *Facebook to Banks: Give Us Your Data, We'll Give You Our Users*, WALL ST. J. (Aug. 6, 2018), https://www.wsj.com/articles/facebook-to-banks-give-us-your-data-well-give-you-our-users-1533564049.

[39] *See, e.g.,* Nathalie Nahai & Tomas Chamorro-Premuzic, *What Would You Pay to Keep Your Digital Footprint 100% Private?*, HARV. BUS. REV. (Dec. 12, 2017), https://hbr.org/2017/12/what-would-you-pay-to-keep-your-digital-footprint-100-private. *But see* Andrew Perrin, *Americans Are Changing Their Relationship with Facebook*, PEW RESEARCH CENTER (Sept. 5, 2018), http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/ (suggesting that 54% of adult Facebook users have adjusted their privacy settings in the past 12 months).

[40] *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2089 (2004).

[41] Gina Pingitore et al., *To Share or Not to Share: What Consumers Really Think About Sharing Their Personal Information*, DELOITTE INSIGHTS (Sept. 5, 2017), https://www2.deloitte.com/insights/us/en/industry/retail-distribution/sharing-personal-information-consumer-privacy-concerns.html. *See also Trends in Customer Trust: The Future of Personalization, Data, and Privacy in the Fourth Industrial Revolution*, SALESFORCE RESEARCH BRIEF at 7 (Sept. 6, 2018), https://www.salesforce.com/form/conf/trust-research/. *But see* Paul Hitlin, *Internet, Social Media Use and Device Ownership in U.S. Have Plateaued After Years of Growth,* PEW RESEARCH CENTER (Sept. 28, 2018), http://www.pewresearch.org/fact-tank/2018/09/28/internet-social-media-use-and-device-ownership-in-u-s-have-plateaued-after-years-of-growth/.

[42] *See* Maeve Duggan, *Privacy and Information Sharing*, PEW RESEARCH CENTER (Jan. 14, 2016), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/ (demonstrating that, in the context of social media platforms, consumers have a strong preference for services which do not incur a monetary fee. One respondent explained that "I voluntarily use a service in return for giving up some information. For example, I use Gmail for free, but I know that Google will capture some information in return. I'm fine with that.") *See also* Jessi Hempel, *The Zuckerberg Hearings Were Silicon Valley's Ultimate Debut*, WIRED (Apr. 16, 2018), https://www.wired.com/story/the-zuckerberg-hearings-were-silicon-valleys-ultimate-debut/ (former Microsoft Director of Search, Stefan Weitz, asserting that most consumers find personal data trade-offs worthwhile).

collection being carried out or how these data are being used. As a result, they may not realize the data price which they pay for the services they consume.[43] For example, few consumers understand the depth of insight which can be generated from location tracking of mobile devices.[44] In addition, consumers find it difficult to properly appreciate the value of the data they generate, particularly as there is no clear price on data. The value of data is usually determined only *after* the data are collected and processed.[45]

Consumers may also be influenced by companies which market their services as free where the price is non-monetary.[46] For example, Facebook's homepage states that Facebook is "free and always will be," suggesting that use of the platform is completely free of charge.[47] Some commentators appear to accept this questionable view.[48] Today, many consumers, including those who are cognizant of the scope and value of data collection, do not conceive of their relationships with data-driven companies as transactional. They do not *experience* the collection of personal data as a price; that companies may benefit from the data they collect is, for them, irrelevant.[49] Consumers also tend to believe that attempts to limit companies' data collection and analysis are futile. They supply personal data out of sense of resignation, not on the basis of a cost-benefit analysis comparing data price to utility.[50]

Denying that the relationships between data-driven firms and consumers are transactional is problematic for several reasons. To begin with, privacy matters to many consumers.[51] For these consumers, parting with personal data *is* paying a price. More generally, these transactions are an exchange. They involve trading one valuable resource for another.[52] In data-for-services deals, irrespective of whether consumers perceive of data as valuable or subjectively experience a disutility or cost, they do give away something valuable

---

[43] *See* Strandburg, *supra* note 28, at 131 (attributing this to, *inter alia*, unknown and potential future uses or misuses of the data collected). *See also id.* at 134–48 (discussing the ramifications of imperfect information).

[44] *See* Richard Harris, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[45] *See infra* Part II.A at 9–10.

[46] *See* European Data Protection Supervisor (EDPS), *Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content* at 7 (Mar. 14, 2017), *available at* https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf.

[47] *See* FACEBOOK (last visited __), https://www.facebook.com. *See also* FINJA, *supra* note 16 (describing itself as "a *zero cost* payment platform . . . with a mission to make payments *free*, frictionless and real time") (emphasis added); Jinyan Zang et al., *Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps*, TECH SCIENCE (Oct. 20, 2015), https://techscience.org/a/2015103001/ (revealing that many "free" mobile apps share personal, behavioral, and location data with third parties).

[48] *See* ANDERSON, *supra* note 20, at 9. *But see id.* at 18–20 (regarding the role of advertising). *See id.* at 24 (regarding data labor). For a recent critique, *see* John M. Newman, *The Myth of Free*, 85 GEO. WASH. L. REV. 513, 524–35 (2018) (arguing that the marginal costs of data-driven service providers are not negligible).

[49] *See* Duggan, *supra* note 42.

[50] *See* Joseph Turow, *The Tradeoff Fallacy, How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation*, ANNENBERG SCHOOL FOR COMMUNICATION, U. PENN. 1, 3–4 (2015), *available at* https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf. *See also* Joseph Turow, *Americans and Marketplace Privacy: Seven Annenberg National Surveys in Perspective*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY [hereinafter PRIVACY HANDBOOK] 151 (Jules Polonetsky et al. eds., 2018).

[51] Alessandro Acquisti et al., *The Economics of Privacy*, 52(2) J. ECON. LIT. 1, 6 (2016) (describing the psychological discomfort of revealing personal information, including in exchange for other benefits).

[52] *See* GLENN REYNOLDS, ARMY OF DAVIDS: HOW MARKETS AND TECHNOLOGY EMPOWER ORDINARY PEOPLE TO BEAT BIG MEDIA, BIG GOVERNMENT, AND OTHER GOLIATHS 158–59 (2007) (describing value as connoting an object's ability to be exchanged for another object).

(personal data) and, in exchange, receive valuable services.[53] Barter is, after all, the exchange of one valuable resource for another without money (directly) changing hands.

Admittedly, although data are valuable, it can be difficult to assign them a precise monetary price,[54] particularly because data are not fungible.[55] Nor do data have an *intrinsic* value. The value of data, like that of many other resources, is not predetermined or fixed, but a function of supply and demand.[56] It derives from organizations' willingness to collect or purchase data (such willingness itself fluctuates over time depending on the utility of the data to the organization) and individuals' willingness to supply or sell data.[57] However, personal data are perhaps different to many other valuable resources in an important way. The value of data typically materializes only after they are captured by firms which can aggregate and monetize them.[58] Privacy interests aside, data are less valuable when in the hands of consumers, who are generally unable to (best) monetize data.

Yet, it is problematic to suggest that, because the value of data only materializes later (once monetized by data collectors or aggregators), consumers do not pay a price by sharing data with service providers. Such a suggestion falsely assumes that a price is paid only where payment is either (i) valuable *prior to* its being made or (ii) valuable *to the payer*. This assumption is not always correct. Value is often context-dependent and time-sensitive.[59] The

---

[53] *See The World's Most Valuable Resource Is No Longer Oil, But Data,* ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data; *Fuel of the Future: Data is Giving Rise to a New Economy*, ECONOMIST (May 6, 2017), https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy. *Cf* Bernard Marr, *Here's Why Data Is Not the New Oil,* FORBES (Mar. 5, 2018), https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#14e256ee3aa9; Adam Schlosser, *You May Have Heard Data Is the New Oil. It's Not*, WORLD ECONOMIC FORUM (Jan. 10, 2018), https://www.weforum.org/agenda/2018/01/data-is-not-the-new-oil/; Antonio Garcia Martinez, *No, Data is Not the New Oil*, WIRED (Feb. 26, 2019), https://www.wired.com/story/no-data-is-not-the-new-oil/; Lauren Henry Scholz, *Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies*, GEO. L.J. ONLINE (forthcoming 2019).

[54] *See* LANIER, *supra* note 19, at 360. There have been many attempts to assess the value of personal data. *See, e.g.,* Ron Hirschprung et al., *A Methodology for Estimating the Value of Privacy in Information Disclosure Systems*, 61 COMPUT. HUM. BEHAV. 443 (2016); Arslan Aziz & Rahul Telang, *What Is a Digital Cookie Worth?* (Apr. 14, 2016), *available at* https://ssrn.com/abstract=2757325. *See also* POSNER & WEYL, *supra* note 22, at 243 (arguing that monetary pricing is necessary to assess the value of data).

[55] *See* Paul Sonderegger, *The Rise of Data Capital*, FORBES 1, 4–5 (Feb. 24, 2015), https://www.forbes.com/sites/oracle/2015/02/24/the-rise-of-data-capital/#54aac7a87c0c (arguing that data are non-fungible, i.e. not uniform, and non-rivalrous, i.e. they can be used more than once, but recognizing that the value of particular data decreases as they become more widely distributed). Privacy, by contrast, is a rivalrous good or right. *See also Rise of Data Capital*, ORACLE–MIT TECH. REV. 1, 2–3 (2016), http://files.technologyreview.com/whitepapers/MIT_Oracle+Report-The_Rise_of_Data_Capital.pdf (describing data as a scarce resource). In addition, although the supply of data is arguably infinite—there being no limit on the information which can be generated and recorded—the attention (or "mindshare") of prospective customers and their spending power are scarce. *See* THOMAS H. DAVENPORT, THE ATTENTION ECONOMY: UNDERSTANDING THE NEW CURRENCY OF BUSINESS (2002); TIM WU, THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS (2016).

[56] *See generally* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW § 1.1 (9th ed. 2014) (explaining that the law of demand does not apply only to goods with explicit prices and that, fundamentally, economics is about claims over scarce resources, not money *per se*). As to the issue that no *specific* data are supplied or that the data to be supplied do not presently exist, arguably what the consumer supplies is future, ongoing *access* to certain data. *See infra* Part II.C.

[57] *See id.* at § 1.2. *See also* Hoofnagle & Whittington, *supra* note 20, at 610.

[58] *See, e.g.,* Elvy, *Paying for Privacy*, *supra* note 3, at 1420; WEIGEND, *supra* note 4, at 344–348. For data aggregators, the marginal value of personal data relating to a particular individual is usually insignificant. *See* POSNER & WEYL, *supra* note 22, at 225 (citing Google Chief Economist, Hal Varian). *But see infra* note 359 (regarding the returns to scale of data).

[59] *See* Gianclaudio Malgieri & Bart Custers, *Pricing Privacy – the Right to Know the Value of Your Personal Data*, COMPUT. L. & SECURITY REV. 1, 11 (2017).

value of a resource can change from place to place and from person to person. It can ripen or deteriorate with time. A raw material may be far more valuable to a company which can process or use it to manufacture other products than to the person who initially discovers or extracts it. Nevertheless, exchanging the raw material for a different resource or asset constitutes payment. The same is true of data-for-services exchanges. Data, like raw materials, are a valuable commodity.[60] Their value is context-dependent and time-sensitive. Exchanging data for services—irrespective of whether consumers subjectively experience a price or disutility—involves a give and-take of valuable resources. Sharing personal data is, therefore, a form of payment.

We can, however, question whether data-for-services exchanges are *bilateral* transactions, that is, whether they are between only two parties. Data are often collected from,[61] and subsequently used by, multiple parties.[62] The inputs into data-driven services are aggregated from many people and may (security and privacy concerns notwithstanding) be harnessed by different organizations—regardless of whether people actually receive any services from them.[63] Nevertheless, an individual consumer may indeed supply personal data to data-driven companies and, in exchange, receive services. Yet, even this transactional paradigm has been called into question. In a thought-provoking article rejecting the idea that data collection constitutes payment, Katherine Strandburg made the following observation:

> The common analogy between online data collection for behaviorally targeted advertising and payment for purchases is seriously misleading. There is no functioning market based on exchanges of personal information for access to online products and services. In a functioning market, payment of a given price signals consumer demand for particular goods and services, transmitting consumer preferences to producers. *Data collection would serve as 'payment' . . . only if its transfer from users to collectors adequately signaled user preferences for online goods and services*.[64]

According to Strandburg, *for data collection to be considered payment, there needs to exist a market in which consumers can actively participate and, through the quantity and quality of data they supply, signal their data price preferences to service providers*. At present, as consumers are often unaware of the scope of data collection taking place, they do not experience any disutility in sharing personal data with service providers.[65] Consequently,

---

[60] *See* Julie E. Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 31 PHIL. & TECH. 213 (2018) (characterizing data as a raw material).

[61] *See Passive Data Collection*, INT'L ASSOC. PRIVACY PROFESSIONALS (last visited __), https://iapp.org/resources/article/passive-data-collection/. *See also Privacy Policy,* GOOGLE (last visited __), https://www.google.com/policies/privacy/ (distinguishing between data "you create or provide to us" and data "we collect as you use our services"); *Data Policy,* FACEBOOK (last visited __), https://www.facebook.com/full_data_use_policy (referring to "[t]hings others do and information that *they* provide about you") (emphasis added). Passive data is also sometimes referred to as "ambient data".

[62] *See supra* note 25 (regarding the transfer and sale of personal data).

[63] *See* Laura Hautala, *Shadow Profiles: Facebook Has Information You Didn't Hand Over*, CNET (Apr. 11, 2018), https://www.cnet.com/news/shadow-profiles-facebook-has-information-you-didnt-hand-over/.

[64] Strandburg, *supra* note 28, at 95 (emphasis added). *See also* Acquisti et al., *The Economics of Privacy*, *supra* note 51, at 6–7 (explaining that the data markets open to infomediaries, such as credit-reporting agencies and advertising companies, are closed to consumers).

[65] Strandburg, *supra* note 28, at 130–31, 147–48 (explaining that consumers are unable to calculate the marginal disutility of a given instance of data collection). *See id.* at 107–8 (suggesting that, in the context of advertising-based business models, data-driven companies do not directly receive additional data or value from consumers by offering them better services). Strandburg adds that consumers, at best, signal their preferences indirectly, through advertisers—the "real" customers of data-driven companies—which pay platforms to reach consumers. However, in reality, companies also collect consumer data for purposes other than advertising, such as to train AI. As the value of data for such purposes is largely independent of advertising revenue, in these contexts

they do not select among services based on data price. Nor do consumers negotiate the data price or the quality of the services provided. Data-for-services deals are usually binary "take it or leave it" offers.[66] To access the service, the consumer must supply certain personal data (namely, whatever data the service provider collects). To avoid supplying these personal data, the consumer must *altogether* refrain from using the service. It is either all or nothing.[67] For example, to access Netflix, a consumer must consent to Netflix's privacy policy and enable the data collection which it permits.[68] There is no possibility of significantly restricting data collection and, in exchange, accessing a more basic version of Netflix. Data collection is a flat fee which all users must pay, irrespective of how they (wish to) use the service.

Even where consumers can opt out of some data collection, there is presently little correlation between the data collection which consumers consent to and the quality of the services they receive. For instance, denying a mobile app (e.g., a news app) certain data collection permissions will not generally affect the services provided. A consumer could receive the very same services at a lower data price simply by restricting the data permissions. Social networking platforms face a similar issue. Different users may spend different amounts of time on a platform and use it in different ways. Heavy users may consume and post content on a daily basis. Light users may use the platform only occasionally. Clearly, not all users reap the same benefits from the platform. Yet, the platform may well subject *all* users to the *same* scope of data collection, especially if the platform collects data from users even whilst they are not accessing the platform.[69] Heavy users and light users may well pay the same data price.[70] This lack of alignment between data price and service quality is a moral hazard.[71] Service providers can unilaterally vary the data price without suffering adverse consequences. They have no incentive to limit the scope of data they extract from consumers. Companies can set arbitrary data prices and charge consumers as they see fit.

But some data-for-services transactions are different. Consider, for example, location-based friend suggestions, in which a platform makes friend suggestions based on the geographic proximity between different users.[72] This function is only available to users who enable the platform to collect location data. If a user wishes to receive these suggestions, she must allow the platform to collect location data, that is, she must pay a higher data price. Here, there is some correlation between the data price and the utility. But, then again, not all

---

advertisers' willingness to pay data-driven companies would not serve as a proxy for consumers' preferences. *See* POSNER & WEYL, *supra* note 22, at 231–2.

[66] *See* Maurice E. Stucke, *Should We Be Concerned About Dataopolies?*, 2 GEO. L. TECH. REV. 275, 289 (2018).

[67] *See* SCHNEIER, DATA AND GOLIATH, *supra* note 3, at 49–50; WEIGEND, *supra* note 4, at 229–236; 531–533; 3403–3410 (arguing that this environment of "binary choice" should be reformed).

[68] *Privacy Policy*, NETFLIX (last visited __), https://help.netflix.com/legal/privacy. *See also* Matthew Gault, *Netflix Has Saved Every Choice You've Ever Made in 'Black Mirror: Bandersnatch,'* MOTHERBOARD (Feb 12., 2019), https://motherboard.vice.com/en_us/article/j57gkk/netflix-has-saved-every-choice-youve-ever-made-in-black-mirror-bandersnatch.

[69] *See* Facebook, Inc., *Responses to the Committee on Commerce, Science, and Transportation* (June 8, 2018), https://www.commerce.senate.gov/public/_cache/files/9d8e069d-2670-4530-bcdc-d3a63a8831c4/7C8DE61421D13E86FC6855CC2EA7AEA7.senate-commerce-committee-combined-qfrs-06.11.2018.pdf (confirming that Facebook can track browsing activity after a user logs off the platform).

[70] *See* POSNER & WEYL, *supra* note 22, at 231–2. But, by sharing or consuming more content on the platform, heavy users arguably pay a higher data price than light users. However, the additional data collected from heavy users may pale in comparison to the vast quantities of data *passively* collected from heavy and light users alike. It is also possible that a heavy user may deny the platform certain data collection permissions while a light user may not. In such a case, paradoxically, the heavy user would pay a *lower* data price and enjoy *greater* utility than the light user.

[71] *See generally* Bengt Hölmstrom, *Moral Hazard and Observability*, 10 BELL J. ECON. 74 (1979).

[72] *See Privacy Policy,* WAZE (last visited __), https://www.waze.com/en/legal/privacy/ (indicating that Waze collects additional data from users who opt in to the "find friends" feature).

users who permit the collection of location data actually take advantage of location-based friend suggestions. Arguably, such users pay an inflated data price as they share location data but receive no additional benefit. They, so to speak, leave data on the table.

Strandburg is largely correct in observing that, at present, consumers cannot effectively signal their data price preferences to service providers. The scope of data collection usually has little impact on the benefits received by consumers. The relationship between the "give" and the "take" is arbitrary. However, contrary to Strandburg, the lack of correlation between data price and utility does not indicate that consumers do not pay for services with personal data. It merely indicates that they do so *in a failed market*.[73] The inability of consumers to signal their preferences does not undermine the fact that consumers exchange personal data for services. Moreover, recognizing that consumers pay for services with personal data is a prerequisite for assessing the data price and comparing it to the utility provided. Only if these transactions were more transparent would consumers be able to signal their preferences to service providers and, ultimately, participate in a more functional market.

B. Data as Labor or Capital?

In their 2018 book, *Radical Markets: Uprooting Capitalism and Democracy for a Just Society*, Eric Posner and Glen Weyl contend that personal data should be treated as a form of labor, performed by individuals for the benefit of data-driven companies. They see individual users as data producers and sellers, and not (merely) as consumers of digital services.[74] Currently, in their view, many people provide "data labor" unwittingly and for inadequate compensation.[75] Benefits accrue primarily to data collectors while individuals are dispossessed and disempowered. Posner and Weyl suggest that treating data as labor, as opposed to capital, would have several advantages. First, it would help ensure that personal data primarily benefit individuals, rather than data collectors. Second, it would incentivize users to increase the quantity and improve the quality of the data they supply, for which they would be duly compensated. Third, it would create a new class of "data jobs" and enhance labor productivity. Fourth, it would protect and renew the dignity of "data workers." Fifth, it would challenge the market power of data collectors.[76] Accordingly, they propose that individuals should organize as "data labor unions" to collectively bargain with data-driven companies and demand better "working" conditions, such a "minimum data wage."[77]

---

[73] Technically, a market failure refers to an inefficient allocation of resources. At present, personal data are not always allocated to the companies which are willing to pay the most for them (by providing the best services). In addition, given that the scope and value of data collection can change, data-for-services arrangements may be affected by uncertainty and maladaptation. *See* Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. REV. 1327, 1333–34, 42, 49 (2012).

[74] *See* POSNER & WEYL, *supra* note 22, at 208–9. *See also* Arrieta-Ibarra et al., *Should We Treat Data as Labor?*, AEA, *supra* note 26, 38–39, 41. *See also* ANDERSON, *supra* note 20, at 24; ALVIN TOFFLER, THE THIRD WAVE 11 (1980) (coining the term "prosumer"); Tiziana Terranova, *Free Labor: Producing Culture for the Digital Economy*, 18 SOCIAL TEXT 33 (2000); TREBOR SCHOLZ, DIGITAL LABOR: THE INTERNET AS PLAYGROUND AND FACTORY 15, 52–53, 151 (2013); Ben Thompson, *Data Factories*, STRATECHERY (Oct. 2, 2018), https://stratechery.com/2018/data-factories/; Chris Marsden, *Prosumer Law and Network Platform Regulation: The Long View Towards Creating Offdata*, GEO. L. TECH. REV. 376, 377 (2018).

[75] *See, e.g.,* Alana Semuels, *The Online Hell of Amazon's Mechanical Turk*, ATLANTIC (Jan. 23, 2018), https://www.theatlantic.com/business/archive/2018/01/amazon-mechanical-turk/551192/.

[76] *See* Arrieta-Ibarra et al., *Should We Treat Data as Labor?*, AEA, *supra* note 26, at 39–40.

[77] *See* Eric Posner & Glen Weyl, *Data Workers of the World, Unite!*, PROMARKET (Apr. 25, 2018), https://promarket.org/data-workers-world-unite/; POSNER & WEYL, *supra* note 22, at 241–43; Arrieta-Ibarra et al., *Should We Treat Data as Labor?*, AEA, *supra* note 26, at 41; Imanol Arrieta Ibarra et al., *Should We Treat Data as Labor?*, BROOKINGS INSTITUTE (Feb. 21, 2018), https://www.brookings.edu/blog/techtank/2018/02/21/should-we-treat-data-as-labor-lets-open-up-the-

Although Posner and Weyl are correct to observe that data-for-services transactions do not currently compensate users in proportion to the quantity or quality of data they supply,[78] the notion of "data as labor" faces several issues. First, it is somewhat misleading to assert that consumers do not receive a share in the value created by the data they supply.[79] Consumers receive valuable (and often cutting edge) services in exchange for data. Second, the analogy between data and labor is questionable as data are mostly supplied passively or inadvertently, while labor implies work which individuals perform consciously and actively.[80] Third, it is foreseeable that data-driven companies may fail to meet the demands of data unions (if established) and thereby lose access to valuable data necessary for future innovation.[81]

In addition, Posner and Weyl do not critically analyze the notion of data as capital, the supposed counterpoint to data as labor. Instead, they use data as capital as a catch-all label for all things problematic in data-for-services transactions and the data economy more generally. They do not engage with "capital" as traditionally defined, that is, as an input or resource (e.g., equipment, structure, etc.) used in the production of goods or services. Moreover, treating data as capital does not necessarily imply that data belong to data collectors.[82] Nor does it imply that data-for-services transactions must remain opaque and primarily benefit data-driven companies. In fact, if data were treated as capital supplied *by consumers*, consumers could better grasp the concept of the exchange underpinning these transactions. But concerns with classifying data as labor do not themselves suggest that data should be classified as capital. Nevertheless, there is support for treating data as a form of capital, an intangible asset that can be used in the production of digital and other services.[83]

Although the data-as-labor—data-as-capital debate is useful in placing a spotlight on the value of data, many issues do not actually hinge on whether data are classified as labor or as capital. However classified, the data which people routinely supply to service providers are valuable. Debating whether data should be treated as labor or capital or fall within some other economic category is helpful only in so far as it can inspire different courses of action.[84] If data are treated as labor then data unions may emerge. If data are treated as capital then individuals may have property rights in data.[85] Yet, analogizing data to familiar categories can inhibit our creativity in imagining and implementing new approaches. Although these analogies can help consumers understand and optimize the data-for-services transactions they enter, they also have the potential to obstruct novel conceptions of, and innovative responses to, the economic function of personal data.

---

discussion/. *See also* Toby Sterling & Alexandra Hudson, *Facebook Users Unite! 'Data Labour Union' Launches in Netherlands*, REUTERS (May 23, 2018), https://www.reuters.com/article/us-netherlands-tech-data-labour-union/facebook-users-unite-data-labour-union-launches-in-netherlands-idUSKCN1IO2M3; THE DATA UNION (last visited __), https://www.thedataunion.eu/; *Data Workers of the World, Unite: What If People Were Paid for Their Data?,* ECONOMIST (July 7, 2018), https://www.economist.com/the-world-if/2018/07/07/what-if-people-were-paid-for-their-data (suggesting that CitizenMe and Datacoup are early forms of data unions); *Data as Labor: Implementations*, RADICAL MARKETS (last visited __), http://radicalmarkets.com/chapters/data-as-labor/implementations/ (containing a rolling list of implementations of data as labor).

[78] *See* POSNER & WEYL, *supra* note 22, at 236; Arrieta-Ibarra et al., *Should We Treat Data as Labor?*, AEA, *supra* note 26, at 39. *See also* Mary L. Gray & Siddharth Suri, *The Humans Working Behind the AI Curtain*, HARV. BUS. REV. (Jan. 9, 2017), https://hbr.org/2017/01/the-humans-working-behind-the-ai-curtain.

[79] *See* Arrieta-Ibarra et al., *Should We Treat Data as Labor?*, BROOKINGS, *supra* note 77.

[80] *See supra* note 61 (regarding passive data collection). *But see* Semuels, *supra* note 75.

[81] *See Digital Proletariat*, ECONOMIST, *supra* note 22.

[82] *Cf* Arrieta-Ibarra et al., *Should We Treat Data as Labor?*, BROOKINGS, *supra* note 77.

[83] *See Rise of Data Capital*, ORACLE & MIT, *supra* note 55, at 3.

[84] *See generally* Scholz, *Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies*, *supra* note 53.

[85] *See infra* Part III.C.

C. Consumer Apathy and Behavioral Biases

According to the theory of bounded rationality, decision making is constrained by available information and people's cognitive capacities.[86] In the context of data-for-services transactions, consumers often lack vital information regarding the scope of data collection, the risks it entails and its commercial value.[87] Consumers do not have the tools to quantify the utility of the services they receive or compare this to the value of the data they supply. As a result, data-for-services transactions are opaque. Service providers and data collectors typically have far more information.[88] Unlike consumers, they are acutely aware of the scope of collection, use and value of personal data. This information asymmetry places consumers and companies in radically different bargaining positions.[89] Data-driven companies can dictate to consumers the terms of data-for-services transactions.

The situation is exacerbated by the fact that many companies do not charge fees for the services they provide. The "free" price-tag is a powerful marketing tactic, which implies that no price whatsoever is extracted from consumers.[90] It entices consumers to blindly accept each and every data-for-services deal.[91] Moreover, where the price of services is non-monetary, consumers do not experience the so-called "pain of paying."[92] As a result, they overlook the data price which they pay.[93] By altogether refraining from engaging in a cost-benefit analysis, consumers tend to overvalue the services which they receive.[94]

---

[86] *See* HERBERT A. SIMON, MODELS OF MAN, SOCIAL AND RATIONAL: MATHEMATICAL ESSAYS ON RATIONAL HUMAN BEHAVIOR IN A SOCIAL SETTING (1957); HERBERT A. SIMON, MODELS OF BOUNDED RATIONALITY: EMPIRICALLY GROUNDED ECONOMIC REASON (1982).

[87] *See* Alessandro Acquisti et al., *Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online*, 50 ACM COMPUT. SURV. 1, 4 (2017).

[88] *But see, e.g.,* GDPR, *infra* note 154, at arts. 12–14 (granting data subjects certain information rights).

[89] *See* SCHNEIER, DATA AND GOLIATH, *supra* note 3, at 195; Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1883–86 (2013). *See generally* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488 (1970). There also exists a collective action problem. While a data-driven company can reap enormous benefits from personal data collected and aggregated *en masse*, the individual consumer does not typically experience any disutility in supplying personal data and will therefore have little incentive to demand more favorable data-for-services deals. *See generally* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION (1965).

[90] *See* Hoofnagle & Whittington, *supra* note 20, at 635, 648; David Adam Friedman, *Free Offers: A New Look*, 38 N.M. L. REV. 49, 68–69 (2008); Kristina Shampanier et al., *Zero as a Special Price: The True Value of Free Products*, 26 MARKETING SCI. 742, 753–54 (2007). *See also* Josh Kopelman, *The Penny Gap*, REDEYE VC (Mar. 10, 2007), http://redeye.firstround.com/2007/03/the_first_penny.html.

[91] *See* Natali Helberger et al., *The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law*, 54 COMMON MKT. L. REV. 1427, 1442–44 (2017) (suggesting that portraying a product as free where it is paid for with personal data may be considered misleading under EU consumer law).

[92] *See* Dan Ariely, *The Pain of Paying* (Feb. 5, 2013), http://danariely.com/2013/02/05/the-pain-of-paying/. *See also* Drazen Prelec & George Loewenstein, *The Red and the Black: Mental Accounting of Savings and Debt*, 17 MARKETING SCI. 4 (1998). *But see* Nina Mazar et al., *Pain of Paying?—A Metaphor Gone Literal: Evidence from Neural and Behavioral Science* (Rotman School of Management Working Paper, Apr. 26, 2017), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2901808.

[93] *See* DANIEL KAHNEMAN, THINKING, FAST AND SLOW 24 (2011) (explaining that people tend to be blind to the obvious, and to their blindness). *But see* Teppo Felin, *The Fallacy of Obviousness*, AEON (July 5, 2018), https://aeon.co/essays/are-humans-really-blind-to-the-gorilla-on-the-basketball-court (positing that such blindness is a feature, not a bug). Accordingly, such blindness may actually allow people to enjoy digital services in a more carefree manner. *See also* Dan Ariely, *The Pain of Paying*, *supra* note 92 (suggesting that consumers should sometimes take steps to reduce their pain of paying in order to enjoy certain goods and services guilt-free, such as booking all-inclusive holiday packages). *See also* Richard H. Thaler, *Mental Accounting Matters*, 12 J. BEHAV. DECIS. MAKING 183, 192 (1999) (regarding payment decoupling).

[94] *See* DAN ARIELY, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS 54–65 (2008).

Consumer behavior in this context can be explained by specific cognitive and behavioral biases.[95] Alessandro Acquisti has identified several systemic errors in judgment which impact consumers' decisions with respect to personal data.[96] Although these studies focused specifically on privacy, their findings can be harnessed to shine light on data-for-services transactions. The main findings are as follows:

> *Framing effects* — As the benefits (services) which consumers receive are communicated upfront, while the costs (data collection) are not, consumers tend to have an overly positive perception of data-for-services transactions.[97] They contemplate the utility they gain but neglect the personal data they supply.
>
> *Hyperbolic discounting* — Data-for-services transactions are structured as "buy now, pay later" offers.[98] The short-term (or immediate) benefits of, for example, a social media experience, can divert consumers' attention away from the longer-term costs of sharing personal data.[99]
>
> *Loss aversion* — The more consumers feel in control of personal data, the more they value them.[100] Hence, in data-for-services transactions, where consumers do not feel in control of the personal data they supply, they usually undervalue those data.
>
> *Availability heuristic* — Consumers find it difficult to tangibly envisage or fully understand the costs associated with data-for-services transactions, such as downstream data security risks, and consequently ignore them.[101]
>
> *Status quo bias* — As with other transactions, consumers are inclined to accept the status quo and default choices of data-for-services deals. They do not question or negotiate the terms offered to them by data-driven companies or seek to propose alternative arrangements.[102]
>
> *Herd mentality* — Consumers usually conform to the choices of other consumers, rather than make individual decisions.[103] In the context of data-for-services transactions, different consumers tend to purchase similar (if not identical) services and strike similar deals with data-driven companies.

---

[95] *See generally* RICHARD H. THALER, MISBEHAVING (2016); Richard Thaler, *Toward a Positive Theory of Consumer Choice*, 1 J. ECON. BEHAV. & ORG. 39 (1980) (harnessing the findings of Kahneman and Tversky to demonstrate that, contrary to rational choice theory, consumers (and people generally) are not consistent or effective utility-maximizers). *See also* Solove, *Privacy Self-Management*, *supra* note 89, at 1886–88.

[96] *See* Acquisti et al., *Nudges*, *supra* note 87, 5ff.

[97] *See* Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, 4 Soc. PSYCHOL. PERS. SCI. 340 (2013). *See generally* Amos Tversky & Daniel Kahneman, *The Framing of Decisions and the Psychology of Choice*, 211 SCIENCE 453 (1981).

[98] *See* Strandburg, *supra* note 28, at 150; Hoofnagle & Whittington, *supra* note 20, at 649.

[99] *See Creepy or Cool? Staying on the Right Side of the Consumer Privacy Line*, KPMG at 20 (2016), https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/creepy-or-cool.pdf (discussing, in addition, the overconfidence and optimism biases).

[100] *See* Jens Grossklags & Alessandro Acquisti, *When 25 Cents Is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*, WEIS ECON. INFO. SECURITY 1 (2007); Alessandro Acquisti et al., *What Is Privacy Worth*?, 42 J. LEGAL STUD. 249 (2013). *See also* Thaler, *Toward a Positive Theory of Consumer Choice*, *supra* note 95, at 43 (coining the term "endowment effect").

[101] *See generally* Amos Tversky & Daniel Kahneman, *Judgment under Uncertainty Heuristics and Biases*, 185 SCIENCE 1124, 1127 (1974) (describing the bias of imaginability, according to which people overlook dangers which are difficult to conceive of or unlikely to come to one's attention.)

[102] *See, e.g.,* Hana Habib et al., *An Empirical Analysis of Website Data Deletion and Opt-Out Choices*, WORKSHOP ON GDPR: AN OPPORTUNITY FOR THE HCI COMMUNITY? (Apr. 2018). *See generally* Daniel Kahneman et al., *Experimental Tests of the Endowment Effect and the Coase Theorem*, 98 J. POL. ECON. 1325, 1342–46 (1990); Russell Korobkin, *Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms*, 51 VAND. L. REV. 1583, 1587–92 (1998).

[103] *See* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 53ff (2008); Alessandro Acquisti et al., *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015) (discussing the pressure to conform to the social norms of data sharing).

These biases help explain consumers' apathy with respect to the data prices which they pay. However, to date, researchers have conspicuously failed to apply a key behavioral insight to these decisions. According to Richard Thaler, in every transaction consumers can gain two different types of utility: *acquisition utility* and *transaction utility*.[104] The former relates to the value of a product or service relative to its price; the latter relates to the perceived merits of a deal, that is, the price paid for a product or service relative to its reference price (i.e., what one would expect to pay for it). In Thaler's classic experiment, the individuals surveyed (in the early 1980s) were, on average, willing to pay far more for a beer in a fancy hotel ($2.65) than in a grocery store ($1.50).[105] The explanation for this difference is that while paying $2.65 for a beer is an expected nuisance in the fancy hotel (all hotels presumably charge exorbitant prices for beer), it would be excessive in the grocery store (where the expected price is far lower). The willingness to pay different prices for the same product in different contexts suggests that consumers appear to be more concerned by transaction utility than acquisition utility.[106] They care less about the value of a product or service relative to its price and more about the perceived merits of the deal, that is, the price paid relative to the reference price, which is context-dependent. Even where there are little or no monetary savings, consumers tend to (unconsciously) attach great importance to the way they *experience* the outcomes of transactions.[107] This mental accounting involves many psychological factors, such as perceptions of fairness.[108]

In light of these findings, one would expect that in data-for-services transactions (i) the pursuit of acquisition utility would prompt consumers to seek to maximize the utility of the services they receive relative to the data price they pay and (ii) the pursuit of transaction utility would prompt consumers to compare the data price they pay for a given service to the expected or ordinary data price payable for such a service. However, consumers do *neither* of these things. Consumers do not have the tools to quantify the utility they receive or the data price they pay. As a result, consumers cannot compare competing data-for-services deals to seek out the lowest price and the maximum utility. They cannot scrutinize data-for-services transactions in the same way they scrutinize other transactions. Consequently, consumers are largely indifferent to the data price they pay and the precise benefits they receive.

Importantly, many firms are familiar with these behavioral insights. They can exploit consumers' apathy to nudge them into sharing greater quantities of more valuable personal data.[109] By not demanding monetary payment for many of the services they offer, companies

---

[104] *See* Richard H. Thaler, *Mental Accounting and Consumer Choice*, 4 MARKETING SCI. 199, 205–10 (1985); Thaler, *Mental Accounting Matters*, *supra* note 93, at 188–89. *See also* Daniel Kahneman, *New Challenges to the Rationality Assumption*, 150 J. INST. & THEOR. ECON. 18, 21 (1994) (distinguishing between experienced utility and decision utility).

[105] *See id.*

[106] Transaction utility perhaps explains the success of businesses' price comparison strategies. *See* Dhruv Grewal at al., *The Effects of Price-Comparison Advertising on Buyers' Perceptions of Acquisition Value, Transaction Value, and Behavioral Intentions*, 62 J. MARKETING 46 (1998).

[107] *See* Daniel Kahneman & Amos Tversky, *Choices, Values and Frames*, 39 AM. PSYCH. 341, 341–42, 348, 349 (1984). *Compare* GEORGE J. STIGLER, THE THEORY OF PRICE (3d ed. 1966) (describing the traditional economic view according to which consumers are rational agents and effective utility-maximizers).

[108] *See generally* GEORGE AKERLOF & ROBERT SHILLER ANIMAL SPIRITS: HOW HUMAN PSYCHOLOGY DRIVES THE ECONOMY, AND WHY IT MATTERS FOR GLOBAL CAPITALISM ch. 2 (2009); Robert M. Schindler, *The Excitement of Getting a Bargain: Some Hypotheses Concerning the Origins and Effects of Smart-Shopper Feelings*, 16 ADVANCES IN CONSUMER RESEARCH 447 (1989); Lan Xia et al., *The Price Is Unfair! A Conceptual Framework of Price Fairness Perceptions*, 68 J. MARKETING 1 (2004); Peter R. Darke & Darren W. Dahl, *Fairness and Discounts: The Subjective Value of a Bargain*, 13 J. CONSUMER PSYCH. 328 (2003); Hyunjoo Im & Yong Ha, *Is This Mobile Coupon Worth My Private Information? Consumer Evaluation of Acquisition and Transaction Utility in a Mobile Coupon Shopping Context,* 9 J. RES. INTERACTIVE MARKETING 92 (2015).

[109] *See, e.g.,* Christoph Bösch et al., *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, 4 PROC. PRIVACY ENHANCING TECH. 237 (2016) (discussing companies' deliberate efforts to avoid

can conceal the data costs which consumers pay and, at the same time, magnify the benefits they receive.[110] For now, consumers are mostly resigned to the terms set by data-driven service providers.[111] They do not see these relationships as transactions.[112] In the absence of tools to effectively assess the data price and utility, consumers cannot—and thus do not—scrutinize data-for-services deals. The privacy paradigm, although consumer-oriented, obstructs efforts to increase transactional transparency and, consequently, reinforces consumer apathy.[113]

D. The Return on Data Paradigm

Despite this sense of resignation, the collection of personal data by tech firms continues to prompt vigorous debate and raise many questions. Should data collection be regulated? If so, how and by whom? What rights do consumers have in personal data relating to them? These and other important questions revolve around *protecting* personal data. They focus on privacy. According to a Pew survey, 80% of social media users are concerned about advertisers and businesses accessing the data which they share,[114] while 83% of users support tougher privacy regulation.[115] Yet, despite the pervasive lack of trust in social media platforms,[116] social media usage continues to rise.[117] Nearly seven out of ten Americans use social media platforms,[118] which invariably collect vast amounts of personal data. While some consumers take steps to protect their privacy,[119] the overwhelming trend is to continue to pay for services with personal data. Data-for-services transactions are flourishing even in the face of privacy concerns.

According to the so-called "privacy paradox," consumers assert that they want privacy but behave as if they do not.[120] They insist on the importance of privacy, but opt to exchange personal data for services. How can this be explained? If data collection is simply

---

making privacy salient, causing consumers to undervalue privacy). *See also* Jeremy B. Merrill & Ariana Tobin, *Facebook Moves to Block Ad Transparency Tools — Including Ours*, PROPUBLICA (Jan. 28, 2019), https://www.propublica.org/article/facebook-blocks-ad-transparency-tools.

[110] *See* SCHNEIER, DATA AND GOLIATH, *supra* note 3, at 50.

[111] *See* Turow, *The Tradeoff Fallacy*, *supra* note 50.

[112] *See* Arrieta-Ibarra et al., *Should We Treat Data as Labor?*, BROOKINGS, *supra* note 77. *See also* Whittington & Hoofnagle, *supra* note 73, at 1343–44 (regarding the mutual dependence between consumers and data-driven service providers).

[113] *See generally* S. J. Liebowitz & Stephen E. Margolis, *The Fable of the Keys*, 33 J.L. & ECON. 1 (1990); S. J. Liebowitz & Stephen E. Margolis, *Path Dependence, Lock-in, and History*, 11 J.L. ECON. & ORG. 205 (1995).

[114] Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RESEARCH CENTER (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/. *See also* Justin McCarthy, *Worried About Personal Data Top Facebook Users' Concerns*, GALLUP (Apr. 12, 2018), https://news.gallup.com/poll/232343/worries-personal-data-top-facebook-users-concerns.aspx.

[115] *See Inaugural Tech Media Telecom Pulse Survey,* HARRISX at 4, 10 (Apr. 2018), http://harrisx.com/wp-content/uploads/2018/04/Inaugural-TMT-Pulse-Survey_-20-Apr-Final.pdf.

[116] *See id.* at 21; Salesforce, *supra* note 41, at 4.

[117] *But see* Kurt Wagner & Rani Molla, *First Time to Spend Less Time on FB, But Arguably More Meaningful Time*, RECODE (Jan. 31, 2018), https://www.recode.net/2018/1/31/16956826/facebook-mark-zuckerberg-q4-earnings-2018-tax-bill-trump.

[118] *See* Rainie, *supra* note 114. *See also* John Gramlich, *8 Facts about Americans and Facebook*, PEW RESEARCH CENTER (Oct. 24, 2018), http://www.pewresearch.org/fact-tank/2018/10/24/facts-about-americans-and-facebook/.

[119] *See* Perrin, *supra* note 39.

[120] *See* Idris Adjerid et al., *The Paradox of Wanting Privacy But Behaving as if It Didn't Matter*, LSE BUS. REV. (Apr. 19, 2018); Idris Adjerid et al., *Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making*, 42 MGMT. INFO. SYS. Q. 465 (2018). *See also* Solove, *Privacy Self-Management*, *supra* note 89, at 1886.

the price of certain services, why are consumers (apparently) reluctant to pay? Data-for-services transactions are, after all, a mutual exchange. Consumers supply data and receive services. Yet, the discourse relating to personal data addresses only what consumers *give*. It overlooks the utility which consumers gain in return for the data they supply, and fails to examine the relationship between the data price paid and the utility gained. These important issues are overshadowed by privacy concerns.[121]

This fixation on privacy has been dubbed a "pessimism problem."[122] Public and scholarly attention is directed toward the risks of data collection, not its benefits or the opportunities it creates. For example, industry indices and public surveys relating to the data economy are primarily concerned with privacy.[123] Law reviews examine the interaction of technology and privacy,[124] while economists advocate nudging people towards protecting personal data.[125] Company data policies are described as "privacy policies,"[126] data law as "privacy law."[127] From industry to academia, the privacy paradigm is dominant. Even if we acknowledge that consumers do not give away personal data for free, we pay little (if any) attention to the utility which consumers gain in return for the personal data they supply.[128]

Andreas Weigend, former Amazon Chief Scientist, suggests that the debate needs to change direction. He proposes engaging an alternative analytical apparatus—*return on data (ROD)*—which adapts the idea of return on investment (ROI) to the data economy.[129] According to ROI, when gauging the profitability of an investment, a business should consider not only the outlay of an investment (capital, labor, etc.), but also its (expected) gains. ROI equals the benefit of an investment divided by the cost of an investment.[130] Notwithstanding its limitations, ROI is a convenient, if rudimentary, measure of profitability, and can be applied to a wide range of activities. ROD is modeled on the classic ROI formula. It aims to help data-driven businesses measure the benefits of particular data relative to the cost of those data (their collection, storage, use, etc.), and equals the benefit of those data divided by their cost.[131]

---

[121] *See, e.g.,* Allison S. Bohm et al., *Privacy and Liberty in an Always-On, Always-Listening World*, 19 COLUM. SCI. & TECH. L. REV. 1 (2017) (examining data-collecting technologies primarily through the lens of privacy); Sheri B. Pan, *Get to Know Me: Protecting Privacy and Autonomy Under Big Data's Penetrating Gaze*, 30 HARV. J.L. & TECH. 239 (2016); Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 BERKELEY TECH. L.J. 997, 1013 (2016) (focusing on the privacy impacts of the IoT). *But see* Stucke, *supra* note 66, at 287 (describing data collection as a price.)

[122] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 441 (2016).

[123] *See, e.g., 2018 Corporate Accountability Index*, RANKING DIGITAL RIGHTS (last visited __), https://rankingdigitalrights.org/index2018/categories/privacy/; *Computers and the Internet: Historical Trends*, GALLUP (Sept. 2018), https://news.gallup.com/poll/1591/computers-internet.aspx. *See also Privacy,* ELECTRONIC FRONTIER FOUNDATION (last visited __), https://www.eff.org/issues/privacy.

[124] *See e.g., The Privacy Paradox: Privacy and Its Conflicting Values*, 64 STAN. L. REV. ONLINE (2012); *Privacy & Technology Symposium*, 126(7) HARV. L. REV. (2013); *Law, Privacy & Technology Commentary Series*, 130 HARV. L. REV. F. (2016); *The Problem of Theorizing Privacy*, 20(1) THEOR. INQ. L. (2019). *See also* INT'L DATA PRIVACY LAW, an OUP peer-reviewed journal dedicated to data protection.

[125] *See especially* Acquisti et al., *Nudges*, *supra* note 87.

[126] *See infra* Part III.A.

[127] *See, e.g.,* DANIEL J. SOLOVE & PAUL H. SCHWARTZ, INFORMATION PRIVACY LAW (6th ed. 2018).

[128] *See, e.g.,* Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 3 (2018) (recognizing data-for-services transactions but advocating extensions of Balkin's *privacy* proposals). *See* Balkin, *infra* note 166.

[129] *See* WEIGEND, *supra* note 4, at 3131–3135; 3193–3198. *See also* Sparapani, *supra* note 19, at 1318 (referring to a data-for-value equation).

[130] *See Return on Investment (ROI)*, INVESTOPEDIA (last visited __), https://www.investopedia.com/terms/r/returnoninvestment.asp.

[131] *See* Dorian Selz, *Return on Data*, SQUIRRO (Jan. 20, 2016), https://squirro.com/2016/01/20/return-on-data/. Most references to ROD address only the service provider's perspective, i.e. business strategies for best utilizing

But, for consumers in data-for-services transactions, ROD has a different meaning.[132] Where consumers pay for services with personal data, the benefit they receive is the utility of certain services; the price is the value of the data they supply. Therefore, this article proposes that—*in data-for-services transactions, ROD is the relationship between the utility (U) consumers gain and the data (D) they supply. Expressed as a ratio, ROD = U / D*. The higher the ROD ratio, the better the deal for the consumer. The lower the ROD ratio, the worse the deal for the consumer. Although it may be very difficult to calculate, ROD sends a powerful message. Just as businesses can quantitatively assess the data investments they make, consumers should be able to meaningfully evaluate the data-for-services transactions they enter. For consumers to make better informed decisions, they need to be able to determine whether or not a deal is in their best interests.[133]

ROD, as an analytical apparatus, is likely to appeal to consumers. In a Deloitte survey of 8,500 consumers across Canada, Chile, Germany, Japan, the U.K. and the U.S., in each of the countries respondents were more willing to share personal data when they received something valuable in exchange.[134] In other words, consumers took interest in the *returns* on the data they supplied. In fact, 79% of respondents were only willing to share personal data if they clearly understood the benefits they were to receive.[135] The idea of ROD is also likely to resonate with commentators who have called on data-driven service providers to offer consumers more favorable data-for-services deals.[136] Yet, at present, the relationship between data price and services remains largely unknown. Perhaps consumers tend to get good deals. Perhaps they are being shortchanged. Data-for-services transactions, although pervasive, are currently under-scrutinized and unscrutinizable. Pivoting away from the privacy paradigm and developing tools to assess ROD is a step in the right direction.

III. LEGAL FRAMEWORKS

Most legal frameworks which govern data-for-services transactions are preoccupied with privacy. Privacy policies focus on the personal data which consumers supply and how these data are used. They overlook the relationship between these data and the benefits which consumers receive. Privacy law in both the United States and the EU aims to protect personal data, not to evaluate the data price which consumers pay relative to the utility they receive. Even proposals to establish property rights in personal data are privacy-centric. With the possible exception of an EU proposal recognizing that the collection of personal data constitutes a form of payment, none of these legal frameworks examines what consumers receive in exchange for the data they supply.

---

consumer data. *See, e.g.*, Brad Brown et al., *Capturing Value from Your Customer Data*, MCKINSEY (Mar. 2017), https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/capturing-value-from-your-customer-data. The benefit of data, also described as the value of information (VoI), may itself be calculated as the (expected) utility from decisions made given the data in question, minus the (expected) utility from decisions made without the data in question.

[132] *See infra* Part V.A.

[133] *See* WEIGEND, *supra* note 4, at 3131–3139; 3142–3146.

[134] *See* Pingitore et al., *supra* note 41.

[135] *Id.*

[136] *See, e.g.,* Nahai & Chamorro-Premuzic, *supra* note 39.

A. Terms of Service and Privacy Policies

There are generally two documents which govern the relationship between a consumer and a data-driven service provider: the terms of service and privacy policy.[137] Typically, the terms of service contain a variety of conditions while privacy policies describe the types of personal data collected and how these are used.[138] As far as ROD is concerned, both documents are problematic. Each document addresses only one aspect of data-for-services transactions: terms of service relate to the services provided while privacy policies relate to the data collected. Terms of service address what consumers *get*. Privacy policies address what consumers *give*.[139] By separating the data price which consumers pay from the utility which they receive, these documents decouple data price from utility and, in doing so, implicitly deny that a mutual exchange takes place.

However, the terms of service and privacy policies of certain companies do seem to recognize that consumers pay for services with personal data. Instagram's terms of service provide that each user grants to the platform a "fully paid" license to exploit the user's content.[140] According to one commentator, as Instagram users are not required to pay money to use Instagram's services, the expression "fully paid" suggests that users make a non-monetary payment in order to access the services, presumably in the form of personal data.[141] Meanwhile, some privacy policies explicitly state that the services provided are supported by advertising.[142] Whilst such statements do not quite imply data-for-services barter, they do allude to the underlying data-driven business model.

In reality, consumers have almost no influence over the terms of service and privacy policies which govern the services they use. These documents are "take it or leave it" contracts of adhesion. If, for example, a consumer wishes to install a mobile app, she must consent to the terms. Understandably, the average consumer does not bother reading them.[143]

---

[137] Terms of service are also known as conditions or terms of use and shrink, clickwrap or browsewrap licenses. *See, e.g.,* Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 460 (2006).

[138] *See, e.g., Google Privacy Policy*, *supra* note 61; *Facebook Data Policy*, *supra* note 61; *WhatsApp Legal Info,* WHATSAPP (last visited __), https://www.whatsapp.com/legal/; *Privacy Notice*, AMAZON (last visited __), https://www.amazon.com/gp/help/customer/display.html/ref=asus_gen_not?ie=UTF8&nodeId=468496&ld=ASUSGeneralDirect. Some privacy policies explain the reasons why certain data are collected. *See, e.g., Privacy Policy*, SNAP (last visited __), https://www.snap.com/en-US/privacy/privacy-policy/; *Waze Privacy Policy*, *supra* note 72. Notably, despite being owned by larger companies, Instagram, WhatsApp and Waze all have their own terms of service and privacy policies. *But see* Mike Isaac, *Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger*, N.Y. TIMES (Jan. 25, 2019), https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html. *See also* Mark Zuckerberg, *A Privacy-Focused Vision for Social Networking*, FACEBOOK (Mar. 6, 2019), https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/.

[139] *See* SCHNEIER, DATA AND GOLIATH, *supra* note 3, at 1 (recognizing that there is no single contract governing the bargain). Notably, Viber separates into two different documents the terms governing data collection and the terms governing monetary payment. *See Privacy Policy,* VIBER (last visited __), https://www.viber.com/terms/viber-privacy-policy/; *Payments Policy*, VIBER (last visited __), https://www.viber.com/terms/viber-payments-policy/.

[140] *Terms of Use*, INSTAGRAM (last visited __), https://help.instagram.com/478745558852511.

[141] Malgieri & Custers, *Pricing Privacy*, *supra* note 59, at 6.

[142] *See, e.g., Privacy Policy*, TWITTER (last visited __), https://twitter.com/en/privacy.

[143] *See, e.g.,* Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, BUS. INSIDER (Nov. 15, 2017), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 (revealing that over 90% of consumers accept terms of service without reading them); Yannis Bakos et al., *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1 (2014). *See also* Joseph Turow et al., *Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies, 2003–2015*, 62 J. BROADCAST. ELECTRON. 461 (2018).

These documents can be (deliberately) long, legalistic and difficult to understand.[144] As a result, consumers are not generally familiar with the terms on which they transact with service providers.[145]

Nevertheless, consumers increasingly depend on the technologies which data-driven companies provide. Although there exist alternatives to Google Chrome and Google Search which do not involve data collection, such as the Brave browser and DuckDuckGo search engine, these are not necessarily adequate substitutes.[146] We cannot expect consumers to refrain from using technologies provided by data-driven companies. "Exiting" Google or Facebook is not generally straightforward (or even possible).[147] Cryptographer and security technologist Bruce Schneier explained that:

> It's not reasonable to tell people that if they don't like the data collection, they shouldn't e-mail, shop online, use Facebook, or have a cell phone. . . .These are the tools of modern life. They're necessary to a career and a social life. Opting out just isn't a viable choice for most of us, most of the time . . .[148]

Data-driven companies control the terms of data-for-services transactions.[149] Consumers cannot realistically negotiate the data price or demand higher ROD. Due to consumers' dependence on these technologies and the information asymmetry between consumers and companies, some commentators have called into question the authenticity of consumers' consent to these transactions.[150] Consent, they suggest, is *presumed* or

---

[144] *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 97 (2013); Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39 (2015); Shmuel I. Becher & Uri Benoliel, *The Duty to Read the Unreadable*, 60 B.C. L. REV. (forthcoming 2019); *How Silicon Valley Puts the 'Con' in Consent*, N.Y. TIMES (Feb. 2, 2019), https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html. *But see, e.g., Google Privacy Policy*, *supra* note 61 (exemplifying a trend towards more readable consumer-oriented documents). *See also* OECD, *Big Data: Bringing Competition Policy to the Digital Era: Background Note by the Secretariat*, at 25, DAF/COMP(2016)14 (Apr. 26, 2017), https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf; Florian Schaub et al., *A Design Space for Effective Privacy Notices*; Mary J. Culnan & Paula J. Bruening, *Privacy Notices: Limitations, Challenges, and Opportunities*, *in* PRIVACY HANDBOOK, *supra* note 50, at 365, 524.

[145] *Cf* WEIGEND, *supra* note 4, at 921–922 (suggesting that most Gmail users *consciously* exchange data for free email). *See also* John D. McKinnon & Douglas MacMillan, *Google Says It Continues to Allow Apps to Scan Data from Gmail Accounts*, WALL ST. J. (Sept. 20, 2018), https://www.wsj.com/articles/google-says-it-continues-to-allow-apps-to-scan-data-from-gmail-accounts-1537459989.

[146] *See, e.g.,* James Frew, *DuckDuckGo vs. Google: The Best Search Engine for You*, MAKE USE OF (Apr. 20, 2018), https://www.makeuseof.com/tag/duckduckgo-vs-google-search-engine/; *Chrome vs Brave Detailed Comparison as of 2018*, SLANT (last visited__), https://www.slant.co/versus/2550/16094/~chrome_vs_brave.

[147] *See* Kashmir Hill, *Life Without the Tech Giants*, GIZMODO (Jan. 22, 2019), https://gizmodo.com/life-without-the-tech-giants-1830258056; Hamza Shaban, *Facebook Literally Can't Be Deleted on Some Phones*, WASH. POST (Jan. 9, 2019), https://www.washingtonpost.com/technology/2019/01/09/facebook-literally-cant-be-deleted-some-phones/.

[148] SCHNEIER, DATA AND GOLIATH, *supra* note 3, at 60–61. *See id.* at 57–59.

[149] *See* Stucke, *supra* note 66, at 289 (explaining that consumers have no viable alternative to consenting). *See also* Bruce Schneier, *You Have No Control Over Security on the Feudal Internet*, HARV. BUS. REV. (June 6, 2013), https://hbr.org/2013/06/you-have-no-control-over-s; POSNER & WEYL, *supra* note 22, at 231 (discussing "technofeudalism"); *Data Workers of the World, Unite, supra* note 77 (discussing "data slavery").

[150] *See* Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 68 (2012). Notably, the GDPR relies heavily on consent. *See, e.g.,* GDPR, *infra* note 154, at rec. 31. *See also* Scott Berinato, *"Stop Thinking About Consent: It Isn't Possible and It Isn't Right"*, HARV. BUS. REV. (Sept. 24, 2018), https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right (discussing Helen Nissenbaum's objections to the reliance on consent).

engineered,[151] or perhaps provided under duress. Firms equipped with data-driven analytics can nudge consumers into accepting the deals they offer. They can exploit individuals' personal traits and biases to manipulate their decision making.[152]

These concerns, however, do not suggest that contract law does not, or cannot, apply to data-for-services transactions. There is no legal rule precluding data from constituting contractual consideration or payment. Contract law may well be the most appropriate legal framework for governing these transactions.[153] The issue, therefore, is not only legal, but commercial. Terms of service and privacy policies fail to treat data collection as the price which consumers pay for services. By obscuring the *quid pro quo* inherent in these deals, terms of service and privacy policies give the false impression that the services provided are genuinely free.

To engage with ROD, terms of service and privacy policies need to be more transparent. They need to openly communicate that an exchange takes place. If consumers internalize the notion of data-for-services transactions, they may reconsider blindly consenting to each and every deal offered to them. Consumers may seek to scrutinize the data price and even negotiate the deal terms. A refusal to pay exorbitant data prices would, in time, signal to service providers consumers' demand for greater ROD.

B. Privacy Law

The preoccupation with privacy and failure to engage with ROD are reinforced by the legal regimes applicable to personal data. In response to the rise of the data economy, the EU adopted the General Data Protection Regulation (GDPR), which treats privacy as a fundamental right and provides various data protections to individuals. These include data access rights, data portability and privacy breach notifications.[154] In the United States, there is no equivalent regime which comprehensively regulates the collection and use of data by private entities[155] or treats data privacy vis-à-vis non-government actors as a fundamental right.[156] Instead, there is a patchwork of judge-made law,[157] sector-specific legislation,[158] contractual arrangements and industry practices.[159] Notably, California passed the Consumer

---

[151] *See* Nancy Kim, *Contract's Adaptation and the Online Bargain*, 79 U. CIN. L. REV. 1327, 1330 (2011). *See also* Lemley, *Terms of Use*, *supra* note 137, at 472–80 (regarding the enforceability of these agreements).

[152] *See, e.g.,* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1003 (2014); Tene & Polonetsky, *Big Data for All*, *supra* note 19, at 252–5.

[153] *See, e.g.,* Carmen Langhanke & Martin Schmidt-Kessel, *Consumer Data as Consideration*, 6 J. EUR. CONSUMER & MKT. L. 218, 219–20, 223 (2015).

[154] *See* EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. *See also* Charter of Fundamental Rights of the European Union art. 8 2010 O.J. C 83/02.

[155] *See generally* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013); Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877, 880–81 (2014).

[156] But there are constitutional protections against data collection carried out by government actors. *See, e.g.,* DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE (2017); Carpenter v. United States, 585 U.S. ____ (2018). However, it is private actors which carry out the majority of data collection. *See* SCHNEIER, DATA AND GOLIATH, *supra* note 3, at 47.

[157] *See* Restatement (Second) of Torts §§ 652A-E; William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

[158] *See, e.g.,* Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d-6 (2012); Children's Online Privacy and Protection Rule, 16 C.F.R. pt. 312 (2013).

[159] *See, e.g.,* SOLOVE & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note 127, at 785ff; Theodore Rostow, *What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers*, 34

Privacy Act, which, commencing in 2020, will grant Californians the right to prohibit the sharing and sale of personal data to third parties.[160]

Despite their differences, both the U.S. and EU data protection regimes embrace the privacy paradigm. They center on data protection, not ROD. Although the principles they enshrine and the methods they endorse differ greatly, privacy law on both sides of the Atlantic treats transactions involving personal data as a privacy issue.[161] Like privacy policies, privacy law (at present) only addresses one aspect of data-for-services transactions—the collection and use of personal data. It does not examine what consumers receive in exchange for the data they supply.

The following legal frameworks and proposals confirm that the overarching concern of privacy law is data protection. The GDPR and the proposed EU ePrivacy Regulation, as their titles suggest, aim primarily to protect personal data.[162] The FTC's Fair Information Practices (FIPs) are an industry data protection regime.[163] Legal textbooks relating to personal data are privacy-oriented.[164] Recent proposals include introducing a Bill of Data Rights to protect individuals' privacy;[165] treating data collectors as "information fiduciaries" obligated to safeguard personal data;[166] expanding the categories of data which warrant special protection;[167] and mandating the integration of data protection into product design.[168] These proposals all revolve around minimizing the risks and harms of data collection.[169] They do not contemplate the ROD of consumers or other data subjects.

By addressing only one aspect of data-for-services deals, these legal regimes fail to scrutinize—and even obscure—the *mutual* exchange underpinning data-for-services transactions. The GDPR, for example, does not clarify the role of data collection *as payment*.[170] Although the GDPR bolsters transparency around the processing of personal data, it does not require companies to disclose whether personal data constitute the price

---

YALE J. ON REG. 667, 676–77 (2017). *See also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 620–27 (2014); CHRIS HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016) (regarding the FTC's role in privacy policy and enforcement).

[160] *See infra* Cal. Civ. Code (as amended by Consumer Privacy Act (A.B. 375)) § 1798.

[161] *See, e.g.,* Margot Kaminski, *Toward Defining Privacy Expectation in an Age of Oversharing*, ECONOMIST (Aug. 16, 2018), https://www.economist.com/open-future/2018/08/16/toward-defining-privacy-expectations-in-an-age-of-oversharing.

[162] *See* GDPR, *supra* note 154, at rec. 6.

[163] *See* SOLOVE & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note 127, at 975.

[164] *Id*. *See also* MARC ROTENBERG & ANITA L. ALLEN, PRIVACY LAW AND SOCIETY (2016).

[165] Martin Tisné, *It's Time for a Bill of Data Rights*, MIT TECH. REV. (Dec. 14, 2018), https://www.technologyreview.com/s/612588/its-time-for-a-bill-of-data-rights/; will.i.am, *We Need to Own Our Data as a Human Right—and Be Compensated for It*, ECONOMIST (Jan 21., 2019), https://www.economist.com/open-future/2019/01/21/we-need-to-own-our-data-as-a-human-right-and-be-compensated-for-it. *See also* Kara Swisher, *Introducing the Internet Bill of Rights*, N.Y. TIMES (Oct. 4, 2018), https://www.nytimes.com/2018/10/04/opinion/ro-khanna-internet-bill-of-rights.html; A bill to establish duties for online service providers with respect to end user data that such providers collect and use, S. 3744, 115th Cong. (2018) (introduced by Senator Brian Schatz); A bill to prohibit certain entities from using facial recognition technology to identify or track an end user without obtaining the affirmative consent of the end user, and for other purposes, S. 847, 116th Cong. (2019) (introduced by Senators Roy Blunt and Brian Schatz).

[166] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016). *See also* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018).

[167] Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1143–44 (2015).

[168] *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018); R. JASON CRONK, STRATEGIC PRIVACY BY DESIGN (2018).

[169] *But see* Jack Hardinges, *What is a Data Trust?*, OPEN DATA INSTITUTE (Jul. 10, 2018), https://theodi.org/article/what-is-a-data-trust/ (harnessing the legal construct of trusts to build infrastructure and ecosystems which both protect data and improve access to data).

[170] *See id.* at recs. 39, 60, 71; arts. 5(1)(a), 12.

payable for services.[171] Privacy law thus fails to confront the bargains which consumers routinely make. By overlooking what consumers receive in return for the data they supply, privacy law maintains a very narrow focus. Its preoccupation with data protection and failure to engage with ROD are misplaced and even misleading.

C. Property Rights in Personal Data

Property law plays a major role in the legal discourse relating to personal data. But, like privacy law, it too is preoccupied with data protection and fails to engage with ROD. Beginning over 50 years ago, many legal scholars and economists have proposed establishing property rights in personal data.[172] Although the seminal articles date from the late 1990s and early 2000s, the proposal has seen a recent revival, especially in Europe.[173] Today, several scholars advocate *propertizing* personal data.[174] Apart from the rhetorical appeal of property,[175] property law is generally considered to be a tool which enhances competition, disperses power and safeguards other fundamental rights.[176] Supporters of propertization suggest that establishing property rights in personal data would facilitate the emergence of a market in which individuals could trade personal data and receive monetary compensation.[177] They contend that such a market would enable individuals to signal their preferences in respect of personal data, including determining the prices for which personal data could be sold. Propertization, they suggest, would most effectively allocate rights in personal data, a

---

[171] *See* GDPR, *supra* note 154, at art. 13 (listing the information which controllers must provide to data subjects). *But see infra* Part III.D.

[172] *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 324-25 (1967), *but see* Lisa M. Austin, *Re-Reading Westin*, 20 THEOR. INQ. L. 53 (2019); Hal R. Varian, *Economic Aspects of Personal Privacy*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (U.S. Dept. Comm., 1996); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy,* 84 GEO. L.J. 2381, 2383–84 (1996); Kenneth C. Laudon, *Markets and Privacy*, COMM. ACM 92 (Sept. 1996); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1246–94 (1998); Lawrence Lessig, *The Architecture of Privacy*, I VAND. J. ENT. L. & PRAC. 56, 63–65 (1999); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 122–35 (1999); Lawrence Lessig, *Privacy as Property*, 69 SOC. RES. 247, 257 (2002); Edward J. Janger, *Privacy Property, Information Costs, and the Anticommons*, 54 HASTINGS L.J. 899 (2002); Vera Bergelson, *It's Personal But Is It Mine: Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 414 (2003); Jamie Lund, *Property Rights to Information*, 10 NW. J. TECH. & INTELL. PROP. 1 (2011); Christopher Rees, *Tomorrow's Privacy: Personal Information as Property*, 3 INT'L DATA PRIVACY L. 220, 220–21 (2013).

[173] *See* Nadezhda Purtova, *The Illusion of Personal Data as No One's Property*, 7 L. INNOV. & TECH. 83 (2015); NADEZHDA PURTOVA, PROPERTY RIGHTS IN PERSONAL DATA: A EUROPEAN PERSPECTIVE (2011); Nadezhda Purtova, *Property in Personal Data: A European Perspective on the Instrumentalist Theory of Propertisation*, 2 EUR. J. LEGAL STUD. 193 (2010); Thomas Hoeren, *Big Data and the Ownership in Data: Recent Developments in Europe*, 12 EUR. INTELLECT PROP. REV. 751, 753–54 (2014); Gianclaudio Malgieri, *'Ownership' of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?*, 20 J. INTERNET L. 1, 11–12, 15–20 (2016). *See also* Victor, *supra* note 19; POSNER & WEYL, *supra* note 22, at 245 (suggesting that the GDPR resembles a property rights regime). *Cf* Purtova, *The Illusion of Personal Data as No One's Property*, *supra* note 173, at 89 (noting that the GDPR does not formally introduce property rights in personal data).

[174] *See* Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220 (2018). *See also* Lauren Henry Scholz, *Privacy as Quasi-Property*, 101 IOWA L. REV. 1113 (2016).

[175] *See, e.g.,* Carol M. Rose, *Property as the Keystone Right?*, 71 NOTRE DAME L. REV. 329, 349 (1996).

[176] *Id.* at 332–3, 240, 362. *See also* James W. Ely, Jr., THE GUARDIAN OF EVERY OTHER RIGHT: A CONSTITUTIONAL HISTORY, OF PROPERTY RIGHTS 26 (1992).

[177] *See, e.g.,* Lessig, *Privacy as Property*, *supra* note 172, at 261; Schwartz, *Property, Privacy, and Personal Data*, *supra* note 40, at pt. I. *See also infra* Part IV.C.

scarce resource.[178] Propertization might also encourage consumers to treat personal data as a valuable asset, which is a pre-requisite for embracing ROD.

Meanwhile, opponents of propertization contend that establishing a market in personal data would be costly. The necessary institutional infrastructure would be expensive. These costs might be passed on to individuals, perhaps in the form of information costs or other transaction costs.[179] Such a market might not function efficiently;[180] it might obstruct, rather than facilitate, trading personal data. Critics also point to several doctrinal issues concerning the propertization of personal data,[181] alongside some constitutional issues.[182] These concerns have led many commentators to reject the proposal.[183]

Data protection is perhaps the salient issue in the propertization debate. Supporters of propertization suggest that property rights can protect personal data better than can contract law, torts, or other non-proprietary legal frameworks.[184] Under a property law regime, a voluntary transaction is required for personal data to be traded. Under a non-proprietary regime, personal data may be traded involuntarily, with monetary compensation the only remedy available to data subjects.[185] In addition, property rights can be enforced against third parties, such as advertisers; contractual rights cannot.[186] Further, tort law only guards against highly intrusive privacy invasions,[187] while property rights provide broader protection.

Opponents of propertization respond that the establishment of property rights in personal data will actually undermine, rather than enhance, data protection.[188] They reason that alienability—the ability of property rights to be freely transferred and sold—is a necessary part of any property regime. Thus, if personal data were propertized, consumers would be free to sell personal data to each and every buyer.[189] In such circumstances, critics

---

[178] *See supra* note 55 (regarding scarcity). *See also* Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. 347, 350 (1967).

[179] *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1135–37 (1999); Mark A. Lemley, *Private Property*, 52 STAN. L. REV. 1545, 1552 (2000); POSNER & WEYL, *supra* note 22, at 238.

[180] *See* Lemley, *Private Property*, *supra* note 179, at 1554; Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1388 (2000).

[181] *See* Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The Numerus Clausus Principle*, 110 YALE L.J. 1 (2000) (regarding the *numerus clausus* principle, which stipulates that property rights are a closed list); *Pamela Samuelson, Information As Property: Do Ruckelshaus and Carpenter Signal a Changing Direction in Intellectual Property Law?*, 38 CATH. U. L. REV. 365, 366, 369 (1989) (regarding the ownership and excludability of data); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1299 (2000) (regarding the alienability of data). But many scholars maintain that property rights are a creature of law which can be actively created and amended. *See, e.g.,* Schwartz, *Property, Privacy, and Personal Data*, *supra* note 40, at 2059–61 (eschewing rigid adherence to the Blackstonian conception of property); Hanoch Dagan, *The Craft of Property*, 91 CAL. L. REV. 1518, 1532 (2003); Kevin Gray, *Property in Thin Air*, 50 CAMB. L.J. 252, 306–7 (1991); JEREMY BENTHAM, *Principles of the Civil Code*, *in* THE THEORY OF LEGISLATION 111 (C. K. Ogden ed., 1931).

[182] *See, e.g.,* Lessig, *Privacy as Property*, *supra* note 172, at 259–60; Samuelson, *Privacy as Intellectual Property?*, *supra* note 179, at 1140–41.

[183] *See* Samuelson, *Privacy as Intellectual Property?*, *supra* note 179; Litman, *supra* note 181; Julie E. Cohen, *Examined Lives*, *supra* note 180; Lemley, *Private Property*, *supra* note 179; Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1 (2001).

[184] *See* Janger, *supra* note 172, at 914; Bergelson, *supra* note 172, at 417. *But see* Ritter & Mayer, *supra* note 174 (supporting propertization but without concentrating on privacy interests).

[185] *See* Mark A. Lemley & Philip J. Weiser, *Should Property or Liability Rules Govern Information?*, 85 TEX. L. REV. 783, 784 (2007). *See generally* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092, 1105 (1972).

[186] *See* Thomas W. Merrill & Henry E. Smith, *The Property/Contract Interface*, 101 COLUM. L. REV. 773, 777 (2001).

[187] *See* Litman, *supra* note 181, at 1291, discussing Nader v. General Motors Corp., 25 N.Y.2d 560 (1970).

[188] *See* Samuelson, *Privacy as Intellectual Property?*, *supra* note 179, at 1128–29.

[189] *See id.* at 1137–38; Lemley, *Private Property*, *supra* note 179, at 1551; Janger, *supra* note 172, at 1852.

suggest, it is likely that consumers will unthinkingly sell the personal data they generate.[190] And, once this initial sale occurs, the data buyer will own the data and be able to transfer them to third parties, prompting serious privacy risks.[191] According to one commentator, "[t]he market in personal data is the *problem*. Market solutions based on a property rights model won't cure it; they'll only legitimize it."[192]

Despite their differences, supporters and opponents of propertization share in common the same principal concern: *privacy*. Supporters claim that propertization will enhance privacy. Opponents claim that it will undermine privacy. The propertization debate centers around privacy. One of the most influential articles on the topic proposed a property regime specially tailored to protect personal data and mitigate against the potential privacy harms of a free market in personal data.[193] In an effort to prevent the careless, ill-informed sale of personal data, it proposed restricting an individual's right to alienate personal data.[194]

Interestingly, little progress has been made in formally instituting privacy-enhancing property rights in personal data. Efforts to establish a standardized or highly regulated national data market have failed.[195] Some scholars have ceased to support propertization.[196] But, in the absence of legal intervention, data-driven companies have independently monetized personal data. The prevalence of data-for-services transactions suggests that there already exist *de facto* property rights in personal data.[197] Whilst personal data have not been formally propertized, there exists an active, largely unregulated market in personal data.[198] The fears of propertization critics have played out. Eager to access valuable services, consumers share personal data with data-driven companies. They routinely alienate personal data and enable their transfer to third parties. Data collectors and brokers are in the business of data trafficking. Deliberating over propertization is, therefore, somewhat anachronistic.

More fundamentally, it is worth questioning the conventional wisdom that formally propertizing consumers' rights in personal data will meaningfully assist consumers, especially as we transition from the privacy paradigm to ROD. Like privacy law, the establishment of property rights in personal data would not alone enable consumers to assess the merits of data-for-services deals. Property rights do not shine light on the utility which consumers gain in exchange for the data they supply. They cannot be used to comprehensively determine whether a particular data-for-services deal is in a consumer's best interests or, in the absence of holistic ROD evaluations, help consumers compare competing data-for-services deals.

---

[190] *See* Schwartz, *Property, Privacy, and Personal Data*, *supra* note 40, at 2078.
[191] *See* Samuelson, *Privacy as Intellectual Property?*, *supra* note 179, at 1142ff.
[192] Litman, *supra* note 181, at 1301.
[193] *See* Schwartz, *Property, Privacy, and Personal Data*, *supra* note 40, at 2093; 2095–116. *See also* Victor, *supra* note 19, at 518–19 (explaining that—unlike Lessig—Bergelson, Janger and Schwartz do not propose free markets in personal data, but highly regulated property regimes specifically tailored to protecting personal data.)
[194] *See* Samuelson, *Privacy as Intellectual Property?*, *supra* note 179, at 1138, 1145. Even economic arguments relating to the internalization of the social costs of data collection focus on data protection. *See id.* at 1134.
[195] *See* Rostow, *supra* note 159, at 674.
[196] *See, e.g.,* Nadezhda Purtova, *Do Property Rights in Personal Data Make Sense After the Big Data Turn?*, 10(2) J.L. & ECON. REG. (2017).
[197] *See* Bergelson, *supra* note 172, at 414; Purtova, *The Illusion of Personal Data as No One's Property*, *supra* note 173, at 88. *See also* Victor, *supra* note 19 (characterizing the GDPR as a property rights regime).
[198] *See* Rostow, *supra* note 159, at 678. *See also* JAMES RULE, PRIVACY IN PERIL: HOW WE ARE SACRIFICING A FUNDAMENTAL RIGHT IN EXCHANGE FOR SECURITY AND CONVENIENCE 97 (2007).

D. Data as "Counter-Performance" in the EU

The GDPR is not the only pioneering EU legal development to affect the data economy. The proposed EU Directive for consumer protection in contracts for the supply of digital content signals a potential shift towards the ROD paradigm.[199] Rather than (merely) enhance data protection, as does the GDPR, the Directive candidly confronts the reality of consumers paying for services with personal data. It expressly regulates data-for-services transactions. Article 3(1) of the Directive states that:

> This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer *actively provides counter-performance other than money in the form of personal data or any other data.*[200]

The Directive treats personal data as the "counter-performance" provided in exchange for services. In common law terminology, personal data constitute contractual consideration. By way of explanation, Recital 13 of the Directive provides that:

> In the digital economy, information about individuals is often and increasingly seen by market participants as having a value comparable to money. *Digital content is often supplied not in exchange for a price but against counter-performance other than money i.e. by giving access to personal data or other data.*[201]

The language of the Directive speaks for itself.[202] It recognizes that consumers pay for certain services with personal data.[203] The Directive enjoys broad support from EU institutions,[204] legal scholars,[205] consumer groups[206] and some industry groups.[207] Supporters

---

[199] *See European Commission Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content*, COM (2015) 0634 final (Dec. 2015), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52015PC0634. *See also* European Parliament, *Briefing: EU Legislation in Progress (Contracts for Supply of Digital Content)* (Feb. 2018), http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614707/EPRS_BRI(2018)614707_EN.pdf (indicating the current status and legislative progress of the Directive).

[200] Emphasis added. *See also* arts. 6(2), 15(2)(b), 16(4)(a).

[201] Emphasis added.

[202] *Cf* EDPS, *Opinion 4/2017*, *supra* note 46, at 3, 9; Madalena Narciso, *'Gratuitous' Digital Content Contracts in EU Consumer Law*, 5 J. EUR. CONSUMER & MKT. L.198, 202 (2017); Claudia Trivilino, *Why Developers Have a Problem with the New Debate Around Data as a Counter-Performance*, DEVELOPERS ALLIANCE (Dec. 12, 2016), https://www.developersalliance.org/news/2016/12/8/why-developers-have-a-problem-with-the-new-debate-around-data-as-a-counter-performance.

[203] *See* Vanessa Mak, *The New Proposal for Harmonised Rules on Certain Aspects Concerning Contracts for the Supply of Digital Content* (Policy Dept C: Citizens' Rights and Constitutional Affairs) at 10 (2016), http://www.europarl.europa.eu/cmsdata/98771/Mak.pdf. *Cf* European Parliament, *Briefing: EU Legislation in Progress (Contracts for the Supply of Digital Content)* at 9–10 (Oct. 2017), http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608748/EPRS_BRI%282017%29608748_EN.pdf (suggesting that the Directive may regulate personal data but does not treat personal data as contractual consideration).

[204] *See, e.g.,* European Parliament Committee on the Internal Market and Consumer Protection & Committee on Legal Affairs (EPC), *Report on the Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content* at 90 (Nov. 21, 2017), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA8-2017-0375%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN.

[205] *See, e.g.,* Hugh Beale, *Scope of Application and General Approach of the New Rules for Contracts in the Digital Environment* (Policy Dept C: Citizens' Rights and Constitutional Affairs) at 12–13 (2016), http://www.europarl.europa.eu/cmsdata/98770/Beale.pdf; Gerald Spindler, *Contracts For the Supply of Digital Content—Scope of Application and Basic Approach*, 12 EUR. REV. CONT. L. 183, 191–92 (2016).

of the Directive applaud it for treating data as "counter-performance" and, in doing so, extending consumer protections to data-for-services transactions.[208] One supporter observed that the Directive merely approves an existing practice (exchanging personal data for services) and is therefore trivial.[209] But, in light of the lack of recognition of data-for-services transactions elsewhere—in terms of service, privacy policies and privacy law—the Directive is groundbreaking. Unlike other legal frameworks, it directly tackles data-for-services transactions and, in doing so, informs and engages consumers.[210]

However, the Directive has also been criticized. Several industry groups suggest that, if enacted, it would overregulate and hamper the data economy.[211] Others suggest that it would inhibit contractual freedom and undermine the kind of transactions which facilitate innovation.[212] The European Data Protection Supervisor, an independent EU institution, while supporting the Directive's expansion of consumer protections, contends that personal data must not be treated as a price or payment for services. Commodifying personal data, it reasons, would infringe fundamental rights, such as privacy, and reduce them to commercial interests.[213] But this criticism is anachronistic. It ignores the reality that consumers routinely exchange personal data for services. Personal data are *already*, among other things, a commodity.

Another criticism relates to the scope of the Directive. Article 3(1) states that the Directive only applies where a consumer "*actively provides* counter-performance . . . in the form of personal data."[214] The problem is that vast quantities of valuable data collected by companies are not *actively provided* by consumers. They are *passively collected* by companies. These data would therefore fall outside the scope of the Directive.[215] Critics also

---

[206] *See, e.g.,* European Commission, *Impact Assessment* (Staff Working Doc., 2015, 274 final/2) at 62, 122–23 (Dec. 17, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2015%3A274%3AREV1.

[207] *See, e.g., id.* at 63.

[208] *See* Helberger et al., *supra* note 91, at 1445.

[209] *See* Axel Metzger, *Data as Counter-Performance: What Rights and Duties do Parties Have?*, 8 J. INTELL. PROP. INFO. TECH. & ELECTRONIC COMM. L. 1, 7 (2017).

[210] *See* Helberger et al., *supra* note 91, at 1442–44.

[211] *See* Business Europe, *Position Paper on the Harmonisation of Contract Rules for Digital Content and Tangible Goods* at 5 (Sept. 3, 2015), https://www.businesseurope.eu/publications/harmonisation-contract-rules-digital-content-and-tangible-goods; DIGITALEUROPE, *Comments on the Proposed Directive on Contract Rules for the Supply of Digital Content* at 1 (Apr. 15, 2016), http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2157&language=en-US&PortalId=0&TabId=353. *See also* Joseph Jerome & Laura Blanco, *EC Proposal to Pay with Personal Data Could Undermine Privacy and Harm the Online Ecosystem*, CENTER FOR DEMOCRACY AND TECHNOLOGY (Apr. 6, 2017), https://cdt.org/blog/ec-proposal-to-pay-with-personal-data-could-undermine-privacy-and-harm-the-online-ecosystem/.

[212] *See Joint Industry Declaration on the Digital Content Directive* at 2 (May 24, 2016), http://www.amchameu.eu/media-centre/press-releases/joint-industry-declaration-digital-content-directive.

[213] *See* EDPS, *Opinion 4/2017*, *supra* note 46, at 7 (likening markets in personal data to human organ trafficking). *See generally* MICHAEL J. SANDEL, WHAT MONEY CAN'T BUY: THE MORAL LIMITS OF MARKETS (2012) (advocating certain limits on commodification). *Cf* JASON BRENNAN & PETER JAWORSKI, MARKETS WITHOUT LIMITS: MORAL VIRTUES AND COMMERCIAL INTERESTS 10 (2016) (criticizing anti-commodification theorists and suggesting that: "If you may do it for free, then you may do it for money"). *See also* Alvin Roth, *Repugnance as a Constraint on Markets*, 21 J. ECON. PERSPECT. 37 (2007); ALVIN E. ROTH, WHO GETS WHAT—AND WHY: THE NEW ECONOMICS OF MATCHMAKING AND MARKET DESIGN 195 (2016) (questioning the moral opprobrium ascribed to certain "repugnant" transactions, such as markets in kidneys.)

[214] Emphasis added. *See also* rec. 14 (elaborating on this limitation).

[215] *See* Ruth Janal, *Data Portability: A Tale of Two Concepts*, 8 INTELL. PROP. INFO. TECH. & ELECTRONIC COMM. L. 59, 65 (2017). This exclusion would have sweeping ramifications. *See* Spindler, *supra* note 205, at 193; Narciso, *'Gratuitous' Digital Content Contracts*, *supra* note 202, at 203–4. *See also* EPC, *supra* note 204, at 53, 90, 94, 97, 105; European Law Institute, *Statement on the European Commission's Proposed Directive on the Supply of Digital Content to Consumers* at 14–15 (2016),

suggest that, because consumers who do not consent to data collection cannot be said to "actively provide" such data, the Directive incentivizes companies to altogether refrain from seeking consumer consent to data collection.[216] Ironically, it is in these circumstances that consumers most need legal protection.[217] However, the GDPR, which requires companies to seek consumer consent to both active and passive collection, largely blunts this criticism.

A further criticism of the Directive relates to Article 3(4), which provides that the Directive does not apply to personal data which are "*strictly necessary* for the performance of the contract."[218] The problem here is that it is not always clear which data are necessary for a particular service to function.[219] For instance, while a mobile payments app might not *require* location data, location data may significantly enhance the app's security (e.g., a mobile payments app). More fundamentally, even if it were clear which data are necessary for a particular service to function, the data supplied (both those which are "necessary" and those which are not) still constitute the price paid for the services. The mere fact that location data are "necessary" for the service should not exempt them from the Directive.[220]

Lastly, the Directive has been criticized for distinguishing between consumers who pay for services with money and consumers who pay with personal data,[221] as has California's Consumer Privacy Act.[222] Studies suggest that the form of payment—monetary or non-monetary—does not impact the level of legal protection which consumers expect.[223] Nevertheless, the Directive affords consumers who pay with money greater legal protection. For instance, consumers who pay with money are entitled to superior termination rights,[224] and can more easily enforce contractual performance.[225] By discriminating against consumers who pay for services with personal data, the Directive undercuts its goal of treating all consumers equally, irrespective of how they pay.[226]

The Directive has spawned vigorous debate. It is *therefore* a welcome development. By regulating data-for-services deals, the Directive expressly recognizes the reality of these

---

https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Statement_on_DCD.pdf (proposing that the word "actively" should be omitted from the Directive).

[216] *See* EDPS, *Opinion 4/2017*, *supra* note 46, at 12; Beale, *supra* note 205, at 12–13; Narciso, *'Gratuitous' Digital Content Contracts*, *supra* note 202, at 204.

[217] *See* Helberger et al., *supra* note 91, at 1446–47.

[218] *See also* rec. 14 ("This Directive should not apply to situations where the supplier collects data necessary for the digital content to function in conformity with the contract, for example geographical location where necessary for a mobile app to function properly, or for the sole purpose of meeting legal requirements, for instance where the registration of the consumer is required for security and identification purposes by applicable laws").

[219] Narciso, *'Gratuitous' Digital Content Contracts*, *supra* note 202, at 205. See *infra* note 287 (regarding data efficiency).

[220] *See* Mak, *supra* note 203, at 9. *See also* EPC, *supra* note 204, at 54, 106 (proposing that this limitation should be omitted from the Directive).

[221] *See* Mak, *supra* note 203, at 17–18.

[222] *See* Cal. Civ. Code (as amended by Consumer Privacy Act (A.B. 375)) § 1798.125(a)(2) ("Nothing . . . prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.") *See also* § 1798.125(b)(1) ("A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data").

[223] *See* Madalena Narciso, *Consumer Expectations in Digital Content Contracts – An Empirical Study* (Tilburg Private Law Working Paper Series No. 01/2017) 1, 19–21, *available at* https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2954491.

[224] *See* art. 13(2); rec. 42.

[225] *See* art. 6(2)(a); European Parliament, *Contracts for Supply of Digital Content, A Legal Analysis of the Commission's Proposal for a New Directive* at 16 (May 2016), http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/582048/EPRS_IDA(2016)582048_EN.pdf.

[226] *See* Spindler, *supra* note 205, at 198–99.

transactions. While other legal frameworks, such as terms of service, privacy policies and privacy law, are preoccupied with privacy, the Directive engages with the mutual exchange between consumers and companies. However, notwithstanding its recognition of personal data as a form of payment, the Directive fails in one key respect. It does not actually assist in making data-for-services transactions more transparent. It does not assess, or reveal, ROD.

IV. DATA PLATFORMS

Like most of the legal frameworks discussed so far, many data platforms perpetuate the privacy paradigm. Some platforms enable consumers to pay a monetary premium to avoid or minimize personal data collection. Others offer monetary discounts to consumers willing to share additional personal data. Meanwhile, platforms which monitor and manage the collection and use of personal data—privacy-tech—aim to protect personal data.

Yet, some platforms have begun to challenge the privacy paradigm. Data exchanges and data investment platforms give consumers the opportunity to sell personal data for cash or other benefits. By offering consumers a range of benefits in exchange for personal data, they implicitly embrace the notion of ROD. But they too fail in one major respect. These platforms only offer consumers the opportunity to enter *new* deals, that is, to strike fresh bargains. These platforms do not engage with the many data-for-services transactions which consumers *already* enter (with Facebook, Google, etc.) The ROD of *these* transactions remains unknown.

This Part begins by examining privacy-enhancing technologies and proceeds to consider the possibility of paying monetary premiums (or receiving monetary discounts) to enhance (or forgo) privacy. It then explores several data platforms which seek to provide various benefits to consumers in return for personal data. While some of these developments openly recognize the reality of data-for-services transactions, further innovation is needed in order to quantify ROD and make these transactions fully transparent.

A. Privacy Tech

Privacy monitors and personal information management systems (PIMs) are the most common privacy tech tools.[227] Privacy monitors, sometimes called privacy dashboards, aim to display to users how personal data relating to them are collected and used.[228] They come in different forms and operate on a variety of devices.[229] For example, Lumen Privacy Monitor, an Android app developed by researchers at the University of California, Berkeley, monitors the type, volume and (apparent) purpose of data collection carried out by mobile apps.[230] It tracks the device's network connections, reveals which data are exported by which apps and identifies the (initial) recipients of those data.[231] Although Lumen provides users with

---

[227] *See generally* Doc Searls, *For Privacy We Need Tech More Than Policy*, DOC SEARLS BLOG (Apr. 2, 2018), http://blogs.harvard.edu/doc/2018/04/02/for-privacy-we-need-tech-more-than-policy/.

[228] *See* Christian Zimmermann et al., *Privacy Dashboards: Reconciling Data-Driven Business Models and Privacy,* ARES AVAILABILITY, RELIABILITY & SECURITY 152 (2014); Christoph Bier et al., *PrivacyInsight: The Next Generation Privacy Dashboard*, PRIVACY TECHNOLOGIES & POLICY 135 (2016); Yuanchun Li et al., *PrivacyStreams: Enabling Transparency in Personal Data Processing for Mobile Apps*, ACM INTERACT. MOB. WEARABLE UBIQ. TECH. 1 (Sept. 2017).

[229] *See, e.g.,* GOOGLE DASHBOARD (last visited __), https://myaccount.google.com/intro/dashboard (which provides information relating to, *inter alia*, Google web and location history, Google Play apps and YouTube).

[230] *See Lumen Privacy Monitor*, GOOGLE PLAY (last visited __), https://play.google.com/store/apps/details?id=edu.berkeley.icsi.haystack.

[231] *See* Phillip Tracy, *Here's How to Find Out Which Apps Are Leaking Your Personal Data*, DAILY DOT (July 11, 2017), https://www.dailydot.com/debug/lumen-apps-leak-personal-data/. Net Monitor, an Android app

important insights, it has several shortcomings. Lumen only monitors network communications, i.e. an app's communications with external servers. It does not monitor data collection which occurs on the actual device.[232] Ironically, Lumen itself collects significant amounts of personal data.[233] Users must grant it a wide range of data collection permissions in order to gain insight into the data collection carried out by other apps.

Unlike Lumen, many privacy monitors do not track *actual* data collection. Instead, they track a device's *permissions* with respect to data collection.[234] MyPermissions Privacy Cleaner, an iOS and Android app, rates mobile apps based on the scope of data collection permissions granted to them by users.[235] Permission Friendly Apps, another Android app, assesses privacy risks arising from permitting different types of data collection and ranks apps accordingly.[236] Although these permission-monitoring apps provide important insights, as they do not monitor data collection (but only permissions), they cannot assess the data price which consumers actually pay for different apps.

The range and functions of privacy monitors are diverse. Several internet browsers (e.g., Cliqz, Brave) and browser extensions (e.g., Ghostery, Privacy Badger) analyze and display the third party trackers which operate on the websites a user visits.[237] Polisis, developed by U.S. and European researchers, uses AI and ML to read, summarize and convey to consumers the content of privacy policies.[238] Princeton University's IoT Inspector, an open-source research project, aims to develop tools for analyzing the privacy and security of IoT devices, such as voice assistants and features of smart homes.[239]

Each of these privacy monitors can help consumers by revealing to them how personal data are collected and used. Although privacy monitors have not proven especially popular,[240] their potential use cases are likely to expand, particularly as the IoT grows.[241] However, from the perspective of ROD, privacy monitors are lacking. They only assess data collection. They do not assess what consumers receive in exchange for the data they supply.

---

developed by German researchers, performs a similar function. *See Privacy Friendly Net Monitor*, KARLSRUHE INSTITUTE OF TECHNOLOGY (last visited __), https://secuso.aifb.kit.edu/english/Net_Monitor.php.

[232] Data processed in-device are often exported and thus cannot be easily monitored. However, privacy monitors may be able to interpret some of the related metadata, which can at times reveal the purpose or intent of a communication. For example, Lumen may be able glean from metadata the destination and timing of a communication, but not the content of the encrypted data.

[233] Lumen is part of a research project which studies how consumers use mobile devices. *See infra* Part V.A.3.

[234] For example, Google Play's descriptions of apps' data permissions typically refer to the default permissions, not the actual permissions (as modified by each individual user). *But see* APPCENSUS (last visited __), https://www.appcensus.mobi/ (which monitors actual data collection, at least during the limited testing period upon which its privacy analysis is based).

[235] *See MyPermissions Privacy Cleaner*, APP STORE (last visited __), https://itunes.apple.com/us/app/mypermissions-privacy-cleaner/id535720736?mt=8. Like other privacy monitors, MyPermissions requires users to grant it various data permissions.

[236] *See Permission Friendly Apps*, GOOGLE PLAY (last visited __), https://play.google.com/store/apps/details?id=org.androidsoft.app.permission.

[237] *See* GHOSTERY (last visited __), https://www.ghostery.com/; CLIQZ, (last visited __), https://cliqz.com/en/; *Privacy Badger*, ELECTRONIC FRONTIER FOUNDATION (last visited __), https://www.eff.org/privacybadger; BRAVE (last visited __), https://brave.com/. *See also* Louise Matsakis, *Ad-Blocker Ghostery Just Went Open Source—And Has A New Business Model*, WIRED (Mar. 8, 2018), https://www.wired.com/story/ghostery-open-source-new-business-model/ (explaining that Ghostery's Rewards feature functions as an affiliate marketing system which effectively replaces websites' default advertisements with its own). *See also* CHARLES: WEB DEBUGGING PROXY APPLICATION (last visited __), https://www.charlesproxy.com/ (which records and displays data sent and received between browsers and servers).

[238] *See* POLISIS/PRIBOT (last visited __), https://pribot.org/. *See also Usable Privacy Policy Project*, CARNEGIE MELLON UNIVERSITY (last visited __), https://usableprivacy.org/publications.

[239] *See IoT Inspector Project*, PRINCETON UNIVERSITY (last visited __), https://iot-inspector.princeton.edu/.

[240] *But see* Perrin, *supra* note 39.

[241] *See generally* Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, *supra* note 37.

As a result, privacy monitors cannot examine the merits of different data-for-services arrangements or evaluate the ROD for a given transaction, let alone explore where greater ROD may be available.

PIMs provide greater functionality than privacy monitors. They enable consumers to exercise control over the personal data they generate.[242] Some PIMs help optimize consumers' decisions regarding who can access the personal data they generate. For example, MyPermissions Privacy Cleaner enables consumers to fine-tune the data collection permissions of mobile apps.[243] Other PIMs serve as gatekeepers between consumers and third parties seeking access to personal data. For example, Digi.me users can connect various data points (such as social media accounts) to the platform so that any third party seeking access to those data points must authenticate via the platform, which limits access in accordance with the scope of the user's consent. Thus, for instance, a user may disclose her credit score but withhold the raw data from which the credit score is generated.[244] Cozy, another PIM, plans to partner with banks and other companies to develop privacy-friendly, GDPR-compliant apps to interact with its cloud ecosystem.[245]

PIMs, like privacy monitors, seek to empower consumers.[246] They encourage and, to some degree, enable consumers to take responsibility for data protection.[247] But therein lies the problem. Privacy tech, like privacy law, aims to protect personal data. Whether by nudging consumer decision making or actively managing consumer data, privacy tech concentrates on protecting consumer privacy. Privacy tech does not meaningfully interact with the benefits which consumers receive in exchange for sharing personal data. Consider, for example, the proposal to offer consumers a universal "Do-Not-Track" feature across all digital platforms.[248] Practical feasibility aside, privacy tech proposals like this exclusively address data protection and overlook the underlying give-and-take. Privacy tech, notwithstanding the benefits it provides, relates only to the data price which consumers pay. It neglects ROD and does not come close to making data-for-services transactions fully transparent.

---

[242] *See* European Commission Directorate-General for Communications Networks, Content and Technology, *An Emerging Offer of "Personal Information Management Services"* (Jan. 2016), https://ec.europa.eu/digital-single-market/en/news/emerging-offer-personal-information-management-services-current-state-service-offers-and; VRM DEVELOPMENT WORK: PERSONAL INFORMATION MANAGEMENT SYSTEMS (last visited __), https://cyber.harvard.edu/projectvrm/VRM_Development_Work#Personal_Information_Management_Systems_.28PIMS.29. The Harvard Berkman Center's Vendor Relationship Management project explores ways to enhance consumer agency, including by enabling consumers to share personal data voluntarily and selectively.

[243] *See MyPermissions Privacy Cleaner*, *supra* note 235. Other privacy monitors, such as Ghostery and Privacy Badger, also function as PIMs by blocking trackers automatically or at a user's request.

[244] *See* DIGI.ME (last visited __), https://digi.me/.

[245] *See* COZY.IO (last visited __), https://cozy.io/en/. *See also* Romain Dillet, *Cozy Is Building a Personal Cloud Service that Respects Your Privacy*, TECHCRUNCH (Jan. 25, 2018), https://techcrunch.com/2018/01/25/cozy-is-building-a-personal-cloud-service-that-respects-your-privacy/. There are many other privacy-friendly data storage and data sharing platforms. *See, e.g.,* MEECO, (last visited __), https://meeco.me/index.html; PERKEEP, (last visited __), https://perkeep.org/.

[246] *See* EDPS, *Opinion 9/2016 on Personal Information Management Systems* (Oct. 20, 2016), *available at* https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf.

[247] *See generally* Anita L. Allen, *An Ethical Duty to Protect One's Own Information Privacy?*, 64 ALA. L. REV. 845 (2013); Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 HARV. L. REV. F. 71, 72–73 (2016). *But see* Solove, *Privacy Self-Management*, *supra* note 89; Richards & Hartzog, *supra* note 122, at 444 (suggesting that privacy self-management is highly problematic). However, some PIMs may help overcome certain human shortcomings and supplement or enhance people's privacy management decisions. *See, e.g., PrivacyAssistant.Org*, PERSONALIZED PRIVACY ASSISTANT PROJECT (last visited __), https://www.privacyassistant.org/.

[248] *See* Strandburg, *supra* note 28, at 169–70.

B. Paying for Privacy

Today, there are increasing opportunities for consumers to pay for privacy.[249] In exchange for paying a monetary premium, consumers can in some contexts limit the scope of data collection carried out when they access certain services. For example, consumers can pay a fee to access specific virtual private networks (VPNs) which better protect user privacy.[250] Several commentators advocate expanding this pay-for-privacy model. They have called on social media platforms to offer paid subscriptions in place of, or alongside, the current data-for-services model.[251] At the same time, several companies have begun to offer consumers monetary discounts on certain services in exchange for consumers sharing more personal data. For example, some automotive insurers offer discount rates to consumers who permit the collection of driving data.[252] One internet service provider (ISP) offered consumers discount rates in exchange for allowing it to use consumer data for personalized advertising.[253] Other utilities, such as mobile carriers and energy providers, may adopt this model in the future. The price of smart TVs is also increasingly subsidized by advertising revenue and other data-generated revenue.[254]

These opportunities seem empowering. Consumers, at least in theory, are given a choice.[255] Those who prize privacy can pay a premium to protect personal data relating to them; those who are less concerned by privacy can enjoy monetary discounts in exchange for supplying more data. It looks like a win-win situation. But there is a catch. Many consumers have only a limited understanding of privacy risks and may therefore opt for monetary discounts over data protection.[256] The prospect of a monetary discount entices them to supply more personal data. In addition, not all consumers are in a position to pay a monetary premium (or refuse a monetary discount) in order to protect their privacy. Many consumers, even if they are particularly concerned about their privacy, may be financially induced (or compelled) to supply more personal data.[257]

Despite these shortcomings, the opportunity to pay for privacy has noteworthy benefits. By paying a monetary price to collect and use personal data, companies signal to consumers that personal data are commercially valuable. Although the monetary premiums

---

[249] *See generally* Elvy, *Paying for Privacy*, *supra* note 3; Nahai & Chamorro-Premuzic, *supra* note 39.

[250] *See* Elvy, *Paying for Privacy*, *supra* note 3, at 1388–91 (discussing the "privacy-as-a-luxury" model). *See also* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION 168–71 (2016).

[251] *See* TIEN TZUO, SUBSCRIBED: WHY THE SUBSCRIPTION MODEL WILL BE YOUR COMPANY'S FUTURE—AND WHAT TO DO ABOUT IT (2018); Philip Hacker & Bilyana Petkova, *Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers*, 15 NW. J. TECH. & INTELL. PROP. 20, 22–27, 36 (2017); Calo, *supra* note 152, at 1047–48. *See also* Zeynep Tufekci, *Mark Zuckerberg, Let Me Pay for Facebook*, N.Y. TIMES (June 4, 2015), https://www.nytimes.com/2015/06/04/opinion/zeynep-tufekci-mark-zuckerberg-let-me-pay-for-facebook.html. *But see Senate Hearing*, *supra* note 1 (Zuckerberg responding that most consumers prefer not to, or would be unable to, pay money for Facebook's services). *See also* Kurt Wagner, *Mark Zuckerberg Explains Why an Ad-Free Facebook Isn't as Simple as It Sounds*, RECODE (Feb. 20, 2019), https://www.recode.net/2019/2/20/18233640/mark-zuckerberg-explains-ad-free-facebook.

[252] *See* O'NEIL, *supra* note 250, at 168; Mark Chalon Smith, *State Farm's In-Drive Discount: What's the Catch?*, CARINSURANCE.COM (June 12, 2015), https://www.carinsurance.com/Articles/state-farm-in-drive-discount.aspx.

[253] *See* Elvy, *Paying for Privacy*, *supra* note 3, at 1391–2 (discussing the "privacy-as-a-discount" model).

[254] *See* Nilay Patel, *Taking the Smarts Out of Smart TVs Would Make Them More Expensive*, VERGE (Jan. 7, 2019), https://www.theverge.com/2019/1/7/18172397/airplay-2-homekit-vizio-tv-bill-baxter-interview-vergecast-ces-2019.

[255] *But see supra* Part III.A.

[256] *See* Elvy, *Paying for Privacy*, *supra* note 3, at 1388. *See also supra* Part II.C.

[257] *See* Joseph W. Jerome, *Buying and Selling Privacy: Big Data's Different Burdens and Benefits*, 66 STAN. L. REV. ONLINE 47, 48 (2013); O'NEIL, *supra* note 250, at 171.

and discounts offered by companies might not accurately reflect the value of personal data,[258] they nevertheless imply that the value of data is not only personal or psychological, but financial. This, of course, is a prerequisite for understanding and embracing ROD.

Nevertheless, the idea of paying for privacy may be somewhat antiquated. It may be too late for individuals to begin to pay to protect their privacy. Personal data relating to them are perhaps already scattered so widely that prospectively restricting their distribution would be fruitless.[259] But, in reality, *new* personal data are continuously being generated. Companies constantly collect, process and distribute new data. Therefore, opportunities to pay for privacy may indeed empower consumers going forward, enabling at least some of them to actively choose between financial considerations and privacy interests.

However, opportunities to pay for privacy face another issue. They do not meaningfully engage with data-for-services transactions in which no money changes hands. The foregoing deals in which the *monetary* price charged is proportionate to the degree of data protection has no bearing on the routine deals in which consumers exchange personal data for services. The ability to pay a monetary premium for privacy in highly specific contexts does not enable or inspire consumers to in other contexts assess what they receive in return for the data they supply. Opportunities to pay for privacy, notwithstanding their potential to empower consumers, do not make data-for-services transactions more transparent.

C. Selling and Investing Personal Data

Several platforms now enable consumers to sell or invest personal data.[260] Datacoup, perhaps the most well-known personal data exchange (PDE), allows consumers to sell personal data for cash.[261] DataBuyer facilitates organizations offering consumers financial rewards in exchange for personal data.[262] Shopkick gives consumers retail vouchers in return for access to location, shopping and other data.[263] Some PDEs provide consumers with non-monetary benefits.[264] In exchange for collecting personal data, OpenDNA delivers individually tailored content while PI.Exchange provides personalized behavioral insights.[265] 23andMe offers health and genealogical insights in return for genetic information (and a monetary fee).[266] DataWallet, a blockchain-powered PDE, enables data to be securely exchanged via smart contracts in return for different rewards.[267]

---

[258] *See supra* note 54 (regarding the difficulty in determining the value of data).

[259] *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION ch. 2 (2015). *See also* KPMG, *supra* note 99, at 18; Strandburg, *supra* note 28, at 145, 150. However, the "right to be forgotten" may facilitate the deletion of certain information. *See, e.g.,* GDPR, *supra* note 154, at art. 17. *See generally* Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2012).

[260] *See* Doc Searls, *We Can Do Better than Selling Our Data*, DOC SEARLS BLOG (Sept. 18, 2018), https://blogs.harvard.edu/doc/2018/09/18/data/ (listing PDEs, including 360 of Me, Bitclave and People.io).

[261] *See How it Works,* DATACOUP (last visited __), https://datacoup.com/docs#how-it-works (explaining that users decide which data points to make available to the platform, which determines the amount of cash they receive).

[262] *See* DATABUYER (last visited __), https://databuyer.hubofallthings.com/about (explaining that organizations can request to access personal data and to influence digital action (e.g., tweets or posts) and even physical action (e.g., paying for transport or interactions with IoT devices)).

[263] *See* SHOPKICK (last visited __), https://www.shopkick.com/how-it-works.

[264] *See* Elvy, *Paying for Privacy*, *supra* note 3, at 1393–98, 1420 (discussing the "data-insights" model).

[265] *See* PI.EXCHANGE (last visited __), https://pi.exchange/.

[266] *See* 23ANDME (last visited __), https://www.23andme.com/en-int/; *FDA Authorizes, with Special Controls, Direct-to-Consumer Test that Reports Three Mutations in the BRCA Breast Cancer Genes*, FDA (Mar. 6, 2018), https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm599560.htm. *See also* Aisha Hassan,

PDEs clearly give consumers the opportunity to benefit from personal data in new ways.[268] The data-for-services transactions which they facilitate are relatively transparent, at least compared with traditional data-for-services transactions. DataBuyer and 23andMe are upfront about trading personal data for other benefits. PDEs do not conceal the give-and-take.[269] They embrace and *market* it. PDE users consciously choose which personal data to share and know what to expect in return.[270] ROD, in these cases, is comparatively explicit and clear-cut.

Yet, PDEs have not proven especially popular.[271] This might be because they tend to pay consumers only relatively small sums of money,[272] which is partly attributable to the fact that payments are made prior to the data being aggregated and monetized. Datacoup's website, for example, showcases a user earning $1.10 a week from the platform.[273] The conceptual impact of PDEs has also been limited, perhaps because PDEs only facilitate *new* transactions. PDEs have no impact whatsoever on the vast number of data-for-services transactions which consumers *already* enter. For example, the opportunity to sell location data to Datacoup does not affect a consumer's ongoing relationship with Waze, to which she *already* supplies the same location data (in return for navigation services). Forging new relationships with PDEs does not illuminate or alter *existing* relationships with data-driven service providers.

One possible response is to introduce elements of PDEs into existing data-for-services transactions. Under micropayment proposals, consumers would receive a small monetary payment for every unit of data they share with service providers.[274] However, micropayments have been widely criticized on several grounds. First, it may be unclear who will be entitled to a given micropayment, particularly as data relating to one person are often collected from others.[275] Second, there is no accepted method for determining what amounts would be paid, especially given that the value of data usually materializes later in the data's lifecycle.[276]

Spotify and Ancestry Can Use Your Real DNA to Tell Your "Musical DNA", QUARTZY (Sept. 22, 2018), https://qz.com/quartzy/1399279/spotify-can-use-your-ancestry-dna-test-to-tell-your-musical-dna/.

[267] DATAWALLET (last visited __), https://app.datawallet.com/. *See also* Daniel Hawthorn et al., *A Data-Ownership Assuring Blockchain Wallet for Privacy-Protected Data Exchange* (Subtitle Draft Version 0.8k, undated), https://tokensale.datawallet.com/pdf/datawallet_whitepaper.pdf; *Datawallet ICO Review and DXT Token Analysis*, CRYPTO BRIEFING (Aug. 25, 2018), https://cryptobriefing.com/datawallet-ico-review-dxt-token-analysis/ (explaining that Data Exchange Tokens are required to access the data supplied).

[268] *See* Jerome, *supra* note 257, at 52.

[269] *But see* Josh Constine, *Facebook Pays Teens to Install VPN that Spies on Them*, TECHCRUNCH (Jan. 30, 2019), https://techcrunch.com/2019/01/29/facebook-project-atlas/.

[270] *Compare supra* Part II.A (regarding the misalignment between data prices and services).

[271] *See* Mindaugas Kiskis, *Ever Dreamed of Selling Your Data for Cash? Dream On*, NEXT WEB (July 7, 2018), https://thenextweb.com/contributors/2018/07/07/ever-dreamed-of-selling-your-data-for-cash-dream-on/. PDEs may also adversely affect lower-income consumers or consumers lacking certain knowledge or experience, who may more willingly accept unfavorable exchanges. *See* Kaveh Waddell, *Would You Let Companies Monitor You For Money?*, ATLANTIC (Apr. 1, 2016), https://www.theatlantic.com/technology/archive/2016/04/would-you-let-companies-monitor-you-for-money/476298/.

[272] *See* Gregory Barber, *I Sold My Data for Crypto. Here's How Much I Made*, WIRED (Dec. 17, 2018), https://www.wired.com/story/i-sold-my-data-for-crypto/.

[273] *See How it Works,* DATACOUP, *supra* note 261.

[274] *See* POSNER & WEYL, *supra* note 22, at 247; LANIER, *supra* note 19, at 6; 317; Jakob Nielson, *The Case for Micropayments*, NIELSON NORMAN GROUP (Jan. 25, 1998), https://www.nngroup.com/articles/the-case-for-micropayments/.

[275] *See* WEIGEND, *supra* note 4, at 508–523 (discussing who will receive the payment where one person uploads a photo which features other people). *See also supra* note 61 (regarding passive data collection).

[276] *See id.* at 508–23. *See also supra* note 54 (regarding the difficulty in determining the value of data).

Third, micropayments might impose additional transaction costs on consumers.[277] Fourth, developing systems and infrastructure to facilitate micropayments would be costly.[278] Fifth, consumers might not actually be interested in receiving minute monetary payments in exchange for sharing highly sensitive personal data.[279]

Apart from these concerns, the introduction of micropayments into existing data-for-services transactions poses a more fundamental problem. The establishment of a new system of payments arguably implies that consumers do not presently receive sufficient compensation for the data they supply. It suggests that consumers must receive additional payment. Yet, given that most existing data-for-services transactions are not transparent, we cannot actually assess what compensation consumers currently receive, let alone judge whether it is sufficient. Consumers may be getting good deals. They may be getting bad deals. There is currently no reliable way to know.

Datavest—like its competitors, Datum, Doc.ai, Ocean Protocol, Permission.io and Wibson—may signal a change of direction.[280] Although its PDE is not yet fully operational, Datavest explicitly refers to ROD. It asks the right questions: "how much have you actually paid Facebook? Instagram? Or Waze? And by how much have you overpaid LinkedIn, Uber, Experian, AMEX, or 23andMe? … If you're unsure, you're not alone."[281] Datavest states that it plans to facilitate a "data investment platform," which it promises will deliver greater ROD. In exchange for investing personal data in different "data funds,"[282] Datavest users, like those of competing platforms, will receive digital currency tokens, known as Datanotes (DXN).[283] Despite its bombastic claim that data investments will overtake cash investments within a decade, Datavest does appear to be addressing the relevant issues.[284] It prompts consumers to reflect on how much they *earn* from the data they supply. It highlights ROD. However, as with privacy tech and other PDEs, there is no indication that Datavest will make *existing* data-for-services transactions more transparent. To do this, we need to nudge ROD.

V. NUDGING RETURN ON DATA

So far, we have seen how the legal frameworks which govern data-for-services transactions are preoccupied with privacy. Privacy policies, privacy law and the property rights discourse all center on data protection. We have also seen how privacy tech embraces the privacy paradigm. Although these frameworks and platforms help bolster consumers' control over personal data, they ignore ROD. They do not analyze the relationship between

---

[277] *See* ANDERSON, *supra* note 20, at 45, 48, discussing Nick Szabo, *Micropayments and Mental Transaction Costs*, SATOSHI NAKAMOTO INSTITUTE (undated), http://nakamotoinstitute.org/static/docs/micropayments-and-mental-transaction-costs.pdf.

[278] *See* WEIGEND, *supra* note 4, at 523–527.

[279] *See id.* at 508–531.

[280] DATAVEST (last visited __), https://www.datavest.org/; DATUM (last visited __), https://datum.org/; DOC.AI (last visited __), https://doc.ai/neuron/; OCEAN PROTOCOL (last visited __), https://oceanprotocol.com/; PERMISSION.IO (last visited __), https://permission.io/; WIBSON (last visited __), https://wibson.org/.

[281] Rob Nicholas Stone, *Data as Capital*, MEDIUM (May 24, 2018), https://medium.com/datavest/data-as-capital-d2a07533b04a.

[282] *See* Emma Firth, *Datavest Partners with Digi.me to Help People Monetise Their Personal Data*, DIGI.ME BLOG (Mar. 26, 2018), https://blog.digi.me/2018/03/26/datavest-partners-with-digi-me-to-help-people-monetise-their-personal-data/ (explaining that the partnership between Datavest and Digi.me will enable users to import multiple data sets to the Datavest platform).

[283] Meanwhile, Datum, Doc.ai, Ocean Protocol, Permission.io and Wibson offer DAT, NRN, OCN, ASK and WIN tokens, respectively.

[284] *See* Stone, *supra* note 281 (suggesting, *inter alia*, that the quantity and value of personal data are increasing exponentially and that, in the future, data investments will be more affordable than cash investments). *See also* POSNER & WEYL, *supra* note 22, at 231–32 (referring to consumers making data investments).

the data consumers supply and the services they receive. As a result, consumers have a very limited understanding of the transactions they enter. One way to deepen consumers' understanding is to assess ROD and actively bring ROD to their attention.

This Part proposes a conceptual roadmap for assessing ROD. As part of this thought experiment, it articulates four principles relating to the nature of ROD and the most appropriate use cases. Next, this Part explores ways to communicate ROD evaluations to consumers—with the goal of enabling them to experience and scrutinize data-for-services transactions. Lastly, this Part suggests that if consumers decide which transactions to enter on the basis of ROD, service providers will find it difficult to remain indifferent to ROD. To attract consumers, service providers will need to offer consumers greater benefits in exchange for the data they supply—creating a market in which data-driven companies compete to maximize consumers' ROD.

A. Evaluating Return on Data

Attempts to assess ROD are still in their infancy. There is no precise formula for gauging the relationship between the utility consumers gain and the data price they pay.[285] The articulation of general principles must, therefore, precede any more concrete proposals. Developers and lawmakers seeking to scrutinize data-for-services transactions need a common language. The following principles, explored in greater depth below, are an attempt to provide this common language:

1. *ROD gauges the relationship between the utility (U) consumers gain and the data (D) they supply in data-for-services transactions. Expressed as a ratio, ROD = U / D.*
2. *ROD evaluations need to be personalized and dynamic.*
3. *To assess ROD, you need to collect personal data.*
4. *ROD evaluations are most appropriate for comparing transactions in which similar services are provided.*

These principles do not endorse specific algorithms or other mechanisms for assessing ROD. They seek only to provide a tentative framework for developing tools to scrutinize data-for-services transactions. To explore how these principles can be implemented in practice, this Part gives particular attention to third party apps in mobile ecosystems. However, the principles equally apply to IoT devices and other emerging technologies.

1. ROD = U / D

ROD gauges the relationship between the two key metrics in data-for-services transactions: (i) the benefits consumers receive and (ii) the data price they pay. Calculating the ratio between these two metrics in a given data-for-services transaction yields the ROD. This is very different from Weigend's notion of "data efficiency," which relates to the purpose of data collection.[286] Data efficiency considers whether the data collected are a genuine input into the services provided. On this view, data are likened to fuel, which can be used with varying degrees of efficiency. For example, a mobile navigation app which collects only location data necessary for the user to reach the destination would be considered *data efficient*. In contrast, a mobile game which collects personal data unrelated to the game would

[285] *See supra* note 54 (regarding the difficulty in determining the value of data). *See also* WEIGEND, *supra* note 4, at 3119–3120.
[286] *See* WEIGEND, *supra* note 4, at 3048–3050ff; 3146–3158.

be considered *data inefficient*. In making these evaluations, data efficiency seeks to explore the actual uses of data, whether beneficial, nefarious or otherwise.

But the notion of data efficiency is problematic for several reasons. First, although data are indeed inputs into many services (in a way that monetary payments are typically not), the analogy between data and fuel is questionable. Unlike fuel, data are not fungible.[287] Second, it is not always clear which data (if any) are necessary for, or actually improve, the services provided.[288] Some data may contribute only to future developments, not present applications.[289] Are such data genuine inputs into the services? Third, the potential uses of data are not always apparent prior to or upon collection. The possibilities for downstream use are endless.[290] Therefore, the purpose of collection may emerge only later.[291] Fourth, data efficiency is arguably less likely than ROD to concern consumers.[292] After all, in ordinary retail transactions consumers do not fret over whether the money they pay *contributes* to the product they purchase. Rather, they conduct a cost-benefit analysis and weigh up the benefits of the product against its price, which is precisely the function of ROD.

The application of cost-benefit analysis to data-for-services deals raises another question. Should ROD factor in monetary payments which consumers may make (alongside data payments)? Uber, Lyft and other ride sharing services, for example, require consumers to pay both personal data and money. Factoring monetary payments into ROD would involve comparing two different forms of payment. This may require placing a monetary price on data, which is riddled with difficulties.[293] Factoring monetary payments into ROD may also stretch the cost-benefit analysis too far. ROD does not purport to capture every externality imposed on consumers.[294] Attention, opportunity costs and data leakage are difficult to quantify.[295] ROD measures only two metrics: (i) the (direct) benefits consumers receive; and (ii) the data price they pay (not the disutility of downstream data risks). It gauges the relationship between the utility consumers gain and the data they supply.

2. Personalized and Dynamic Insight

ROD is unique to each consumer. Different consumers can pay different data prices for similar services. A mobile app, for example, may collect different types and quantities of data from different users' devices. Consumers also relate to data collection in different ways. For example, some consumers are more sensitive than others to apps accessing a device's microphone.[296] In addition, the performance, and thus utility, of an app may vary across

---

[287] *See supra* note 55 (regarding the economic characteristics of personal data).
[288] *See* Narciso, *'Gratuitous' Digital Content Contracts*, *supra* note 202, at 205.
[289] *See, e.g.,* Timothy Morey et al., *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.
[290] *See, e.g.,* Hoofnagle & Whittington, *supra* note 20, at 647. *See also In re: WhatsApp*, ELECTRONIC PRIVACY INFORMATION CENTER (last visited __), https://www.epic.org/privacy/internet/ftc/whatsapp/ (describing the transfer by WhatsApp of its users' personal data to Facebook in 2016); Isaac, *supra* note 138.
[291] However, there may be methods to discern the purpose at an earlier point in time. *See, e.g.,* Haoyu Wang et al., *Understanding the Purpose of Permission Use in Mobile Apps*, ACM TRANS. INF. SYST. 35 (July 2017).
[292] *But see* Morey et al., *supra* note 290 (discussing surveys which indicate that consumers tend to see data-for-services transactions as more favorable where the data supplied contribute to the service received).
[293] *See supra* note 54 (regarding the difficulty in determining the value of data).
[294] *But see* Solove, *Privacy Self-Management*, *supra* note 89, at 1902 (suggesting that the focus of privacy law should be the downstream uses of data and associated risks, not their initial collection).
[295] WEIGEND, *supra* note 4, at 3146–3158, 3131–3135.
[296] *See* KPMG, *supra* note 99, at 4, 12 (demonstrating that people from different countries draw the line in dramatically different places with respect to privacy and data protection. For example, in the survey, 78% of Indian respondents found geo-location by taxi companies "cool" and 22% found it "creepy," while the findings for Danish respondents were the reverse.) *See also Chinese Willing to Lose Privacy for Convenience, Says*

different devices. Consumers also value services differently. A particular feature may be important to some consumers but not others. ROD must factor in these personalized, consumer-specific metrics.

Quantifying the more subjective metrics, such as the value which consumers attach to certain types of personal data or certain aspects of services, will be very challenging. Questionnaires and feedback could provide some insight into consumers' experiences. But analyzing consumers' actual interactions with services and data collection would be far more illuminating. For example, a consumer's decision to block apps from accessing location data could indicate that the consumer attaches significant value to location data. Similarly, a consumer's frequent use of a particular feature of an app could indicate that the consumer prizes that feature. But measuring frequency of use can be misleading as the value of some features, such as those designed for emergency situations, is not related to the frequency with which they are accessed. The utility function, like the corresponding loss function, is both complex and personal.

ROD varies not only among different consumers, but over time. The scope of data collection and the utility of services are not fixed.[297] For example, an app may modify the scope of data it collects; a consumer may alter an app's data collection permissions; an app's features may evolve; its performance may fluctuate over time; a consumer may change the way in which she uses an app and the value which she attaches to its features or different types of personal data. Clearly, data price and utility cannot be precisely calculated in advance. ROD evaluations must therefore be dynamic.[298]

Assessing ROD in real time requires using different metrics at different points in time. The *initial* ROD evaluation of a mobile app (upon installation or before it has been used) will probably need to rely on more generic, non-personalized metrics, as the information required to produce personalized evaluations can probably only be sourced from a consumer's actual interaction with the app.[299] An app's default data permissions could be instructive, as could the average ROD of other users of the app. In addition, a consumer's interactions with other apps could shine light on the types of personal data and services which she values. By contrast, *later* ROD evaluations (after the consumer has interacted with the app) could employ more personalized metrics, based on a consumer's actual interaction with the app. The scope of data collection actually occurring, app performance and the customer's engagement with different features will all be relevant.

Importantly, just as ROD evaluations will need to be dynamic and employ different metrics at different times, the conceptual framework of ROD will also need to adapt to changing circumstances. Clearly, the more ROD is used and refined, the more useful it will become. As data practices evolve, the principles for gauging the relationship between the data consumers supply and the services they receive will themselves need to change with time[300]—and remain transparent.[301]

Baidu CEO, EJI INSIGHT (Mar. 27, 2018), http://www.ejinsight.com/20180327-chinese-willing-to-lose-privacy-for-convenience-says-baidu-ceo/. *But see In China, Consumers Are Becoming More Anxious About Data Privacy*, ECONOMIST (Jan. 25, 2018), https://www.economist.com/china/2018/01/25/in-china-consumers-are-becoming-more-anxious-about-data-privacy.

[297] *See* WEIGEND, *supra* note 4, at 3213–3216.

[298] *Cf id.* at 5349–5352 (arguing that frequent updates to the ROD metrics would make it difficult for consumers to conduct meaningful comparisons between different service providers.)

[299] *See generally* Andrew I. Schein et al., *Methods and Metrics for Cold-Start Recommendations*, ACM SIGIR 253 (2002); Xuan Nhat Lam et al., *Addressing Cold-Start Problem in Recommendation Systems*, ACM UBIQ. INFO. MANAG. & COMMUNICATIONS 208 (2008); Blerina Lika et al., *Facing the Cold Start Problem in Recommender Systems*, EXPERT SYS. APPLICATIONS 2065 (2014).

[300] *See id.* at 3234–3237. *See also* Strandburg, *supra* note 28, at 145.

[301] *See infra* note 331 (regarding algorithmic accountability).

3. It Takes Data to Evaluate ROD

Calculating ROD is a data-intensive process. Information regarding both data collection and consumer behavior is necessary to gain insight into data-for-services transactions. Consumers will need to supply an ongoing stream of personal data in order to receive dynamic, personalized ROD evaluations. Weigend calls this the "*Give to Get*" philosophy: "If you want your decision-making to be improved by data, you usually have to agree to having your data collected . . . ."[302] As is the case for privacy tech and other personalized services, data collection is a pre-requisite for generating ROD evaluations.[303] It is the price of making data-for-services transactions more transparent.

Many data points are required to measure the data which consumers supply and the utility they gain in data-for-services transactions. In the context of mobile ecosystems, an app's privacy policy, its data permissions and the applicable regulatory framework may be informative. But these only reflect the *potential* scope of data collection. Assessing the *actual* scope of data collection relies on monitoring an app's outbound data. The encryption and compression of outbound data pose additional challenges.[304] Assessing only the quantity of data collected is obviously inadequate. The type and quality of data matter. For example, Social Security numbers and private Bitcoin keys are highly sensitive and valuable despite their small size.

Several of these data points are contained in the communications between a mobile app and the device's operating system. Whenever an app seeks to access data from the device (e.g., location data, camera access), it sends an API request to the operating system.[305] For example, Skype must send an API request to access the device's microphone. The operating system then responds by delivering the requested data. Given that operating systems receive all API requests made by apps, they can closely monitor the data collection carried out by different apps.[306] In the case of Skype, this would include the length of calls and associated metadata. Apple and Google, the proprietors of the iOS and Android operating systems, have full access to these APIs. For the time being, they hold the keys to monitoring the data which consumers share with mobile apps.

Mobile apps owned by Google and Apple, such as Google Calendar and Apple Music, complicate ROD evaluations.[307] As explained, Google and Apple can, via API requests, indirectly access most data collected by mobile apps. Accordingly, monitoring the API requests sent by Google Calendar to Android (Google's own operating system) would not be

---

[302] WEIGEND, *supra* note 4, at 229–236. *See also id.* at 145. In addition, the title of Weigend's book is "Data *for* the People" (emphasis added). *But see* Lydia Nicholas, *The High Cost of Being Digital*, NEW SCIENTIST (Feb. 8, 2017), https://www.newscientist.com/article/mg23331120-900-the-high-cost-of-being-digital/ (accusing Weigend of "data utopianism"). *See also* David A. Hoffman & Patricia A. Rimo, *It Takes Data to Protect Data*, *in* PRIVACY HANDBOOK, *supra* note 50, at 546.

[303] *See, e.g.,* Molly McLaughlin, *The Best Privacy and Security Apps for Android*, LIFEWIRE (May 2, 2018), https://www.lifewire.com/privacy-and-security-apps-for-android-4116583 (comparing Google search, which collects personal data and provides customized results, with DuckDuckGo, which does not).

[304] *See supra* note 232 (discussing the information which can be gleaned from metadata).

[305] *See generally* Jenn Chen, *What Is an API & Why Does It Matter?*, SPROUT SOCIAL (Jan. 31, 2018), https://sproutsocial.com/insights/what-is-an-api/; WEIGEND, *supra* note 4, at 3601–3606.

[306] But operating systems may find it difficult to monitor passive data collection, such as data relating to a user sourced from the activities of others. *See supra* note 61 (regarding passive data collection).

[307] 23 of the 25 most-downloaded Android apps are owned by either Google or Facebook. *See Android Market History Data and Ranklists*, ANDROIDRANK (last visited __), https://www.androidrank.org/. *But see* Sam Schechner, *Google Will Charge Phone Makers to Pre-Install Apps in Europe*, WALL ST. J. (Oct. 16, 2018), https://www.wsj.com/articles/google-will-charge-phone-makers-to-pre-install-apps-in-europe-1539707606 (suggesting that the demand for these apps may decline).

instructive. That Google Calendar may, for example, collect location data is uninformative; Google *already* has the ability to, and perhaps already does, collect location data via the Android operating system or other Google apps, such as Google Maps. Seen in this light, data-for-services transactions involving apps owned by Google and Apple are part of the much larger transactions with Google and Apple.[308] Consumers do not share specific data with Google in exchange for using Google Calendar. Google already collects data from consumers in various contexts and, in return, provides them with a wide array of services. ROD may therefore need to be evaluated in relation to the proprietor of each app, rather than in relation to the app itself (on a per-app basis).[309]

Just as many data points are needed to assess the data price which consumers pay in data-for-services transactions, many data points are needed to assess the utility which consumers gain. Exploring which metrics can best serve as a proxy for consumer utility and deciding what weight to place on each of them will be challenging. A significant number of the services which data-driven companies provide are "experience goods" or "credence goods" (such as professional services), the quality of which is difficult for consumers to evaluate, even post-fact.[310] Consumer ratings of apps, app popularity and comparisons with competing apps may shed light on an app's utility.[311] Technical metrics, such as app performance, and personal metrics, such as the frequency of use and the user's specific type of use, are also informative.[312] More subjective metrics, such as an individual's personal assessment of an app's features, should also be considered.[313]

But subjective metrics, whether relating to utility or data price, are difficult to quantify.[314] How can one measure the value of forging a new relationship via a dating app or finding a dream job on LinkedIn?[315] How can one calculate an individual's personal sensitivity to certain types of data collection? Answering all of these questions is beyond the scope of this article. Nevertheless, to holistically reflect the data price which consumers supply and the utility they gain, ROD evaluations will need to factor in certain subjective metrics. Capturing these subtle insights is likely to require further access to personal data.

---

[308] A similar issue complicates ROD evaluations of apps owned by Facebook (e.g., WhatsApp and Instagram) and Microsoft (e.g., Skype and LinkedIn). *See also* Isaac, *supra* note 138 (regarding Facebook's plans to consolidate the infrastructure of the various platforms which it owns).

[309] The per-app approach may also be problematic as most data are accessed through third party libraries which function across multiple apps. *See* Saksham Chitkara et al., *Does this App Really Need My Location? Context-Aware Privacy Management for Smartphones*, ACM INTERACT. MOB. WEARABLE UBIQ. TECH. 1 (Sept. 2017). Further, given that the infrastructure of certain tech firms (especially Google) is ubiquitous and their utility is provided and experienced across many applications, the per-(app) proprietor approach may also be problematic.

[310] *See* Strandburg, *supra* note 28, at 131–32. *See generally* Uwe Dulleck & Rudolf Kerschbamer, *On Doctors, Mechanics, and Computer Specialists: The Economics of Credence Goods*, 44 J. ECON. LIT. 5 (2006) (discussing how vendors can use information asymmetries to overcharge consumers). *See also* Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 AM. ECON. REV. 941 (1963).

[311] Some of these already feature in Google Play, Apple's App Store and third party comparison sites. *See e.g., Snapchat vs. WhatsApp*, VERSUS (last visited __), https://versus.com/en/snapchat-vs-whatsapp.

[312] *See* WEIGEND, *supra* note 4, at 3181–3184. But simple measurements of screen time and data consumption are poor indicators of utility. Whilst watching Netflix may consume large quantities of data and involve lengthy screen time, its utility is not necessarily greater than that of an email client. More importantly, video streaming and email clients provide very different types of utility. *See infra* Part V.A.4.

[313] This could be gleaned from consumer experience questionnaires similar to Net Promoter assessments. *See generally What Is Net Promoter?*, NICE SATMETRIX (last visited __), https://www.netpromoter.com/know/.

[314] *See* WEIGEND, *supra* note 4, at 3140; 3176–3179.

[315] *Id.* at 2911–2916.

4. Assessing Comparable Transactions

ROD evaluations will, at least initially, only be helpful in assessing comparable data-for-services transactions. The range of services provided in data-for-services transactions—from Microsoft's LinkedIn to Amazon's Alexa—is vast. Different mobile apps, for instance, perform very different functions. Dropbox stores files in the cloud. Fitbit provides health and exercise insights. Instagram connects people through shared media. Comparing the utility which a consumer gains from one of these apps with another would be meaningless.[316]

The key is to compare like with like. For example, Skype, LINE, Viber and Tango all provide similar services, namely, voice and video calls. Therefore, comparing their respective sound and picture quality, connection reliability and user experience would be instructive. Indeed, many mobile apps offer similar services. Consider the competing apps within each of the following categories: music (e.g., Spotify and SoundCloud), podcasts (e.g., Stitcher and TuneIn), cloud storage (e.g., Dropbox and OneDrive), productivity (e.g., Microsoft Office and OfficeSuite or Quick PDF Scanner and CamScanner), and photo sharing (e.g., Flickr and Imgur).[317] Consider also competing voice assistants: Alexa, Siri and Google Assistant. Each of these categories is ripe for ROD evaluation.

Going forward, additional use cases are likely to emerge as new categories of apps and IoT devices are developed for smart homes and smart cities.[318] In the meantime, there is certainly no shortage of opportunities for deploying ROD. Comparable mobile apps and voice assistants are prime candidates for quantifying utility and measuring the type and quantity of data collection. It is these ROD evaluations, which asses the utility and data price of similar services, which are most likely to draw consumer attention.[319] They will reveal which services within a given category provide the highest utility to data price ratio, enabling consumers to comparison shop—and make informed choices when deciding between similar services offered by competing providers.

B. Transactional Transparency and Choice Architecture

Assessing ROD cannot alone make data-for-services transactions fully transparent. Alongside developing tools to measure data price and utility, we need to communicate the ROD paradigm to consumers. ROD needs to be salient. Although it is widely understood that many technologies are data-intensive, public attention remains overwhelmingly focused on privacy. Consumers do not appreciate the transactional nature of their relationships with data-driven companies. To understand and *experience* the bargains facilitated by these relationships, consumers need to engage in a cost-benefit analysis.

Simplicity is key. ROD should convey only the most essential transactional information. The average consumer needs to be cognizant of what they give to, and receive

---

[316] Even apps which provide ostensibly similar services are not necessarily comparable, often because of their respective network effects. Consider social networking and other relationship apps, such as Tinder and Bumble, whose utility is intimately related to the groups of people they capture and create. *See, e.g.,* Case M.8124, Microsoft / LinkedIn, 2016 E.C. 139/2004 ¶ 341 (Dec. 6, 2016), *available at* http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf (regarding the benefits of network effects); *Rise of Data Capital*, ORACLE & MIT, *supra* note 55, at 7 (differentiating between direct and indirect network effects).

[317] Mobile payments apps, health and lifestyle services and ride sharing may also provide similar services, however many of these also involve monetary payments. *See supra* Part V.A.1.

[318] *See generally* Kelsey Finch & Omer Tene, *Smart Cities: Privacy, Transparency, Community*, *in* PRIVACY HANDBOOK, *supra* note 50, at 125.

[319] *See* Xia et al., *supra* note 108, at 3–4 (explaining that consumers tend to pay greater attention to price discrepancies between similar products).

from, service providers.[320] Transparency-enhancing technologies can help develop practical, consumer-friendly tools to report ROD evaluations to consumers.[321] These tools will relieve consumers of the burden of conducting overly complex analysis and associated cognitive overhead.[322] Richard Thaler calls these tools *choice engines*.[323] By providing information to consumers in palatable formats, choice engines will enable consumers to reflect on the data prices they pay and the services they receive. Consciously thinking through the pros and cons of each data-for-services deal, consumers will make slower, more deliberative decisions.[324]

Visualizing ROD could be particularly helpful. Currently, several browsers use visual symbols to communicate to users the security status of the websites they visit.[325] Google Chrome, for example, uses different symbols to flag whether a website is secure, unsecure or highly unsecure.[326] A similar interface could communicate ROD. A sliding scale (or traffic light system) could color-code transactions according to their ROD—green for high ROD; amber for intermediate ROD; and red for low ROD.[327] A red light might, for example, be displayed where a VOIP mobile app continuously collects audio and visual data (even when no call is in session) and provides poorer quality calls than other VOIP apps. Meanwhile, a green light might be displayed where a VOIP app collects smaller quantities of sensitive data but still provides high quality calls.

Understandably, some consumers may want more granular ROD insights. They may wish to know which data points and metrics contribute to ROD. User interfaces should be developed to effectively convey this information.[328] These could be similar to "Schumer boxes," which outline to consumers the key terms of credit card agreements.[329] For ROD, it may be helpful to illustrate the precise factors which establish the ratio between the data a consumer supplies and the utility she receives in a given transaction. Yet, the ROD output—insights into, and assessments of, data-for-services transactions—is not sufficient. The mechanics of ROD evaluations must themselves be transparent. Without disclosing the ROD algorithm, those conducting ROD evaluations could not be held accountable.[330] But,

---

[320] *See* Kevin Cochrane, *To Regain Consumers' Trust, Marketers Need Transparent Data Practices*, HARV. BUS. REV. (June 13, 2018), https://hbr.org/2018/06/to-regain-consumers-trust-marketers-need-transparent-data-practices. *See generally* F.A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 526–27 (1945) (regarding the function of prices in supplying information to purchasers).

[321] *See generally* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1414 (2011); Christian Zimmermann, *A Categorization of Transparency-Enhancing Technologies* (revised July 22, 2015), https://arxiv.org/abs/1507.04914; Urs Gasser, *Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy*, 130 HARV. L. REV. F. 61, 65 (2016). *See, e.g.,* Javier Parra-Arnau et al., *MyAdChoices: Bringing Transparency and Control to Online Advertising*, 11 ACM TRANS. WEB 1 (2017) (proposing tools for fine-grained control over advertising, in place of all-or-nothing ad-blockers).

[322] POSNER & WEYL, *supra* note 22, at 244–5. However, as consumers do not currently dedicate time or resources to deliberating over data-for-services transactions, the introduction of ROD may actually impose on consumers new costs.

[323] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARV. BUS. REV. (Jan.–Feb. 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.

[324] *See generally* KAHNEMAN, *supra* note 93.

[325] *See What is an SSL Certificate?*, SYMANTEC (last visited __), https://www.symantec.com/page.jsp?id=ssl-information-center#.

[326] *Check If a Site's Connection Is Secure*, GOOGLE CHROME HELP (last visited __), https://support.google.com/chrome/?p=ui_security_indicator.

[327] *See* KPMG, *supra* note 99, at 19; WEIGEND, *supra* note 4, at 3221–3229 (likening the ROD scale to energy-efficiency ratings of appliances).

[328] *See, e.g.,* GHOSTERY, *supra* note 237 (which displays both simple and detailed dashboards).

[329] *See* Fair Credit and Charge Card Disclosure Act of 1988, Pub. L. No. 100-583, § 2, 102 Stat. 2960 (1988).

[330] *See generally* Berkeley J. Dietvorst et al., *Algorithm Aversion: People Erroneously Avoid Algorithms After Seeing Them Err,* 144 J. EXP. PSYCHOL. GEN. 114 (2015); Aaron Smith, *Public Attitudes Toward Computer Algorithms*, PEW RESEARCH CENTER (Nov. 16, 2018), http://www.pewinternet.org/2018/11/16/public-attitudes-toward-computer-algorithms/. *See also* Christian Sandvig et al., *Auditing Algorithms: Research Methods for*

arguably, the more transparent the ROD algorithm, the higher the chances of companies successfully gaming it and building apps with artificially high ROD.[331]

In the context of mobile ecosystems, there are many potential ways to communicate ROD evaluations to consumers. Apple's App Store and Google Play could display ROD scores in each app's profile, which would feature alongside other information (such as an app's rating and popularity). ROD evaluations could also be displayed in the settings portals of devices or as pop-ups within apps[332]—which would enable consumers to regularly monitor the ROD of the apps they actually use. Making ROD salient will help consumers perceive their relationships with data-driven companies as transactional. Being presented with ROD evaluations, consumers will be in a position to judge for themselves the merits of each data-for-services exchange.

The introduction of transactional transparency through ROD could have a significant impact on consumers' decisions. Behavioral studies demonstrate that consumers do not make decisions in a vacuum. They are affected by a variety of factors, including default options, status quo bias and the information presented to (or withheld from) them.[333] The shaping of the environment in which consumers make decisions is known as *choice architecture*.[334] Acquisti observes that:

> [E]very design decision behind the construction of every online (e.g., software, online social networks, online blogs, mobile devices and applications, etc.) or offline (e.g., conference rooms, vehicles, food menus, etc.) system or tool we use has the potential to influence users' behaviors, regardless of whether the designer, or the user, is fully aware of those influences and their consequences. In simple terms, there is no such thing as a neutral design in privacy, security, or anywhere else.[335]

Put differently, every design choice is a *nudge*. Sunstein and Thaler define a nudge as any mechanism designed to "alter[] people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives."[336] With the assistance of behavioral insights, choice architecture can be used to nudge consumer decision making.[337] This is certainly the case for decisions relating to personal data. In one study,

---

Detecting Discrimination on Internet Platforms, 64TH MEETING INT'L COMMUNICATION ASSOC. (May 22, 2014); PASQUALE, *supra* note 259, at ch. 5; Paul Hitlin & Lee Rainie, *Facebook Algorithms and Personal Data*, PEW RESEARCH CENTER (Jan. 16, 2019), http://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/.

[331] *See* Hacker & Petkova, *supra* note 251, at 17; JERRY MULLER, TYRANNY OF METRICS 3, 24, 77, 149 (2018). *See also* POSNER & WEYL, *supra* note 22, at 238 (discussing a Microsoft experiment in which a personal data payment system was exploited by rogue bots).

[332] *See* Rebecca Balebako et al., *The Impact of Timing on the Salience of Smartphone App Privacy Notices*, CCS SECURITY & PRIVACY IN SMARTPHONES & MOBILE DEVICES 63 (2015) (suggesting that consumers may pay greater attention to information provided within an app, compared with information available on an app store).

[333] *See* THALER & SUNSTEIN, *supra* note 103, at 3; Richard H. Thaler et al., *Choice Architecture* (Working Paper, Apr. 2, 2010), *available at* http://papers.ssrn.com/abstract=1583509.

[334] *Id.*

[335] Acquisti et al., *Nudges*, *supra* note 87, at 32. *See also* Ron Hirschprung et al., *Analyzing and Optimizing Access Control Choice Architectures in Online Social Networks*, ACM TRANS. INTELL. SYST. TECH. (May 2017); Idris Adjerid et al., *Choice Architecture, Framing, and Cascaded Privacy Choices*, MANAG. SCI. (2018).

[336] THALER & SUNSTEIN, *supra* note 103, at 6. *See also* Cass R. Sunstein & Richard Thaler, *Libertarian Paternalism,* 93 AM. ECON. REV. 175 (2003); Cass R. Sunstein & Richard Thaler, *Libertarian Paternalism Is Not an Oxymoron,* 70 U. CHI. L. REV. 1159 (2003).

[337] The term "behavioral insights" originates from the UK Cabinet Office's Behavioural Insights Team. *See* BEHAVIOURAL INSIGHTS TEAM (last visited __), http://www.behaviouralinsights.co.uk/.

individuals were more willing to pay a premium for privacy friendly mobile apps where a selection of less privacy friendly apps was also made available to them.[338]

In recent years, several economists and computer scientists have proposed techniques for nudging consumers to protect their privacy.[339] They suggest that disclosing privacy risks will mitigate consumers' tendency to overlook and underestimate these risks.[340] Where the risks are salient, consumers are more likely to take them seriously. In addition, framing privacy risks as costs or burdens will appeal to consumers' reluctance to bear losses and, thereby, encourage them to better protect personal data relating to them.[341]

However, these choice architecture proposals relate only to privacy.[342] They do not advocate comparing the data consumers supply with the utility they gain. Nor do these proposals seek to disclose ROD or incentivize consumers to demand better deals from service providers. Like most of the legal frameworks and data platforms which have been discussed, choice architecture relating to personal data is preoccupied with privacy. This need not be the case. *Choice architects can nudge ROD.*

Communicating ROD evaluations to consumers would frame their interactions with data-driven companies as genuine transactions. If data-for-services transactions were transparent, consumers would realize that the services they consume are not free, but paid for with personal data. Nudging ROD would reduce the information asymmetry between consumers and companies. It could tackle, and perhaps harness, several cognitive and behavioral biases. If the data price were disclosed to consumers, consumers would be less likely to overlook the longer-term costs of trading personal data. Upon seeing data collection as a price, consumers may be more selective in deciding which transactions to enter.[343]

ROD nudges could be more or less robust; that is, they could employ different degrees of forcefulness. For example, by simultaneously displaying the ROD of comparable mobile apps, app stores could nudge consumers toward selecting apps with higher ROD.[344] This would be a relatively soft nudge, as it would only provide information. It would not impact consumers' ability to access apps with lower ROD. A more robust nudge could, for example, engineer the search results in an app store to give priority to apps with higher ROD. This nudge would be more forceful as it would significantly alter the choices presented to consumers. It might even border on a *shove*.[345] Yet, it would still not impose a particular choice. A consumer could, after a longer search, nonetheless opt for an app with lower

---

[338] *See* Serge Egelman et al., *Choice Architecture and Smartphone Privacy: There's a Price for That*, WEIS ECON. INFO. SECURITY 211 (2013).

[339] *See, e.g.,* Hazim Almuhimedi et al., *Your Location Has Been Shared 5398 Times! A Field Study on Mobile Privacy Nudges*, ACM CHI HUMAN FACTORS COMPUT. SYS. (2015).

[340] *See* Acquisti et al., *Nudges*, *supra* note 87, at 13–14 (explaining how disclosing information about these risks may overcome the availability and overconfidence biases).

[341] *See id.* at 17.

[342] However, some data-driven companies have begun to use nudges for other purposes. *See, e.g.,* Heather Schwedel, *Gmail's New Nudge Feature Is a More Efficient Way to Feel Guilty About Your Inbox*, SLATE (May 21, 2018), https://slate.com/technology/2018/05/gmails-nudge-feature-is-a-more-efficient-way-to-feel-guilty-about-your-inbox.html.

[343] Yet, it need not altogether deter them from using data-driven services. *See, e.g.,* Salesforce, *supra* note 41, at 9 (indicating that consumers demand *both* personalized services and transparency around the use of personal data).

[344] *See* Serge Egelman et al., *Timing Is Everything?: The Effects of Timing and Placement of Online Privacy Indicators*, ACM SIGCHI HUMAN FACTORS COMPUT. SYS. 319 (2009) (explaining that nudges are most effective when introduced prior to consumers committing to particular choices).

[345] *See* Dan M. Kahan, *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem*, 67 U. CHI. L. REV. 607 (2000); THALER & SUNSTEIN, *supra* note 103, at 6 (explaining that where a design choice is very forceful, it will not constitute a nudge. "Putting fruit at eye level counts as a nudge. Banning junk food does not").

ROD.[346] ROD nudges, by definition, leave consumers free to choose for themselves which services to purchase with the personal data they generate.[347] Nudging ROD would merely enable consumers to engage in a cost-benefit analysis and consciously weigh the pros and cons of each transaction.

C. Consumer Engagement and Competition

Different economic actors could introduce ROD nudges in different ways.[348] Government regulators, for example, could require that mobile operating systems assess and disclose the ROD of third party apps to consumers.[349] Apart from the political impediments to adopting such regulation, this proposal could have unintended consequences. After all, it would not *incentivize* companies to embrace ROD, but *compel* them to do so. By mandating that companies comply with onerous requirements, such regulation could stifle the technological innovation and risk-taking which drive the data economy.[350]

One alternative is industry self-regulation. Rather than mandate particular courses of action, self-regulation relies on companies *voluntarily* pursuing favorable policies.[351] Under this model, companies could decide to assess ROD and choose how to engage consumers. But, in the absence of mandatory regulation, why would data-driven companies volunteer to make data-for-services transactions more transparent? Why would they choose to subject their businesses to unnecessary scrutiny and threaten the highly profitable status quo?[352] One reason is that data-driven companies are facing a crisis of confidence, particularly in the wake of high-profile privacy scandals.[353] Data-driven companies want to be seen to proactively tackle concerns relating to personal data.[354] Although public attention is largely focused on protecting consumer privacy, the notion that consumers deserve to receive more in return for the personal data they supply may be gaining traction. Voluntary ROD evaluations could

---

[346] A consumer may do this because she trusts the app developer. *See generally* Morey et al., *supra* note 290 (explaining that consumers supply to companies they consider trustworthy more valuable data in exchange for comparable services). *See also* Tim Cooper, *If Data Is Money, Why Don't Businesses Keep It Secure?*, HARV. BUS. REV. (Feb. 10, 2015), https://hbr.org/2015/02/if-data-is-money-why-dont-businesses-keep-it-secure (emphasizing the significance of trust in the data economy).

[347] *See* Adjerid et al., *Choice Architecture, Framing, and Cascaded Privacy Choices*, *supra* note 335, at 43; Acquisti et al., *Privacy and Human Behavior in the Age of Information*, *supra* note 103, at 509–10.

[348] *See generally* Acquisti et al., *Nudges*, *supra* note 87, at 29.

[349] *See* Thaler & Tucker, *supra* note 323 (arguing that regulation should be used to jump-start the introduction of nudges); SCHNEIER, DATA AND GOLIATH, *supra* note 3, at 198 (discussing a regulatory proposal requiring all mass data collectors to file "Privacy Impact Notices"); WEIGEND, *supra* note 4, at 3221–3229 (advocating the establishment of a regulatory body to evaluate companies' data protection systems).

[350] *See* Jack Goldsmith, *The Ends of Privacy*, NEW RAMBLER (2015), http://newramblerreview.com/book-reviews/law/the-ends-of-privacy. *See generally* ADAM THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM (2014).

[351] *See* Acquisti et al., *Economics of Privacy*, *supra* note 51, at 42–44. For criticism of privacy self-regulation, *see* Litman, *supra* note 181, at 1283, 1287; Lemley, *Private Property*, *supra* note 179, at 1554–55; Ira S. Rubinstein, *The Future of Self-Regulation Is Co-Regulation*, *in* PRIVACY HANDBOOK, *supra* note 50, at 503.

[352] *See* POSNER & WEYL, *supra* note 22, at 234; Acquisti et al., *Nudges*, *supra* note 87, at 29.

[353] *See* Sam Schechner, *Privacy Problems Mount for Tech Giants*, WALL ST. J. (Jan. 21, 2019), https://www.wsj.com/articles/privacy-problems-mount-for-tech-giants-11548070201; *supra* note 116 (regarding the lack of trust in data-driven companies).

[354] Although Apple and Google might be reluctant to subject third party mobile apps to ROD evaluations—after all, iOS and Android reap enormous benefits from third party apps—doing so might direct scrutiny away from Apple and Google. *See, e.g.,* Apple Inc. v. Pepper, No. 17-204 (S. Ct. 2018) (alleging that Apple's use of the App Store breaches antitrust laws). It may also give them a public relations advantage over privacy-infringing rivals. *See, e.g.,* Kevin Roose, *Maybe Only Tim Cook Can Fix Facebook's Privacy Problem*, N.Y. TIMES (Jan. 30, 2019), https://www.nytimes.com/2019/01/30/technology/facebook-privacy-apple-tim-cook.html.

improve these companies' tarnished reputations and bolster trust among current and prospective customers.[355]

If data-driven companies embrace ROD, data prices will become more elastic and better correlate with the utility of the services they provide. Consumers will, in turn, take greater interest in ROD because paying a higher data price—whether in terms of the quantity or quality of data—will potentially buy them better services. By deciding on the basis of ROD which services to purchase, consumers could signal their preferences to service providers (namely, lower data prices and higher quality services). If, in due course, a critical mass of consumers generates sufficient demand for greater ROD, companies will have to respond by increasing ROD.[356] Then, once several major service providers offer consumers greater ROD, others will have to follow or risk losing business. A competitive market will emerge. To retain and attract ROD-conscious consumers, companies will need to pay close attention to the ROD they offer. They will have to carefully consider the relationship between the data collection they carry out and the services they provide. With strong incentives to improve the quality of their services and rethink the scope of data collection, data-driven firms will have skin in the game.

At the same time, new market entrants, by offering consumers superior data-for-services deals, could draw business away from the tech giants.[357] Companies which are early to embrace ROD may have a first-mover advantage. ROD-conscious consumers, aware of the transactional value of personal data, will be more willing to share valuable data with companies offering competitive ROD deals.[358] Thus, startups which offer greater ROD will receive higher quality and more relevant data from consumers, which will give them an edge over larger rivals, not only in performing consumer and product analytics, but in developing and training AI.[359] ROD-driven competition could, in this way, disperse market power among different service providers.[360] New market entrants could, in time, even challenge the dominance of the FANGs, BATs and other incumbents.[361]

---

[355] *See, e.g.,* Jonathan Vanian, *Facebook Is the Least Trusted Major Tech Company When It Comes to Safeguarding Personal Data, Poll Finds*, FORTUNE (Nov. 8, 2018), http://fortune.com/2018/11/08/mark-zuckerberg-facebook-reputation/. In addition, perhaps falls in their stock prices may prompt data-driven companies to consider bold new opportunities, such as ROD. *See Big Tech's Sell-Off*, *supra* note 29.

[356] Consumer herd mentality could drive additional consumers to take interest in the ROD they receive and integrate it into their decision making. *See also* POSNER & WEYL, *supra* note 22, at 234, 241–43.

[357] *See generally* Mireille Hildebrandt, *Primitives of Legal Protection in the Era of Data-Driven Platforms*, 2 GEO. L. TECH. REV. 252 (2018) (describing certain data-driven platforms as monopolies and monopsonies).

[358] *See* POSNER & WEYL, *supra* note 22, at 231–2.

[359] *Id*. at 220–1 (discussing LANIER, *supra* note 19, explaining that the failure of "siren servers" to pay their users for data disincentivizes users from supplying the most valuable data). *See also id.* at 225–30 (arguing that companies' transition from standard statistics to ML-enhanced analysis will facilitate increasing marginal returns on personal data). *See also* Arrieta-Ibarra et al., *Should We Treat Data as Labor?*, AEA, *supra* note 26, at 41. *But see* Dan Breznitz, *Balancing Privacy and Commercial Values Data and the Future of Growth: The Need For Strategic Data Policy*, CENTER FOR INTERNATIONAL GOVERNANCE INNOVATION (Apr. 19, 2018), https://www.cigionline.org/articles/data-and-future-growth-need-strategic-data-policy (suggesting that companies already benefit from increasing marginal returns on personal data).

[360] *See* Stucke, *supra* note 66, at 303–7 (suggesting that large tech corporations can have a chilling effect on innovation); Noah Smith, *Big Tech Sets Up a 'Kill Zone' for Industry Upstarts*, BLOOMBERG (Nov. 7, 2018), https://www.bloomberg.com/opinion/articles/2018-11-07/big-tech-sets-up-a-kill-zone-for-industry-upstarts. *See also* Kiran Stacey, *Senior Democrat Suggests 'Glass-Steagall' Law for Tech Companies*, FINANCIAL TIMES (Mar. 4, 2019), https://www.ft.com/content/561b8546-355c-11e9-bd3a-8b2a211d90d5; Elizabeth Warren, *Here's How We Can Break Up Big Tech*, MEDIUM (Mar. 8, 2019), https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c.

[361] *See generally* Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2016); FRANKLIN FOER, WORLD WITHOUT MIND: THE EXISTENTIAL THREAT OF BIG TECH (2017); TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE (2018); SARAH SPIEKERMANN & WOLFIE CHRISTL, NETWORKS OF CONTROL: A REPORT ON CORPORATE SURVEILLANCE, DIGITAL TRACKING, BIG DATA & PRIVACY (2018);

VI. CONCLUSION

This article has not proposed abolishing the data-for-services business model. Rather, it has sought to make the case for a new analytical apparatus—*return on data (ROD)*. As we debate the future of U.S. data law, including the introduction of new federal privacy legislation, we must acknowledge that privacy is not the only issue at stake. We should also consider what consumers receive in exchange for the data they share. Most legal frameworks and many data platforms remain preoccupied with privacy and continue to overlook the give-and-take which characterizes the data economy. This article aims to buck that trend and challenge the privacy paradigm. By proposing principles for assessing the relationship between the data consumers supply and the utility they receive, this article seeks to grapple with the exchange underpinning data-for-services transactions.

In addition to refining the precise mechanics of ROD evaluations, conveying these evaluations to consumers is equally important in making data-for-services transactions more transparent. Consumers should understand the transactional nature of their relationships with data-driven service providers. Showcasing the ROD of competing services will help consumers become conscious of the trade-offs they make. Equipped with this understanding, consumers will be able to make better informed decisions regarding which data-for-services deals to accept, and which to reject.

The introduction of ROD clearly warrants further investigation. Who will develop and test practical models for assessing ROD? Will these be scalable? How can we mitigate the risk of ROD evaluations being manipulated or gamed by sophisticated service providers? Notwithstanding these important questions, we can assume that if consumers begin to factor ROD into their decision making, data-driven service providers will need to respond. If consumers decide which services to use even partly on the basis of ROD, data-driven firms will be incentivized to increase the ROD they offer. To compete for the business of ROD-conscious consumers, service providers will need to reduce the scope of data collection and improve the quality of services.

Looking forward, emerging technologies are expected to increase the size, complexity and accuracy of our data footprints. Although data-for-services transactions are unlikely to disappear in the near future, new legal frameworks and data platforms may begin to treat them differently. Consumers may question the often arbitrary relationship between the personal data they supply and the services they receive. While it is difficult to envisage exactly how consumers and companies will engage with ROD, now is the time to reflect on the possibilities.

MARTIN MOORE & DAMIAN TAMBINI, DIGITAL DOMINANCE: THE POWER OF GOOGLE, AMAZON, FACEBOOK, AND APPLE (2018); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).