YALE LAW & POLICY REVIEW

# Return on Data:

# Personalizing Consumer Guidance in Data Exchanges

*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 consumers receive. This article, drawing on the emerging field of personalized law, suggests that privacy concerns should not be viewed in isolation, but as part of ROD. Just as businesses can quantify return on investment (ROI) to optimize investment decisions, individual consumers should be able to assess ROD in order to make informed decisions on how to spend and invest personal data. Making ROD transparent will enable consumers to navigate the range of data-for-services deals on offer, evaluate their merits, and negotiate their terms. Pivoting from the privacy paradigm to ROD will also incentivize technology companies to offer consumers higher ROD, as well as create opportunities for new market entrants.*

## I. INTRODUCTION

Many technology 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 Big Tech firms and other service providers rely on consumers trading personal data for services. Consumers,

* Associate, Yigal Arnon & Co. 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. The views expressed in this article are the author's own and should not be attributed to any company or organization.

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 [https://perma.cc/84SQ-9C4M] [hereinafter *Senate Hearing*] ("There will always be a version of Facebook that is free."); s*ee 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 [https://perma.cc/VH36-64CU].

in effect, pay for services with personal data.[2] The bargain is data for services. Although lawmakers have addressed the erosion of privacy, they have not directly confronted this bargain, which is now at the core of the increasingly post-privacy economy.[3] Privacy and data protection continue to monopolize the debate. Change is overdue. We must begin to explore the notion of return on data (ROD)—*the relationship between the price consumers pay, in the form of personal data, and the utility of the services they receive*.

Skepticism around the prevailing privacy paradigm is growing. Brittany Kaiser, former Business Development Director at Cambridge Analytica, provocatively declared that "[p]rivacy just isn't possible in the post-Facebook crisis era . . . . Just like with Airbnb – if somebody is going to come and use your physical assets, you would expect to agree [on] 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?"[4] Kaiser's remarks are revealing. Apart from implying that we can no longer adequately protect

2. *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 1, 47 (2015); MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY § 1.26 (2016); Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1420 (2017) [hereinafter *Paying for Privacy*]; *see, e.g.*, 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 [https://perma.cc/CC4U-P4VK]; 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 [https://perma.cc/LAR4-4LHR]; 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 [https://perma.cc/2PK6-YNYW].

3. *See* ANDREAS S. WEIGEND, DATA FOR THE PEOPLE: HOW TO MAKE OUR POST-PRIVACY ECONOMY WORK FOR YOU 969 (2017); *The End of Privacy (Special Issue)*, 347 SCIENCE 490 (2015).

4. 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 [https://perma.cc/346L-57LU]. *See generally* BRITTANY KAISER, TARGETED: THE CAMBRIDGE ANALYTICA WHISTLEBLOWER'S INSIDE STORY OF HOW BIG DATA, TRUMP, AND FACEBOOK BROKE DEMOCRACY AND HOW IT CAN HAPPEN AGAIN (2019).

personal data, she asserts that we must scrutinize what consumers receive *in return* for the data they supply.

Lawmakers are also beginning to recognize the limitations of the privacy paradigm. In the 2018 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 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."[5] Tellingly, even Facebook's own homepage no longer states that its services are "free."[6]

Despite growing recognition of data-for-services transactions, several important questions have been ignored. What is the precise data price that 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 personalized, granular insight into data-for-services transactions, it is difficult to answer these questions. At present, individual consumers cannot assess precisely how much personal data they pay for the services they receive. Nor can they assess the specific utility they gain in return for the data they supply. The ROD of these deals—*the relationship between the data price consumers pay and the benefits they receive*—is unknown.

To date, there are no legal frameworks that regulate ROD or data platforms that evaluate ROD. Existing legal frameworks and data platforms tend to focus overwhelmingly on privacy. The chief response to the many privacy scandals embroiling Big Tech has been to demand greater protection for personal data.[7] Although privacy laws in the United States

5. *Senate Hearing*, *supra* note 1.

6. Joshua Bote, *Facebook Tweaks Homepage, No Longer Says It Is 'Free and Always Will Be,'* USA TODAY (Aug. 27, 2019), https://www.usatoday.com/story/tech/2019/08/27/facebook-no-longer-says-free-and-always-be-homepage/2133300001 [https://perma.cc/N9WV-FA9B].

7. *See* Angela Chen, *Why San Francisco's Ban on Face Recognition Is Only the Start of a Long Fight*, MIT TECH. REV. (May 16, 2019), https://www.technologyreview.com/s/613536/facial-recognition-ban-san-francisco-surveillance-privacy-private-corporate-interests [https://perma.cc/VL69-8X8V]; Jessica Rich, *Beyond Facebook: It's High Time*

and in the EU have significantly developed in recent years,[8] 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 (CCPA), which is due to come into effect in 2020, do not scrutinize the benefits that consumers reap from data-for-services transactions or investigate how these benefits weigh up against the data price that 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.[9]

Alongside these legal developments, innovations in privacy tech are flourishing.[10] There are scores of technologies that monitor data collection and seek to provide data protection.[11] Some companies give consumers the option of paying a monetary premium to receive privacy-friendly versions of services that would otherwise collect vast amounts of personal data.[12] Privacy is also increasingly being integrated into the design of consumer products and services.[13] With few exceptions, privacy tech aims only to

---

*for Stronger Privacy Laws*, WIRED (Aug. 4, 2018), https://www.wired.com/story/beyond-facebook-its-high-time-for-stronger-privacy-laws [https://perma.cc/C8XH-DKYE]; 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 [https://perma.cc/KE3C-MAHW].

8. *See infra* Section III.B.

9. *See infra* Section III.A. *But see infra* Section III.D.

10. *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 [https://perma.cc/R6U5-YUK7]; *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 [https://perma.cc/LQ9E-2QCA].

11. *See infra* Section IV.A.

12. *See infra* Section IV.B.

13. *See, e.g.*, 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 [https://perma.cc/W3GR-K3RJ]; 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-

protect personal data.[14] It does not attempt to assess what consumers receive in exchange for the personal data they supply.

Although data protection and privacy are vital and understandably fuel much of the "techlash" against data-driven companies, they are not the only issues confronting the data economy. Regulators and developers seeking to tackle the collection, use, and trade of personal data largely overlook the benefits 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 most major tech firms. To properly grapple with data-for-services transactions, we need to pivot away from the prevailing privacy paradigm and build a feasible alternative.[15]

The goal of ROD is to make data-for-services transactions more transparent and guide consumers as they navigate the offerings of different service providers. Equipped with this choice engine, consumers will be able to optimize their decisions on how to spend and invest personal data. The implications of ROD are far-reaching. If consumers begin to select services even partly on the basis of ROD, service providers will have an incentive to pay close attention to ROD. In order to compete with companies providing comparable services, they will need to increase consumers' ROD, either by reducing the data price or providing additional benefits to consumers. In this way, ROD would bolster competition between tech firms, stimulate innovation, and, ultimately, offer consumers more favorable data-for-services deals.

This Article begins by revealing the shortcomings of the privacy paradigm, before proceeding to consider the advantages of ROD and explore how ROD can be implemented in practice. Section II 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. Section III considers the legal frameworks that regulate data-for-services transactions and depicts how these frameworks largely fail to address the underlying exchanges between consumers and service providers. Section IV canvasses a range of data platforms that aim to protect

---

privacy-at-ces-why-other-companies-should-pay-attention/#50675f0a10bf [https://perma.cc/J2AV-9PVA].

14. *See infra* Section IV.C.

15. To be sure, the author does not deny that the right to privacy is of paramount importance. Rather, the emphasis in this Article is that privacy is only one aspect of data-for-services deals and that at present these deals are not scrutinized holistically, but only in terms of their impact on privacy.

personal data or provide benefits in exchange for personal data but do not make data-for-services transactions transparent. Section V outlines the steps required to implement ROD: (A) establishing a conceptual roadmap for evaluating ROD, (B) developing personalized tools to engage consumers, and (C) exploring regulatory and other pathways to adopting ROD. It concludes that ROD has the potential both to empower individual consumers and to incentivize companies to carefully consider the relationship between the personal data they collect and the services they provide.

## 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 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. 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

16. FINJA, http://finja.pk/Index [https://perma.cc/DB7X-MCAN].

17. *Money Talks: Don't Bank with Me Argentina*, ECONOMIST (May 8, 2018), https://soundcloud.com/theeconomist/money-talks-dont-bank-with-me [https://perma.cc/TM9Q-STRP].

18. *See also infra* Section V.A (considering the role of monetary payments alongside data payments). *But see, e.g.*, Elvy, *supra* note 2, at 1387 (discussing freemium models).

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).

they must bear in order to receive nominally "free" services.[20] Data collection is simply the *price* of the services.[21] Conversely, service providers do not receive personal data at no cost.[22] They provide services in return for personal data. Data-for-services transactions are exchanges that deliver value to both parties. Consumers access personalized newsfeeds, real-time traffic updates, and other valuable services. Meanwhile, companies collect personal data that enable them to glean consumer preferences and perform targeted advertising.[23] Personal data can also help companies train artificial intelligence systems,[24] as well as perform A/B tests and other product analytics.[25] Importantly, payment—in the form of data collection—is not a one-off event. Nor is it comprised of several distinct installments, as is

20. *Cf.* CHRIS ANDERSON, FREE: THE FUTURE OF A RADICAL PRICE 18–20 (2009) (describing data-driven advertising revenue as a form of cross-subsidy); 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).

21. *But see infra* note 164 (discussing objections to commodifying personal data).

22. *But see* 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 [https://perma.cc/N9QR-N69K] (describing data-driven service providers as free-riders); LANIER, *supra* note 19, at 49 (arguing that "siren servers" do not pay for the data they collect).

23. *See generally* David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, 23 J. ECON. PERSP. 37 (2009). Some companies provide or sell data to other firms which then perform targeted advertising. *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 [https://perma.cc/C63Q-XY4U]; Ava Kofman, *Google's Sidewalk Labs Plans to Package and Sell Location Data on Millions of Cellphones,* INTERCEPT (Jan. 28, 2019), https://theintercept.com/2019/01/28/google-alphabet-sidewalk-labs-replica-cellphone-data [https://perma.cc/PQ2S-Y7FE].

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

25. *See, e.g.*, Ya Xu et al., *From Infrastructure to Culture: A/B Testing Challenges in Large Scale Social Networks*, 21 PROC. ASS'N FOR COMPUTING MACHINERY'S (ACM) SPECIAL INT. GROUP ON KNOWLEDGE DISCOVERY AND DATA MINING INT'L CONF. ON KNOWLEDGE DISCOVERY & DATA MINING 2227 (2015).

common in retail transactions. Rather, payment is continuous.[26] 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 ten largest companies globally—namely Alphabet, Amazon, Tencent, Alibaba and Facebook and, increasingly, Apple and Microsoft—are, to varying degrees, data-driven.[27] Facebook, for example, does not charge users a monetary fee. Instead, it collects personal data that users generate and uses these to power a targeted advertising platform.[28] From the consumers' perspective, the deal is data-*for*-services. In the case of Facebook, over two billion people accept this deal.[29] Similarly, Google does not charge users a monetary fee for many of the services it offers, including Google Search, Gmail, and Google Drive. Instead, Google collects personal data that users generate and uses these for a variety of purposes.[30] Billions of people, in practice, embrace this deal.[31]

---

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

27. *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 [https://perma.cc/8ALX-S72H].

28. *See How the Big Five Tech Companies Make Their Money, Visualized*, DIGG (Apr. 1, 2019), http://digg.com/2019/tech-companies-main-revenue-stream-data-visualization [https://perma.cc/B4FQ-X76T] (indicating that over 98.5 percent of Facebook's revenue is generated by advertising).

29. *See Number of Monthly Active Facebook Users Worldwide as of 3rd Quarter 2018*, STATISTA, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide [https://perma.cc/E7YE-HLZD].

30. *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 [https://perma.cc/MVJ5-PLH5].

31. *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 [https://perma.cc/TGV7-GGH7]; 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 [https://perma.cc/58EY-8Q5T]. *But see infra* Section III.A (challenging the notion of consumer consent to such transactions).

But Google and Facebook are not alone. Data-for-services transactions are ubiquitous.[32] Many companies now have an intimate portrait of their customers' lives and the lives of the people with whom they interact.[33] Amazon, Netflix, Spotify, and other tech firms use personal data to generate personalized product recommendations.[34] As companies apply data-driven business models to new industries and 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.[35]

Despite privacy concerns, consumers have not, on average, reduced their consumption of services paid for with personal data.[36] Predictions that

32. 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 [https://perma.cc/AZA4-8PZX] (discussing how municipalities supplied Amazon with vast quantities of data in exchange for the opportunity to bid to host the company's new headquarters).

33. *See, e.g.*, Youyou Wu et al., *Computer-Based Personality Judgments Are More Accurate than Those Made by Humans*, 112 PROC. NATL. ACAD. SCI. 1036 (2015); Rory Cellan-Jones, *Facebook Explored Unpicking Personalities to Target Ads*, BBC NEWS (Apr. 24, 2018), http://www.bbc.com/news/technology-43869911 [https://perma.cc/8F4L-X6BH].

34. Joeran Beel & Siddharth Dinesh, *Real-World Recommender Systems for Academia: The Pain and Gain in Building, Operating, and Researching Them*, 5 PROC. WORKSHOP ON BIBLIOMETRIC-ENHANCED INFO. RETRIEVAL 6 (2017).

35. *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 [https://perma.cc/E2D6-L2BP]; 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 [https://perma.cc/F9U5-63D3]; 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 [https://perma.cc/K49Y-MCZF]; *see also* BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD (2018); Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 427 (2018).

36. *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),

privacy breaches would discourage individuals from sharing personal data have proven false. 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.[37] These figures appear to suggest that consumers are content with data-for-services deals.[38]

However, not all consumers are fully aware of the scope of the data collection that companies are carrying out or how they are using personal data. As a result, consumers may not realize the data price that they pay for the services they consume.[39] For example, few consumers understand the depth of insight that companies can glean from location-tracking technology on mobile devices.[40] In addition, consumers find it difficult to fully appreciate the value of the data they generate, particularly because there is

---

https://hbr.org/2017/12/what-would-you-pay-to-keep-your-digital-footprint-100-private [https://perma.cc/7B9U-ZCRV].

37. 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 [https://perma.cc/PJN9-VVX5].

38. *See* Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, PEW RES. CTR. (Jan. 14, 2016), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing [https://perma.cc/494E-QV6F] (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." *Id.*; *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 [https://perma.cc/9YT2-QN8A] (asserting that former Microsoft Director of Search, Stefan Weitz, believes most consumers find personal data trade-offs worthwhile).

39. *See* Strandburg, *supra* note 26, 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).

40. *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 [https://perma.cc/JC98-5J8Y].

no clear monetary price on data.[41] The value of data is usually determined only *after* the data are collected and processed.[42] Furthermore, crude statistics describing consumers' "willingness to share personal data" obscure consumers' subtle preferences vis-à-vis personal data.[43] Various factors affect consumer behavior in this domain, including privacy attitudes, technical experience, and the specific type of data collection and use.[44]

Consumers may also be influenced by companies that market their services as free where the price is non-monetary.[45] For example, Facebook's homepage stated for over a decade that Facebook is "free and always will be," suggesting that use of its platform was completely free of charge.[46] Some commentators appear to accept this questionable view.[47] 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, either irrelevant or inevitable.[48] Consumers tend to

41. *See infra* Section II.A at 90–91 (regarding attempts to assess the value of personal data).

42. *Id.*

43. *See, e.g.*, Yaxing Yao, *Folk Models of Online Behavioral Advertising*, 2017 PROC. ACM CONF. ON COMPUTER SUPPORTED COOPERATIVE WORK & SOC. COMPUTING 1957.

44. *See* Farah Chanchary & Sonia Chiasson, *User Perceptions of Sharing, Advertising, and Tracking*, 2015 PROC. SYMP. ON USABLE PRIVACY AND SECURITY (SOUPS) 53, 61–62; Sonia Chiasson, *Privacy Concerns Amidst OBA and the Need for Alternative Models*, 22 INT. ELECTRICAL & ELECTRONIC ENGINEERS (IEEE) INTERNET COMPUTING 52 (2018); *see also* Pedro Giovanni Leon et al., *What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers*, 2013 PROC. SOUPS 1, 5–8.

45. *See Opinion on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content*, EUROPEAN DATA PROTECTION SUPERVISOR (EDPS) 7 (Mar. 14, 2017), https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf [https://perma.cc/QVQ3-NYGG].

46. *See* Bote, *supra* note 6.

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

48. *See* Rainie & Duggan, *supra* note 38.

believe that attempts to limit companies' data collection and analysis are futile. Consumers supply personal data out of resignation, not on the basis of a cost-benefit analysis.[49]

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.[50] For these people, parting with personal data *is* paying a price. More broadly, these transactions are an exchange. They involve trading one valuable resource for another.[51] In data-for-services deals, irrespective of whether consumers perceive of data as valuable or subjectively experience a disutility or cost, consumers do give away something valuable (personal data) and, in exchange, receive valuable services.[52] This is the definition of barter: the exchange of one valuable resource for another without money changing hands.

---

49. *See* Joseph Turow, *The Tradeoff Fallacy, How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation*, ANNENBERG SCH. FOR COMM., U. PENN. 1, 3–4 (2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf [https://perma.cc/P7MD-K4B5]*; see also* Joseph Turow, *Americans and Marketplace Privacy: Seven Annenberg National Surveys in Perspective*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 151 (Jules Polonetsky et al. eds., 2018) [hereinafter PRIVACY HANDBOOK].

50. Alessandro Acquisti et al., *The Economics of Privacy*, 54 J. ECON. LIT. 442, 447 (2016) (describing the psychological discomfort of revealing personal information, including in exchange for other benefits).

51. *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).

52. *See 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 [https://perma.cc/FV89-5VJR]; *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 [https://perma.cc/6BSS-QSKG]; *cf.* Lauren Henry Scholz, *Big Data Is Not Big Oil: The Role of Analogy in the Law of New Technologies*, 86 TENN. L. REV. (forthcoming 2019); 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 [https://perma.cc/498L-ZFEG]; 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 [https://perma.cc/XF27-9UV9]; Adam Schlosser, *You May Have Heard Data Is*

Admittedly, although data are valuable, it can be difficult to assign them a precise monetary price,[53] particularly because data are not fungible.[54] 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.[55] It derives from organizations' willingness to collect or purchase

*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 [https://perma.cc/CWU9-4EGM].

53. *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); Angela G. Winegar & Cass R. Sunstein, *How Much Is Data Privacy Worth? A Preliminary Investigation*, 42 J. CONSUMER POL'Y (forthcoming 2019); 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 [https://perma.cc/R2YZ-YDGE] (using experimental auctions to discover the monetary value which users place on Facebook's services); Arslan Aziz & Rahul Telang, *What Is a Digital Cookie Worth?* (Apr. 14, 2016), https://ssrn.com/abstract=2757325 [https://perma.cc/EG66-2XQE].

54. *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 [https://perma.cc/2GRB-L92J] (arguing that data are non-fungible and non-rivalrous but recognizing that the value of particular data decreases as they become more widely disseminated). Privacy, by contrast, is a rivalrous good or right. *See 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 [https://perma.cc/UL9V-9YVW] (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).

55. *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* Section II.C.

data, which itself fluctuates over time depending on the utility of the data to the organization, and individuals' willingness to supply data.[56] However, personal data are perhaps different in an important way from many other valuable resources. The value of data typically materializes only after firms that can aggregate and monetize them choose to do so.[57] Privacy interests aside, data are less valuable when in the hands of consumers, who are generally unable to 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.[58] The 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 that 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.[59] 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.

---

56. *See id.* at § 1.2; *see also* Hoofnagle & Whittington, *supra* note 20, at 610.

57. *See, e.g.*, WEIGEND, *supra* note 3, at 344–48; Elvy, *supra* note 2, at 1420. 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).

58. *See* Gianclaudio Malgieri & Bart Custers, *Pricing Privacy—The Right to Know the Value of Your Personal Data*, 34 COMPUT. L. & SECURITY REV. 289, 294 (2018).

59. *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). But others characterize data as labor. *See, e.g.*, POSNER & WEYL, *supra* note 22, at 208–09; Arrieta-Ibarra et al., *supra* note 24, at 38–39, 41; *see also* ANDERSON, *supra* note 20, at 24; TREBOR SCHOLZ, DIGITAL LABOR: THE INTERNET AS PLAYGROUND AND FACTORY 15, 52–53, 151 (2013); ALVIN TOFFLER, THE THIRD WAVE 11 (1980) (coining the term "prosumer"); Chris Marsden, *Prosumer Law and Network Platform Regulation: The Long View Towards Creating Offdata*, GEO. L. TECH. REV. 376, 377 (2018); Tiziana Terranova, *Free Labor: Producing Culture for the Digital Economy*, 18 SOCIAL TEXT 33 (2000).

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, and subsequently used by, multiple actors.[60] The inputs into data-driven services are aggregated from many people and harnessed by different organizations, regardless of whether people actually receive any services from those other organizations.[61] Although these exchanges may not be strictly bilateral, an individual consumer does indeed supply personal data to data-driven companies and, in exchange, receive services.

Yet, this *quid pro quo* conception of the relationship between consumers and service providers 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*.[62]

60. *See Passive Data Collection*, INT'L ASSOC. PRIVACY PROFESSIONALS, https://iapp.org/resources/article/passive-data-collection [https://perma.cc/V9L7-B2P4]; *see also Privacy Policy,* GOOGLE, https://www.google.com/policies/privacy [https://perma.cc/C9RD-YHNE] (distinguishing between data "you create or provide to us" and data "we collect as you use our services"); *Data Policy,* FACEBOOK, https://www.facebook.com/full_data_use_policy [https://perma.cc/BQR2-C47S] (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." *See supra* note 25 (regarding the transfer and sale of personal data).

61. *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 [https://perma.cc/M5SS-46FA].

62. Strandburg, *supra* note 26, at 95 (emphasis added); *see also* Acquisti et al., *supra* note 50, at 447-48 (explaining that the data markets open to

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.[63] Consequently, they do not select among competing services based on data price. Nor do consumers negotiate the data price or the quality of services. Data-for-services deals are usually binary "take it or leave it" offers.[64] To access the service, the consumer must supply whatever data the service provider seeks to collect. To avoid supplying these personal data, the consumer must altogether refrain from using the service. It is all or nothing.[65] For example, to access Netflix, a consumer must consent to Netflix's privacy policy and enable the data collection that it permits.[66]

infomediaries, such as credit-reporting agencies and advertising companies, are closed to consumers).

63. Strandburg, *supra* note 26, 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 107–08 (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 advertisers' willingness to pay data-driven companies would not serve as a proxy for consumers' preferences. *See* POSNER & WEYL, *supra* note 22, at 231–32.

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

65. *See* SCHNEIER, *supra* note 2, at 49–50; WEIGEND, *supra* note 3, at 229–36; 531–33; 3403–10 (arguing that this environment of "binary choice" should be reformed).

66. *Privacy Policy*, NETFLIX, https://help.netflix.com/legal/privacy [https://perma.cc/E9FY-7MMG]; *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 [https://perma.cc/38MQ-3MQR].

There is no possibility of significantly restricting data collection and, in exchange, accessing a stripped-down version of Netflix. Data collection is a flat fee that 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 to which consumers consent 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 service provided. A consumer could receive the very same service 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 while they are not accessing the platform.[67] In other words, heavy users and light users may well pay the same data price.[68] This lack of alignment between data price and service quality is a moral hazard. 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

67. *See, e.g.*, Facebook, Inc., *Responses to the Committee on Commerce, Science, and Transportation*, 197 (June 8, 2018) https://www.judiciary.senate.gov/imo/media/doc/Zuckerberg%20Responses%20to%20Commerce%20Committee%20QFRs.pdf [https://perma.cc/MM6N-EMRW] (confirming that Facebook can track browsing activity after a user logs off the platform).

68. *See* POSNER & WEYL, *supra* note 22, at 231–32. 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.

users.[69] This feature is available only to users who enable the platform to collect location data. If a user wishes to receive location-based friend 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 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 consumers receive. The relationship between the "give" and the "take" is arbitrary. Contrary to Strandburg's position, however, 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*.[70] The inability of consumers to signal their preferences does not undermine the fact that consumers do indeed participate in a value-for-value exchange. In fact, recognizing that consumers pay for services with personal data is a prerequisite for assessing the merits of data-for-services transactions. Only if these transactions were more transparent would consumers be able to signal their preferences to service providers and, ultimately, precipitate a more functional and consumer-friendly market.

69. *See Privacy Policy,* WAZE, https://www.waze.com/en/legal/privacy/ [https://perma.cc/ZU86-B9DM] (indicating that Waze collects additional data from users who opt in to the "find friends" feature); *see also* Amelia Tait, *Why Does Facebook Recommend Friends I've Never Even Met?*, WIRED (May 29, 2019), https://www.wired.co.uk/article/facebook-people-you-may-know-friend-suggestions [https://perma.cc/J3UH-7ML9].

70. *Cf.* Caleb S. Fuller, *Is the Market for Digital Privacy a Failure?*, 180 PUB. CHOICE 353 (2019). Technically, a market failure refers to an inefficient allocation of resources. At present, personal data are not always allocated to the companies that 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, 1342, 1349 (2012).

*B. Consumer Apathy and Behavioral Biases*

According to the theory of bounded rationality, decision-making is constrained by available information and cognitive capacities.[71] 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.[72] 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 than consumers. Unlike consumers, tech firms 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.[73] Tech firms can dictate to consumers the terms of data-for-services transactions.

The fact that many companies do not charge fees for the services they provide exacerbates this situation. The "free" price tag is a powerful marketing tactic that implies that no price whatsoever is extracted from consumers.[74] It entices consumers to blindly accept each and every data-

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

72. *See* Alessandro Acquisti et al., *Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online*, 50 ACM COMPUTING SURVEYS, no. 3, 2017, at 44:1, 44:4.

73. *See* SCHNEIER, *supra* note 2, 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 tech firm 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).

74. *See* David Adam Friedman, *Free Offers: A New Look*, 38 N.M. L. REV. 49, 68–69 (2008); Hoofnagle & Whittington, *supra* note 20, at 635, 648; 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),

for-services deal.[75] Moreover, where the price of services is non-monetary, consumers do not experience the so-called "pain of paying."[76] As a result, they overlook the data price they pay.[77] By altogether refraining from engaging in a cost-benefit analysis, consumers tend to overvalue the services they receive.[78]

Consumer behavior in this context can be explained by specific cognitive and behavioral biases, as identified by Alessandro Acquisti.[79]

---

http://redeye.firstround.com/2007/03/the_first_penny.html [https://perma.cc/NV2T-AX82].

75. *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).

76. *See* Dan Ariely, *The Pain of Paying*, DAN ARIELY (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 Sch. of Mgmt., Working Paper No. 2901808, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2901808 [https://perma.cc/J3P7-ADDG].

77. *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 [https://perma.cc/M8ZL-ECCL] (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* Richard H. Thaler, *Mental Accounting Matters*, 12 J. BEHAV. DECISION MAKING 183, 192 (1999) (regarding payment decoupling); Dan Ariely, *supra* note 76 (suggesting that consumers 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).

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

79. *See* Acquisti et al., *supra* note 72, at 27-31; s*ee also* Solove, *supra* note 73, at 1886–88. *But see* Fuller, *supra* note 70 (questioning some of these findings). *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,

Although studies by economists and psychologists focused specifically on privacy, their findings can be harnessed to shine light on data-for-services transactions more generally. The main findings are as follows:

*Framing effects* — As the benefits (services) 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.[80] 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.[81] 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.[82]

*Loss aversion* — The more consumers feel in control of personal data, the more they value them.[83] 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.[84]

---

contrary to rational choice theory, individuals are not consistent or effective utility-maximizers and instead make systemic errors in decision making).

80. *See generally* Amos Tversky & Daniel Kahneman, *The Framing of Decisions and the Psychology of Choice*, 211 SCIENCE 453 (1981).

81. *See* Strandburg, *supra* note 26, at 150; Hoofnagle & Whittington, *supra* note 20, at 649.

82. *See Creepy or Cool? Staying on the Right Side of the Consumer Privacy Line*, KPMG 20 (2016), https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/creepy-or-cool.pdf [https://perma.cc/6476-6CLV] (discussing, in addition, the status quo, framing, overconfidence and optimism biases).

83. *See* Alessandro Acquisti et al., *What Is Privacy Worth*?, 42 J. LEGAL STUD. 249 (2013); Jens Grossklags & Alessandro Acquisti, *When 25 Cents Is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*, 6 PROC. WORKSHOP ON ECON. INFO. SECURITY 1 (2007)*; see also* Daniel Kahneman et al., *Experimental Tests of the Endowment Effect and the Coase Theorem*, 98 J. POL. ECON. 1325 (1990); Thaler, *supra* note 79, at 43 (coining the term "endowment effect").

84. *See generally* Amos Tversky & Daniel Kahneman, *Judgment under Uncertainty Heuristics and Biases*, 185 SCIENCE 1124, 1127 (1974) (describing the bias of

*Status quo bias* — As with other transactions, consumers are inclined to accept the status quo and default choices with respect to personal data. They do not question or negotiate the deals that tech firms offer them or make counter-offers.[85]

*Herd mentality* — Consumers usually conform to the choices of other consumers, rather than make individual decisions.[86] Different consumers tend to purchase similar services and strike similar data-for-services deals.

These biases help explain consumers' apathy with respect to the data prices 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*.[87] The former concerns the value of a product or service relative to its price; the latter concerns 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 from the early 1980s, the individuals surveyed were, on average, willing to pay far more for a beer in a fancy hotel ($2.65) than in a grocery store ($1.50).[88] The explanation for this difference is that

---

imaginability, according to which people overlook dangers that are difficult to conceive of or unlikely to come to one's attention.).

85. *See, e.g.,* Hana Habib et al., *An Empirical Analysis of Website Data Deletion and Opt-Out Choices*, 2018 PROC. ON ACM COMPUTER HUM. INTERACTION CONF. WORKSHOP ON GENERAL DATA PROTECTION REGULATION: AN OPPORTUNITY FOR THE HCI COMMUNITY?, https://uploads-ssl.webflow.com/5a2007a24a11ce000164d272/5ac8833b99758e1fbb1e21e0_chi-2018-opt.pdf [https://perma.cc/4FPQ-SKWX]; Hana Habib et. al., *An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites*, 15 PROC. SOUPS 387 (2019), (regarding the usability challenges in privacy choice environments). *See generally* 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).

86. *See* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 53 (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).

87. *See* Richard H. Thaler, *Mental Accounting and Consumer Choice*, 4 MARKETING SCI. 199, 205–10 (1985); Thaler, *supra* note 77, at 188–89*; see also* Daniel Kahneman, *New Challenges to the Rationality Assumption*, 150 J. INSTITUTIONAL & THEORETICAL ECON. 18, 21 (1994) (distinguishing between experienced utility and decision utility).

88. *See* Thaler, supra note 87.

while paying the higher price 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.[89] 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 attach great importance to the way they *experience* the outcomes of transactions.[90] This mental accounting involves many psychological factors, including perceptions of fairness.[91]

In light of Thaler's research, 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 and, consequently, cannot compare competing data-for-services deals to seek out the lowest price and the maximum utility. They cannot scrutinize data-

89. 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).

90. *See* Daniel Kahneman & Amos Tversky, *Choices, Values and Frames*, 39 AM. PSYCH. 341, 341–42, 348, 349 (1984). *But cf.* 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).

91. *See generally* GEORGE AKERLOF & ROBERT SHILLER, ANIMAL SPIRITS: HOW HUMAN PSYCHOLOGY DRIVES THE ECONOMY, AND WHY IT MATTERS FOR GLOBAL CAPITALISM ch. 2 (2009); 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); Robert M. Schindler, *The Excitement of Getting a Bargain: Some Hypotheses Concerning the Origins and Effects of Smart-Shopper Feelings*, 16 ADVANCES IN CONSUMER RES. 447 (1989); Lan Xia et al., *The Price Is Unfair! A Conceptual Framework of Price Fairness Perceptions*, 68 J. MARKETING 1 (2004).

for-services transactions in the way they scrutinize other transactions. The result is that 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 therefore exploit consumers' apathy to nudge them into sharing greater quantities of more valuable personal data.[92] By not demanding monetary payment for the services they offer, companies can conceal the data costs consumers pay and magnify the benefits they receive.[93] For now, consumers are mostly resigned to the terms set by data-driven service providers.[94] They do not see these relationships as transactions.[95] 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, actually obstructs efforts to increase *transactional* transparency and, consequently, reinforces consumer apathy.

### *C. The Return on Data Paradigm*

Despite consumers' 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 they

92. *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 making privacy salient, causing consumers to undervalue privacy); 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 [https://perma.cc/HA4T-E2FW].

93. *See* SCHNEIER, *supra* note 2, at 50.

94. *See* Turow, *supra* note 49.

95. *See* Arrieta-Ibarra et al., *supra* note 24.

share,[96] and 83% of users support tougher privacy regulation.[97] Yet, despite the pervasive lack of trust in social media platforms,[98] social media usage continues to rise.[99] Nearly seven-in-ten Americans use social media platforms,[100] which invariably collect vast amounts of personal data. While some consumers take steps to protect their privacy,[101] 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.[102]

According to the so-called "privacy paradox," consumers assert that they want privacy but nonetheless opt to exchange personal data for services.[103] How can this be explained? If data collection is simply the price

96. Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RES. CTR. (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/ [https://perma.cc/5NQL-M5GF].

97. *See Inaugural Tech Media Telecom Pulse Survey,* HARRISX 4, 10 (Apr. 2018), http://harrisx.com/wp-content/uploads/2018/04/Inaugural-TMT-Pulse-Survey_-20-Apr-Final.pdf [https://perma.cc/AXA7-JGUZ].

98. *See id.* at 21; *Trends in Customer Trust: The Future of Personalization, Data, and Privacy in the Fourth Industrial Revolution*, SALESFORCE RESEARCH BRIEF at 4 (Sept. 6, 2018), https://www.salesforce.com/form/conf/trust-research/ [https://perma.cc/T33D-XM25].

99. *But see* Kurt Wagner & Rani Molla, *People Spent 50 Million Hours Less per Day on Facebook Last Quarter*, RECODE (Jan. 31, 2018), https://www.recode.net/2018/1/31/16956826/facebook-mark-zuckerberg-q4-earnings-2018-tax-bill-trump [https://perma.cc/QW7L-DMRT].

100. *See* Rainie, *supra* note 96.

101. *See* Andrew Perrin, *Americans Are Changing Their Relationship with Facebook*, PEW RES. CTR. (Sept. 5, 2018), http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/ [https://perma.cc/PR4J-DHLC] (suggesting that 54 percent of adult Facebook users have adjusted their privacy settings in the past 12 months).

102. *See supra* notes 36–38 and accompanying text.

103. *See* Idris Adjerid et al., *Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making*, 42 MGMT. INFO. SYS. Q. 465 (2018); Idris Adjerid et al., *The Paradox of Wanting Privacy but Behaving as if It Didn't Matter*, LSE BUS. REV. (Apr. 19, 2018), https://blogs.lse.ac.uk/businessreview/2018/04/19/the-paradox-of-wanting-privacy-but-behaving-as-if-it-didnt-matter.

of certain services, why are consumers 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 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 typically overshadowed by privacy concerns.[104]

This fixation on privacy has been dubbed a "pessimism problem."[105] Public and scholarly attention is directed toward the risks of data collection, not its benefits or the opportunities it creates. This is reinforced in many contexts. Non-governmental organizations working on technology policy overwhelmingly focus on privacy.[106] Public surveys and indices relating to the data economy are primarily concerned with privacy.[107] Journalists conduct privacy investigations,[108] economists seek to optimize privacy decision-making,[109] and legal scholars advocate data privacy law.[110]

---

[https://perma.cc/G4D4-AW8Y]; Patricia A. Norberg, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFF. 100 (2007). *But see* Fuller, *supra* note 70.

104. *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); Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 BERKELEY TECH. L.J. 997, 1013 (2016) (regarding the privacy impacts of the IoT). *But see* Stucke, *supra* note 64, at 287 (describing data collection as a price.)

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

106. *See, e.g., Privacy,* ELECTRONIC FRONTIER FOUND, https://www.eff.org/issues/privacy [https://perma.cc/ZYN6-8XE9].

107. *See, e.g., 2018 Corporate Accountability Index*, RANKING DIGITAL RIGHTS, https://rankingdigitalrights.org/index2018/categories/privacy/ [https://perma.cc/H4SL-9UNQ]; *Computers and the Internet: Historical Trends*, GALLUP (Sept. 2018), https://news.gallup.com/poll/1591/computers-internet.aspx [https://perma.cc/D4CT-R5F5].

108. *See, e.g., New York Times Privacy Project*, N. Y. TIMES, https://www.nytimes.com/interactive/2019/opinion/internet-privacy-project.html [https://perma.cc/8NSW-3UBB].

109. *See, e.g.,* THALER & SUNSTEIN, *supra* note 86.

110. *See, e.g.,* Symposium, *The Privacy Paradox: Privacy and Its Conflicting Values*, 64 STAN. L. REV. (2012); *Symposium on Privacy and Technology*, 126 HARV. L.

Company data policies are described as "privacy policies,"[111] data law as "privacy law."[112] From industry to academia, the privacy paradigm dominates. Even those who acknowledge that consumers do not give away personal data for free pay little attention to the utility consumers gain in return for the personal data they supply.[113]

What explains the dominance of the privacy paradigm? One possibility is that legislators and other policymakers are themselves consumers and, therefore, are not immune to the factors that discourage consumers from conceiving of their relationships with data-driven companies as transactional. As outlined above, these factors include: (1) *Mental models.* Due to a number of cognitive and behavioral biases, consumers do not experience data collection and data use as a price or scrutinize data-for-services transactions as they scrutinize other transactions. (2) *The "free" misnomer.* Despite the privacy "techlash," the seductive misnomer that many of the services of tech firms are free is surprisingly resilient. (3) *Opaqueness.* Data-for-services transactions remain opaque, due partly to the absence of tools for evaluating the merits of a given data-for-services deal. Upon failing to conceive of data-for-services deals as transactions, the privacy paradigm—by virtue of its rhetorical appeal and legal precedent—is the natural fallback.

These factors have further, far-reaching implications. They entrench an information asymmetry and cognitive asymmetry between consumers and the tech firms with which they interact. Data-driven companies can dictate to consumers the terms of data-for-services deals. They often present them as binary "take it or leave it" offers in which consumers must consent to broad data collection and use of personal data in order to access services, there being no intermediate option of supplying less data in exchange for inferior services. Tech firms can also exploit consumers' apathy to nudge them into sharing greater quantities of more valuable personal data. They

REV. (2013); *Law, Privacy & Technology Commentary Series*, 130 HARV. L. REV. F. 1180 (2016); *The Problem of Theorizing Privacy*, 20 THEORETICAL INQUIRIES L. i (2019); *see also* INT'L DATA PRIVACY LAW—an OUP peer-reviewed journal dedicated to data protection.

111. *See infra* Section III.A.

112. *See, e.g.,* DANIEL J. SOLOVE & PAUL H. SCHWARTZ, INFORMATION PRIVACY LAW (6th ed. 2018) (the title of which refers to "privacy law").

113. *See, e.g.,* Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 4, 7 (2018) (recognizing data-for-services transactions but advocating extensions of Balkin's privacy proposals); *see* Balkin, *infra* note 149.

have no incentive to consider the relationship between the personal data they collect from consumers and the quality of the services they provide. To address these concerns, we need a new policy and legal paradigm.

Andreas Weigend, former Amazon Chief Scientist, proposes engaging the concept of *return on data (ROD)*, which adapts the notion of return on investment (ROI) to the data economy.[114] 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.[115] 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 (collection, storage, use, etc.), and it equals the benefit of those data divided by their cost.[116]

But, for consumers in data-for-services transactions, ROD has a different meaning.[117] Where consumers pay for services with personal data, the benefit they gain is the utility of the services they receive, and 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 /*

114. *See* WEIGEND, *supra* note 3, at 3131–35, 3193–98; *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, 1318 (2012) (referring to a data-for-value equation).

115. *See Return on Investment (ROI)*, INVESTOPEDIA, https://www.investopedia.com/terms/r/returnoninvestment.asp [https://perma.cc/28YM-HYUQ].

116. *See* Dorian Selz, *Return on Data*, SQUIRRO (Jan. 20, 2016), https://squirro.com/2016/01/20/return-on-data/ [https://perma.cc/CB5K-3NCM]. Most references to ROD address only the service provider's perspective, i.e., business strategies for best utilizing 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 [https://perma.cc/7SBC-7EMN]. In this context, the benefits derived 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.

117. *See infra* Section V.A.

*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 is difficult to calculate, ROD sends a powerful message. Just as businesses can quantify the profitability of data investments they make, individual consumers should be able to evaluate the merits of the data-for-services transactions they enter.[118]

The introduction of ROD, whether as part of a legal framework or as a tool voluntarily adopted by tech firms, would enable consumers to better navigate the tradeoffs inherent in data-for-services transactions. ROD evaluations would nudge consumers toward conceiving of their relationships with data-driven companies as transactional. ROD would also make salient the data price individual consumers pay and thereby assist them in overcoming many of the cognitive and behavioral biases that rigidly ingrain the misnomer that services paid for with data are free. Making ROD transparent would reduce the information asymmetry between consumers and tech firms. Consumers would be able to determine whether a given data-for-services deal is in their best interests. In time, consumers might even seek to renegotiate these deals and demand greater ROD.

Before leaping ahead, it is worth noting that ROD is likely to have broad appeal. A Deloitte survey found that respondents across several countries were more willing to share personal data when they received something valuable in exchange.[119] 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.[120] ROD is also likely to resonate with commentators who have called on tech firms to offer consumers more equitable data-for-services deals.[121]

The key takeaway is that the privacy paradigm is, on its own, inadequate.[122] Although privacy concerns warrant continued technological innovation and regulation, there are other issues at stake. With few exceptions, the relationship between data price and services in any given transaction remains unknown. Perhaps consumers tend to get good deals. Perhaps they are being shortchanged. Data-for-services transactions,

118. *See* WEIGEND, *supra* note 3, at 3131–39; 3142–46.

119. *See* Pingitore et al., *supra* note 37.

120. *Id.*

121. *See, e.g.,* Nahai & Chamorro-Premuzic, *supra* note 36.

122. *See id.* (acknowledging that the right to privacy remains of paramount importance).

although pervasive, remain under-scrutinized. We therefore need to pivot away from the privacy-only paradigm and develop tools to assess ROD. Only if consumers can actually evaluate each data-for-services deal will they be able to engage in a cost-benefit analysis and make informed decisions on which deals to accept and which to reject.

## III. LEGAL FRAMEWORKS

Most legal frameworks that govern data-for-services transactions are preoccupied with privacy. Privacy policies focus on the personal data consumers supply and how these data are used. They overlook the relationship between these data and the benefits consumers receive. Privacy law in both the United States and the EU aims to protect personal data, not to evaluate the data price consumers pay relative to the utility they receive. With the possible exception of an EU Directive that recognizes 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.

### *A. Terms of Service and Privacy Policies*

There are generally two documents that govern the relationship between a consumer and a data-driven service provider: the terms of service and privacy policy. Typically, the terms of service contain a variety of conditions, while privacy policies describe the types of personal data collected and how these data are used.[123] 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*.[124] By separating the data price consumers pay from the utility they

123. *See, e.g., Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html/ref=asus_gen_not?ie=UTF8&nodeId=468496&ld=ASUSGeneralDirect [https://perma.cc/QTG4-7FV3]; FACEBOOK, *supra* note 60; GOOGLE, *supra* note 60; *WhatsApp Legal Info,* WHATSAPP, https://www.whatsapp.com/legal/ [https://perma.cc/9A59-ZY2C].

124. *See* SCHNEIER, *supra* note 2, at 1 (recognizing that there is no single contract governing the bargain).

receive, these documents decouple data price from utility and, in doing so, implicitly deny that a mutual exchange takes place.

In addition, it is well known that consumers have almost no influence over the terms of service and privacy policies that 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.[125] These documents can be long, legalistic, and difficult to understand.[126] As a result, consumers are not generally familiar with the terms on which they transact with service providers.[127]

Nevertheless, consumers increasingly depend on the technologies that data-driven companies provide. Although there exist alternatives to Google Chrome and Google Search that do not involve data collection, such as the Brave browser and DuckDuckGo search engine, these are not necessarily adequate substitutes.[128] We cannot expect consumers to refrain from using technologies provided by Big Tech. "Exiting" Google or Facebook is not

125. *See, e.g.,* Yannis Bakos et al., *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1 (2014); 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 [https://perma.cc/Q6UD-VSYY] (revealing that over 90% of consumers accept terms of service without reading them); Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html [https://perma.cc/655D-43RY].

126. *See* Shmuel I. Becher & Uri Benoliel, *The Duty to Read the Unreadable*, 60 B.C. L. REV. (forthcoming 2019); Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39 (2015); *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 [https://perma.cc/ACH8-F2CN].

127. *Cf.* WEIGEND, *supra* note 3, at 921–22 (suggesting that most Gmail users *consciously* exchange data for free email).

128. The same arguably applies to substituting Apple Maps for Google Maps. *See Apple Maps vs. Google Maps: Which Is Better?*, THE MANIFEST (Sept. 12, 2018), https://medium.com/@the_manifest/apple-maps-vs-google-maps-which-is-better-9ceaf28f9bf0 [https://perma.cc/3L89-CZ3P].

generally straightforward (or even possible).[129] Public-interest technologist Bruce Schneier explains 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 . . . .[130]

Tech firms control the terms of data-for-services transactions.[131] 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 questioned the authenticity of consumers' consent to these transactions.[132] Consent, they suggest, is *presumed* or *engineered*,[133] or perhaps given under duress. Firms equipped with data-driven analytics can nudge consumers into accepting the deals they offer. They can exploit

129. *See* Kashmir Hill, *Life Without the Tech Giants*, GIZMODO (Jan. 22, 2019), https://gizmodo.com/life-without-the-tech-giants-1830258056 [https://perma.cc/38GK-CS7P]; 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/ [https://perma.cc/XZE6-FDKS].

130. SCHNEIER, *supra* note 2, at 57-59, 60–61.

131. *See* Stucke, *supra* note 64, at 289 (explaining that consumers have no viable alternative to consenting); *see also* POSNER & WEYL, *supra* note 22, at 231 (discussing "technofeudalism"); *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 [https://perma.cc/5RBY-L5BK] (discussing "data slavery").

132. *See* Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 67 (2012). Notably, the GDPR relies heavily on consent. *See, e.g.,* GDPR, *infra* note 136, 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 [https://perma.cc/8XMY-YPHB] (discussing Helen Nissenbaum's objections to the reliance on consent).

133. *See* Nancy Kim, *Contract's Adaptation and the Online Bargain*, 79 U. CIN. L. REV. 1327, 1330 (2011).

individuals' personal traits and biases to manipulate their decision-making.[134]

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.[135] Nevertheless, terms of service and privacy policies currently fail to treat data collection as the price 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 and expressly communicate that an exchange takes place. If consumers internalize the notion of data-for-services transactions, they may reconsider blindly consenting to every deal offered to them. Consumers may scrutinize and even seek to renegotiate the deals they enter. A refusal to pay exorbitant data prices would, in time, signal to service providers consumers' demand for more favorable deals.

### *B. Privacy Law*

The preoccupation with privacy and failure to engage with ROD are buttressed by the current data protection regimes. The EU's General Data Protection Regulation (GDPR) treats privacy as a fundamental right and affords individuals various data protections. These include data access rights, data portability, and privacy breach notifications.[136] In the United States, there is no equivalent regime that comprehensively regulates the collection and use of data by private entities or treats data privacy vis-à-vis

134. *See, e.g.*, Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1003 (2014).

135. Although, due to the doctrine of privity, privacy policies and terms of service are unlikely to bind third parties— i.e., parties other than the consumer and service provider.

136. *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.

non-governmental actors as a fundamental right.[137] Instead, there is a patchwork of judge-made law,[138] sector-specific legislation,[139] contractual arrangements, and industry practices.[140] However, California's Consumer Privacy Act (CCPA) signals a shift toward the EU's approach and, beginning in 2020, will grant Californians the right to prohibit the sharing and sale of personal data to third parties.[141]

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.[142] Like privacy policies, privacy law currently addresses only one aspect of data-for-services transactions—the collection and use of personal data.[143] 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.[144] The FTC's Fair Information Practices (FIPs) are an industry data protection regime.[145] Legal textbooks relating to personal

137. But there are constitutional protections against data collection carried out by government actors. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206 (2018); DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE (2017). However, it is private actors that carry out the majority of data collection. *See* SCHNEIER, *supra* note 2, at 47.

138. *See* RESTATEMENT (SECOND) OF TORTS §§ 652A-E.

139. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d-6 (2012).

140. *See, e.g.*, SOLOVE & SCHWARTZ, *supra* note 112, at 785.

141. *See* CAL. CIV. CODE § 1798 (as amended by Consumer Privacy Act (A.B. 375)).

142. *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, 878–81 (2014).

143. This of course is a valuable and necessary function, given the importance of the right to privacy. However, it alone is not sufficient.

144. *See* GDPR, *supra* note 136, at rec. 6.

145. *See* CHRIS HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 216-35 (2016); SOLOVE & SCHWARTZ, *supra* note 112, at 975.

data are privacy-oriented.[146] The debate on establishing property rights in personal data centers around privacy concerns.[147] Recent proposals also revolve around data protection: introducing a Bill of Data Rights to protect individuals' privacy,[148] treating data collectors as information fiduciaries obligated to safeguard personal data,[149] and mandating the integration of data protection into product design.[150] None contemplates 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 that underpins data-for-services transactions. The GDPR, for example, does not clarify the role of data collection as payment.[151] Although the GDPR bolsters transparency around the processing of personal data, it does not require companies to disclose whether personal data constitute the price payable

146. SOLOVE & SCHWARTZ, *supra* note 112.; *see also* MARC ROTENBERG & ANITA L. ALLEN, PRIVACY LAW AND SOCIETY (2016).

147. *See, e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2093, 2095–2116 (2004); *see also* Victor, *supra* note 19, at 518–19 (explaining that several legal scholars do not propose free markets in personal data, but highly regulated property regimes specifically designed to protect personal data).

148. *See, e.g.*, Russell Brandom, *DuckDuckGo Wrote a Bill to Stop Advertisers from Tracking You Online*, VERGE (May 1, 2019), https://www.theverge.com/2019/5/1/18525140/do-not-track-duckduckgo-ad-tracking [https://perma.cc/5MA7-3C9D]; 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/ [https://perma.cc/P3XL-9RS5]; 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 [https://perma.cc/R5AX-H4RW]; *see also* Data Care Act of 2018, S. 3744, 115th Cong. (2018) (introduced by Senator Brian Schatz); Consumer Data Protection Act, S.I.L. 18B29, 115th Cong. (2018) (introduced by Senator Ron Wyden).

149. *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016); Lina M. Khan & David Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. (forthcoming 2019).

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

151. *See* GDPR, *supra* note 136, at recs. 39, 60, 71; arts. 5(1)(a), 12.

for services.[152] Privacy law thus fails to holistically address the bargains consumers routinely make. By overlooking what consumers receive in return for the data they supply, privacy law maintains a very narrow focus.

### *C. Data as "Counter-Performance"*

The GDPR is not the only pioneering EU legal development in the field of personal data. The EU Directive for consumer protection in contracts for the supply of digital content signals a potential shift toward the ROD paradigm.[153] Rather than merely enhance data protection, as the GDPR does, the Directive confronts the reality of consumers paying for services with personal data. The original proposed version of the Directive, however, did so more explicitly than the version ultimately adopted by the European Parliament, and sought to expressly regulate data-for-services transactions. Article 3(1) of the Proposed Directive stated 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.*[154]

The Proposed Directive aimed to treat personal data as the "counter-performance" provided in exchange for services. In common law terminology, personal data would constitute contractual consideration. By way of explanation, Recital 13 of the Proposed Directive provided 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*

152. *Id.* at art. 13 (listing the information which data controllers must provide to data subjects).

153. *See 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) 634 final (Dec. 9, 2015) [hereinafter *Proposed Directive*], https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015PC0634&from=en [https://perma.cc/WU7Q-6VK7] (indicating the current status and legislative progress of the Directive).

154. *Id*. at 24-25 (emphasis added); *see also id.* at 26, 31 (concerning arts. 6(2), 15(2)(b), and 16(4)(a) respectively).

> *exchange for a price but against counter-performance other than money i.e. by giving access to personal data or other data*.[155]

The language of the Proposed Directive speaks for itself.[156] It recognizes that consumers pay for certain services with personal data. The Proposed Directive enjoyed broad support from EU institutions,[157] legal scholars,[158] consumer groups,[159] and some industry groups.[160] Supporters of the Proposed Directive applauded it for treating data as "counter-performance" and, thereby, extending consumer protections to data-for-services

155. *Id.* at 16 (emphasis added).

156. By comparison, the endorsement of the notion of data constituting counter-performance that features in the version of the Directive adopted by the European Parliament is far more subtle. *See* Directive 2019/770, of the European Parliament and of the Council of 20 May 2019 on Certain Aspects Concerning Contracts for the Supply of Digital Content and Digital Services, 2019 O.J. (L 136) 1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0770&from=en [https://perma.cc/UE6H-3SKN]. Article 2(7) states that "'price' means money or a digital representation of value that is due in exchange for the supply of digital content or a digital service." *Id.* at 17. Assuming data amount to a "digital representation of value," the Directive implies that data can comprise the price that consumers pay.

157. *See, e.g., 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 [https://perma.cc/VX68-J6HJ].

158. *See, e.g.,* Gerald Spindler, *Contracts for the Supply of Digital Content—Scope of Application and Basic Approach*, 12 EUR. REV. CONT. L. 183, 191–92 (2016); Hugh Beale, *Scope of Application and General Approach of the New Rules for Contracts in the Digital Environment* (Policy Department C: Citizens' Rights and Constitutional Affairs) at 12–13 (2016), http://www.europarl.europa.eu/cmsdata/98770/Beale.pdf [https://perma.cc/57Q6-W8PB].

159. *See, e.g., Commission Staff Working Document: Impact Assessment*, at 62, 122–23, COM (2015) 274 final (Dec. 17, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2015%3A274%3AREV1 [https://perma.cc/57Q6-W8PB].

160. *See, e.g., id.* at 63.

transactions.[161] The Directive, even in its final form, is groundbreaking. Unlike other legal frameworks, it acknowledges the existence of, and directly tackles, data-for-services transactions.

However, the Directive, following its original proposal, has also been criticized. Several industry groups suggested that, if enacted, it would overregulate and hamper the data economy.[162] Others suggested that it would inhibit contractual freedom and undermine the kind of transactions that foster technological innovation.[163] The European Data Protection Supervisor, an independent EU institution, while supporting the Directive's expansion of consumer protections, contended that personal data must not be treated as a price or payment for services. Commodifying personal data, it reasoned, would infringe fundamental rights, such as privacy, and reduce them to commercial interests.[164] 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 related to Article 3(4) of the Proposed Directive, which provided that the Proposed Directive would not apply to personal data that are "*strictly necessary* for the performance of the contract."[165] The problem here is that it is not always clear which data are "necessary" for a

161. *See* Helberger et al., *supra* note 75, at 1445.

162. *See, e.g.,* BUSINESS EUROPE, *Position Paper on the Harmonisation of Contract Rules for Digital Content and Tangible Goods* 5 (Sept. 3, 2015), https://www.businesseurope.eu/publications/harmonisation-contract-rules-digital-content-and-tangible-goods [https://perma.cc/XKW4-ZZLS].

163. *See* AMERICAN CHAMBER OF COMMERCE TO THE EUROPEAN UNION, *Joint Industry Declaration on the Digital Content Directive* 2 (May 24, 2016), http://www.amchameu.eu/media-centre/press-releases/joint-industry-declaration-digital-content-directive [https://perma.cc/G7DC-JXN5].

164. *See* EDPS, *supra* note 45, 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). *Compare* Sandel with 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 "repugnant" transactions).

165. *Proposed Directive,* supra note 153, at 14 (emphasis added).

particular service to function.[166] For instance, while a mobile payments app might not require location data, those data may significantly enhance the app's security. More fundamentally, even if it were clear which data are necessary for a particular service to function, the data supplied (both those that are necessary and those that are not) still constitute the price paid for the services. The mere fact that location data are deemed necessary for the service should not exempt them from the Directive.[167]

Furthermore, the Proposed Directive has been criticized for distinguishing between consumers who pay for services with money and consumers who pay with personal data,[168] as has the CCPA.[169] Notwithstanding studies that suggest that the form of payment—monetary or non-monetary—does not impact the level of legal protection that consumers expect,[170] the Proposed Directive afforded consumers who pay with money greater legal protection.[171] By discriminating against consumers who pay for services with personal data, the Proposed Directive

166. Madalena Narciso, *'Gratuitous' Digital Content Contracts*, J. EUR. CONSUMER & MARKET L., 198 , 205 (2017). See *infra* note 287 (regarding data efficiency).

167. *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 9 (2016), http://www.europarl.europa.eu/cmsdata/98771/Mak.pdf [https://perma.cc/9RRH-N733].

168. *Id.* at 17–18.

169. *See* CAL. CIV. CODE § 1798.125(a)(2) (as amended by Consumer Privacy Act (A.B. 375)) ("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 id.* § 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.").

170. *See* Madalena Narciso, *Consumer Expectations in Digital Content Contracts – An Empirical Study* 19–21 (Tilburg Priv. Law, Working Paper No. 01/2017, 2017), https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2954491 [https://perma.cc/HHT9-S3J2].

171. *See Proposed Directive*, supra note 153, at 29-30 (concerning art. 13(2)); *id*. at 21 (concerning rec. 42 and its discussion of termination rights).

would have undercut its goal of treating all consumers equally, irrespective of how they pay.[172]

The Directive has spawned vigorous debate and is therefore a welcome development. By regulating data-for-services deals, the Directive recognizes the reality of these transactions. While other legal frameworks, such as privacy policies and privacy law, are preoccupied with privacy, the Directive engages with the underlying exchange between consumers and companies. However, despite 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 institute ROD assessments or enable consumers to better navigate the tradeoffs inherent in these transactions.

## 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 that 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 in-kind benefits. By offering consumers assets of concrete value in exchange for personal data, they implicitly embrace the notion of ROD. But they too are imperfect. 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 that consumers *already* enter with Facebook, Google, etc. The ROD of *these* transactions remains unknown.

### *A. Privacy Tech*

Privacy monitors and personal information management systems (PIMs) are perhaps the most common privacy tech tools.[173] Privacy

172. *See* Spindler, *supra* note 158, at 198–99.

173. *See VRM Development Work: Personal Information Management Systems*, PROJECT VRM, https://cyber.harvard.edu/projectvrm/VRM_Development_Work#Personal_

monitors, sometimes called privacy dashboards, aim to display to users how personal data relating to them are collected and used. For example, Lumen Privacy Monitor, an Android app, monitors the type, volume, and (apparent) purpose of data collection carried out by mobile apps.[174] Tools like this helpfully reveal to consumers how the personal data they generate are collected and used.

Although privacy monitors have not proved especially popular, their potential use cases are likely to expand, particularly as the IoT grows. However, from the perspective of ROD, privacy monitors are lacking. They only gauge data collection. They do not assess what consumers receive in exchange for the data they supply. As a result, privacy monitors cannot evaluate the merits of data-for-services transactions, let alone indicate where greater ROD may be available.

PIMs provide greater functionality than privacy monitors as they enable consumers to exercise control over the personal data they generate.[175] For example, MyPermissions Privacy Cleaner enables consumers to control the data collection permissions of mobile apps.[176] Other PIMs function as gatekeepers between consumers and third parties seeking access to personal data.[177] Like privacy monitors, PIMs seek to empower consumers and enable them to take responsibility for data protection.[178]

---

Information_Management_Systems_.28PIMS.29 [https://perma.cc/R3QG-GDX6].

174. *See Lumen Privacy Monitor*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=edu.berkeley.icsi.haystack [https://perma.cc/UEA5-BJFL].

175. *See, e.g.,* Christoph Busch, *Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law*, 86 U. CHI. L. REV. 309, 322-324 (2019); *The Personalized Privacy Assistant Project*, PRIVACYASSISTANT.ORG, https://www.privacyassistant.org/ [https://perma.cc/QN44-N4JJ].

176. *See* MYPERMISSIONS PRIVACY CLEANER, https://mypermissions.com/ [https://perma.cc/MTE4-YKWS]. Other privacy monitors, such as Ghostery and Privacy Badger, also function as PIMs by blocking trackers automatically or at a user's request.

177. *See, e.g.,* DIGI.ME, https://digi.me/ [https://perma.cc/4ANE-75ZP].

178. *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* Richards & Hartzog, *supra* note 105, at 444 (suggesting that privacy self-management is highly problematic); Solove, *supra* note 73.

But therein lies the problem. The aim of these privacy tools is to *protect* personal data. Whether by informing consumers of data security risks or actively managing personal data, privacy tech concentrates on improving privacy protection. It does not engage with the benefits consumers receive in exchange for sharing personal data. Privacy tech, notwithstanding the benefits it delivers, addresses only the data price consumers pay. It overlooks the underlying give-and-take in data-for-services transactions and does not attempt to make ROD transparent.

*B. Paying for Privacy*

Today, there is an increasing number of opportunities for consumers to pay for privacy.[179] In exchange for paying a monetary premium, consumers can in some contexts limit the scope of data collection when they access certain services. For example, consumers can pay a fee to use virtual private networks (VPNs), which help protect user privacy.[180] At the same time, several service providers have begun to offer consumers monetary discounts in exchange for consumers sharing more personal data. Some automotive insurers, for example, offer discount rates to consumers who permit the collection of driving data.[181]

---

179. *See generally* Elvy, *supra* note 2; Nahai & Chamorro-Premuzic, *supra* note 36.

180. *See* Elvy, *supra* note 2, at 1388–91 (discussing the "privacy-as-a-luxury" model); *see also* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION 168–71 (2016). Several commentators advocate expanding the pay-for-privacy model by demanding the option of paid subscriptions to social media platforms. *See* TIEN TZUO, SUBSCRIBED: WHY THE SUBSCRIPTION MODEL WILL BE YOUR COMPANY'S FUTURE—AND WHAT TO DO ABOUT IT (2018); Calo, *supra* note 134, at 1047–48; 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); *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 [https://perma.cc/HR4E-9T27]. *But see Senate Hearing*, *supra* note 1 (discussing Zuckerberg's statement that most consumers prefer not to, or would be unable to, pay money for Facebook's services); 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 [https://perma.cc/JTN8-UGX3].

181. *See* O'NEIL, *supra* note 180, at 168; Mark Chalon Smith, *State Farm's In-Drive Discount: What's the Catch?*, CARINSURANCE.COM (June 12, 2015),

These opportunities seem empowering. Consumers, at least in theory, are given a choice.[182] Those who prize privacy can pay a premium to protect personal data relating to them, while those who are less concerned about 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.[183] 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 compelled to supply more personal data.[184]

Despite these shortcomings, the opportunity to pay for privacy has some advantages. 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 and discounts offered by companies might not accurately reflect the value of personal data,[185] 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 could be seen as somewhat antiquated. It may already 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 dissemination would be fruitless.[186] But, in reality, *new* personal data are continuously being generated. Companies constantly collect, process, and exploit new data.

---

https://www.carinsurance.com/Articles/state-farm-in-drive-discount.aspx [https://perma.cc/K7NE-KNQ5].

182. *But see supra* Section III.A.

183. *See* Elvy, *supra* note 2, at 1388; *see also supra* Section II.C.

184. *See* O'NEIL, *supra* note 180, at 171; Joseph W. Jerome, *Buying and Selling Privacy: Big Data's Different Burdens and Benefits*, 66 STAN. L. REV. ONLINE 47, 48 (2013).

185. *See* sources cited *supra* note 53 (regarding the difficulty in determining the value of data).

186. *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION ch. 2 (2015); Strandburg, *supra* note 26, at 145, 150. However, the "right to be forgotten" may facilitate the deletion of certain information. *See, e.g.*, GDPR, *supra* note 136, at art. 17. *See generally* Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2012).

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 tackle data-for-services transactions in which no money changes hands. The ability to pay a monetary premium for privacy in highly specific contexts does not enable or inspire consumers to assess what they receive in return for the data they supply in routine data-for-services deals. Opportunities to pay for privacy do not make these transactions any more transparent, let alone equitable.

### *C. Selling and Investing Personal Data*

Several platforms now enable consumers to sell or invest personal data. Datacoup, perhaps the most well-known personal data exchange (PDE), allows consumers to sell personal data for cash.[187] Users decide which data points to make available to the platform, which then determines the amount of cash they receive. PDEs clearly give consumers the opportunity to benefit from personal data in new ways. The data-for-services transactions that they facilitate are relatively transparent. PDEs are upfront about trading personal data for various benefits. They do not conceal the give-and-take but embrace it. PDE users consciously choose which personal data to share and know what to expect in return.[188] ROD, in these cases, is comparatively explicit and clear-cut.

Yet, PDEs have not proved especially popular.[189] This might be because they tend to pay consumers only relatively small sums of money,[190] which is partly attributable to the fact that payments are made prior to the data being aggregated and monetized. Datacoup's website, for example,

187. *See How It Works,* DATACOUP, https://datacoup.com/docs#how-it-works [https://perma.cc/N287-AZPZ].

188. *Cf. supra* Section II.A (regarding the misalignment between data prices and services).

189. *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/ [https://perma.cc/M2BR-6B8V].

190. *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/ [https://perma.cc/J2K6-HP8V].

showcases a user earning just $1.10 a week from the platform.[191] 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 consumers have *already* entered. 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 affect *existing* relationships with data-driven service providers.

One possible solution is to introduce elements of PDEs into existing data-for-services transactions. Consumers could receive a small monetary payment ("micropayment") for every unit of data they share with service providers.[192] However, micropayments have been widely criticized on several grounds. First, it may be unclear who should be entitled to a given micropayment, particularly as data relating to one person are often collected from others.[193] 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.[194] Third, micropayments might impose additional transaction costs on consumers.[195] Fourth, developing systems and infrastructure to facilitate micropayments

191. *See* DATACOUP, *supra* note 187.

192. *See* LANIER, *supra* note 19, at 6, 317; POSNER & WEYL, *supra* note 22, at 247; Jakob Nielson, *The Case for Micropayments*, NIELSON NORMAN GROUP (Jan. 25, 1998), https://www.nngroup.com/articles/the-case-for-micropayments/ [https://perma.cc/J6NS-ZGKD].

193. *See* WEIGEND, *supra* note 3, at 508–23 (discussing who will receive the payment where one person uploads a photo which features other people); *see also* sources cited *supra* note 59 (regarding passive data collection). Notably, the need to disaggregate personal data on an individual basis is also a challenge for ROD, which purports to separately evaluate the utility-to-data ratio for each individual user.

194. *See* WEIGEND, *supra* note 3, at 508–23; *see also supra* note 53 (regarding the difficulty in determining the value of data). This issue is less relevant to ROD, which does not purport to price data. However, subsequent changes in the value of the data *from the consumer's perspective* may alter the ROD score over time. *See infra* Section V.A.2.

195. *See* ANDERSON, *supra* note 20, at 45, 48 (discussing Nick Szabo, *Micropayments and Mental Transaction Costs*, SATOSHI NAKAMOTO INST. (undated), http://nakamotoinstitute.org/static/docs/micropayments-and-mental-transaction-costs.pdf [https://perma.cc/6463-BTNN]); *see also infra* note 210 (regarding the imposition of transaction costs under ROD).

would be costly.[196] Fifth, consumers might not actually be interested in receiving minute monetary payments in exchange for sharing highly sensitive personal data.[197]

Apart from these notable 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 deserve *additional* payment. Yet, given that most existing data-for-services transactions are opaque, we cannot at present actually assess what compensation consumers receive, let alone judge whether it is equitable. Due to the lack of transparency, there is currently no reliable way to know whether or not consumers are getting fair deals.

Some PDEs may signal a change of direction and tentative shift toward ROD. Datavest, a data investment platform, appears to ask 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."[198] Datavest prompts consumers to reflect on how much they *earn* from the data they supply. But again, there is no indication that the platform will in fact make existing data-for-services transactions more transparent.

## V. IMPLEMENTING RETURN ON DATA

So far, we have seen how the legal frameworks that govern data-for-services transactions embrace the privacy paradigm. We have also seen how privacy tech is geared toward data protection. Although these frameworks and platforms bolster consumers' control over personal data, they overlook the relationship between the data consumers supply and the services they receive. Consumers cannot presently evaluate the merits of the data-for-services transactions they enter or make informed decisions on how to spend and invest personal data.

196. *See* WEIGEND, *supra* note 3, at 523–27.

197. *See id.* at 508–31. By contrast, under ROD, it is hoped that consumers will eventually receive superior services and/or supply less personal data, both of which are likely to appeal to them.

198. Rob Nicholas Stone, *Data as Capital*, MEDIUM (May 24, 2018), https://medium.com/datavest/data-as-capital-d2a07533b04a [https://perma.cc/67KG-M2C9]; *see also* DATAVEST, https://www.datavest.org/ [https://perma.cc/7YL5-WJQQ].

To effect the necessary paradigm shift, this Section maps out how ROD can be implemented in practice. First, it outlines a conceptual framework for assessing ROD and considers the most appropriate use cases. Next, this Section examines how best to engage consumers and enable them to scrutinize data-for-services transactions. Last, this Section explores potential regulatory and other pathways to adopting ROD, with the aim of creating a competitive market in which tech firms are incentivized to maximize consumers' ROD.

### *A. Principles for Evaluating Return on Data*

At present, there is no precise formula, algorithm, or diagnostic tool for gauging the relationship between the utility consumers gain and the data price they pay.[199] Before attempting to advance more concrete proposals, developers and lawmakers need at least a tentative conceptual framework for evaluating data-for-services transactions. The following principles, explored below, aim to provide this framework:

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.*

#### 1. ROD = U / D

ROD gauges the relationship between two variables in data-for-services transactions: (i) the benefits consumers receive and (ii) the data price they pay. Calculating the ratio between these variables in a given data-for-services transaction yields the ROD. This is different from Weigend's notion of "data efficiency," which relates to the *purpose* of data collection.[200] Data efficiency considers whether the data collected are a genuine input into the services provided. Weigend likens data to fuel, which can be used with varying degrees of efficiency. For example, a mobile navigation app that collects only location data necessary for the user to reach the destination

199. *See* sources cited *supra* note 53 (regarding the difficulty in determining the value of data); *see also* WEIGEND, *supra* note 3, at 3119–20.

200. *See* WEIGEND, *supra* note 3, at 3048–50, 3146–58.

would be "data efficient." In contrast, a mobile game that collects personal data unrelated to the game would be "data inefficient."

The notion of data efficiency is problematic for several reasons. First, although data are indeed inputs into many services, the analogy between data and fuel is questionable. Unlike fuel, data are not fungible.[201] Second, it is not always clear which data are necessary for, or actually improve, the services provided.[202] Some data may contribute only to future developments, not present applications.[203] Are these 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.[204] Therefore, the purpose of collection may emerge only later.[205] Fourth, consumers are unlikely to be concerned about data efficiency.[206] Consider the fact that in ordinary retail transactions consumers do not fret over whether the money they pay *contributes* to the product they purchase. Rather, consumers care about how much they spend and for what. In conducting a cost-benefit analysis, consumers weigh up the benefits of a 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 that consumers

201. *See supra* note 54 (regarding the economic characteristics of personal data).

202. *See* Narciso, *supra* note 166, at 205. *Cf* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019) ch. 3 fig. 2 (purporting to distinguish between behavioral data required for services and "behavioral surplus").

203. *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 [https://perma.cc/NL78-46KR].

204. *See, e.g., In re: WhatsApp*, ELECTRONIC PRIVACY INFO. CTR., https://www.epic.org/privacy/internet/ftc/whatsapp/ [https://perma.cc/57LM-WL5V] (regarding the transfer by WhatsApp of its users' personal data to Facebook in 2016); 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 [https://perma.cc/XP7D-6E64].

205. 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*, 35 ACM TRANSACTIONS ON INFO. SYS., no. 4, 2017, at 43:1.

206. *But see* Morey et al., *supra* note 203 (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).

make alongside data payments? Ride sharing services, for example, typically require consumers to pay both personal data and money. Factoring monetary payments into ROD would involve comparing two different forms of payment—personal data and money. Computing both of these together to produce the ROD score would require a common unit of measurement, most likely money, which would involve converting the personal data provided by consumers into a specific monetary figure.[207] But, as discussed, placing a monetary price on data is riddled with difficulties, including due to the different subjective value which different people attach to personal data.[208] While pseudo-calculations of the monetary value of data may create a façade of precision and rigor, due to their enormous variance and conflicting methodologies they would be unhelpful and even misleading.

Even if there existed an accepted method for pricing data, it is not clear that doing so would actually assist in assessing ROD. Unlike micropayments that require placing a monetary price on data (as users are actually paid that amount in exchange for supplying data), ROD obviates the need for such calculations as it instead evaluates a ratio between two variables, namely (i) the benefits consumers receive and (ii) the data price they pay. Its focus is the relationship between these two variables—i.e., what a user receives in exchange for the data they supply—not translating them into monetary terms. Further, ROD does not purport to capture every externality or cost imposed on consumers in the context of data-for-services transactions, such as downstream data risks, user attention, opportunity costs or, for that matter, monetary payments.[209] While the concept of ROD could be expanded in the future to include these and other factors, stretching it too broadly at this stage would undermine its implementation. For now, the cost-benefit analysis that ROD facilitates must remain within more narrowly-defined parameters.

The challenges involved in measuring ROD, although shaped by the particular characteristics of the services that data-driven companies provide to consumers, have an analog in ordinary business accounting—namely, measuring the value of intangible assets. Techniques used to value patents, good will, or human resources are highly subjective and often incomplete and costly, especially in the absence of an efficient market that

207. *See* POSNER & WEYL, *supra* note 22, at 243 (arguing that monetary pricing is necessary to assess the value of data).

208. *See supra* note 53 (regarding the difficulty in determining the value of data).

209. *But see* WEIGEND, *supra* note 3, at 3146–58, 3131–35; Solove, *supra* note 73, at 1902 (suggesting that privacy law should address the downstream uses of data and associated risks, not their initial collection).

can price them with greater precision.[210] Nevertheless, various proxies are routinely employed to determine the value of intangible assets. Accounting tools, ranging from cost-based measures to anticipated cash flow, suggest that these measuring challenges are not altogether intractable.

Although ROD may at first glance appear to lack many of the ostensibly concrete yardsticks typically used to measure the value of the intangible assets that populate company financial statements, a few qualifications are in order. First, accounting techniques and the results they render are notoriously malleable, yet they continue to be used.[211] Second, ROD does not seek to price in monetary terms the utility which consumers receive and the personal data they provide (as accountants purport to do for intangible assets).[212] By, instead, comparing the relationship between data provided and utility received, ROD is arguably less ambitious than many run-of-the-mill accounting practices. Third, as will be elaborated, in data-rich contexts consumers' actual engagement with the services they access can be highly instructive. The way each individual uses a service can reveal the value of the utility she gains and the disutility (if any) she experiences in supplying personal data. Fourth, even if the methods of calculating ROD are imperfect, the very act of translating the exchange inherent in data-for-services deals into a mental model which consumers can understand—ROD—will convey to consumers the transactional nature of their relationships with tech firms and prompt consumers to treat these arrangements as a *quid pro quo*.[213]

### 2. Personalized and Dynamic Insight

The growing literature on the personalization of law supports tailoring legal solutions and regulatory tools to the needs, preferences and characteristics of individuals.[214] ROD is no exception. ROD scores must be

210. Nick Szabo, *Measuring Value*, SATOSHI NAKAMOTO INST. (1997), https://nakamotoinstitute.org/measuring-value [https://perma.cc/U9V6-96WV].

211. *Id.* This can perhaps be explained by the misalignment of interests that plagues the valuations of assets in company financial statements, which are not configured for clarity but to satisfy the relevant stakeholders.

212. *See supra* note 53 (regarding attempts to assess the value of personal data).

213. *See* L. Jean Camp, *Mental Models of Privacy and Security*, 28 IEEE TECH. & SOC'Y 37 (2009).

214 *See* Busch, *supra* note 175, at 315–19 (regarding the personalization of consumer law), 319–22 (regarding the personalization of data privacy law). *See generally* Ariel Porat & Lior Jacob Strahilevitz, *Personalizing Default Rules and Disclosure with*

unique to each consumer for several reasons. Different consumers typically 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 subjectively relate to data collection in different ways. For example, some consumers may be more sensitive than others to apps accessing a device's microphone. In addition, the performance, and thus utility, of an app may vary across different users' devices. Consumers also value services differently. A particular feature may be important to some users but not others. ROD must therefore be personalized and factor in these individual, consumer-specific metrics.

Encoding the more subjective metrics, such as the value that specific individuals attach to certain types of personal data or certain features of services, will also be challenging. Survey feedback could provide some insight into consumers' experiences. However, analyzing consumers' actual interactions with services and data collection would be far more illuminating.[215] 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, does not necessarily correlate with the frequency with which they are accessed.

The utility function of ROD, like its corresponding data price, is both complex and personal. However, this does not mean that it cannot be calculated or at least approximated. Tech firms regularly conduct A/B tests that measure users' responses to different versions of a digital product and thereby reveal users' otherwise hidden subjective experiences and preferences. In a similar way, consumers' interactions with the services they access could be used to tacitly elicit their experiences and preferences,

*Big Data*, 112 MICH. L. REV. 1417 (2014); Omri Ben-Shahar & Ariel Porat, *Personalizing Negligence Law*, 91 N.Y.U. L. REV. 627 (2016); Omri Ben-Shahar & Ariel Porat, *Personalizing Mandatory Rules in Contract Law*, 86 U. CHI. L. REV. 255 (2019); Matthew Kugler & Lior Jacob Strahilevitz, *Assessing the Empirical Upside of Personalized Criminal Procedure*, 86 U. CHI. L. REV. 489 (2019); Adi Libson & Gideon Parchomovsky, *Toward the Personalization of Copyright Law*, 86 U. CHI. L. REV. 527 (2019).

215. *But see* Nick Merola, *The Satisfaction Trap: Navigating Sentiment Measurement for Complex Products*, MEDIUM (Dec. 19, 2017), https://medium.com/facebook-research/the-satisfaction-trap-35f94ee9d9d8 [https://perma.cc/7AKY-UBEE] (discussing the emphasis a researcher at Facebook placed on the benefits of qualitative testing over quantitative measuring in measuring user satisfaction).

whether concerning the services themselves or the data consumers supply in order to access the services. These insights could then be encoded in personalized ROD evaluations.

One notable challenge to calculating and personalizing ROD scores is the need to disaggregate personal data on an individual basis—i.e. for each particular user.[216] When User X supplies to a platform data relating to User Y (who also uses the platform but did not supply such data), who is deemed to supply the data in question? The data relate to User Y, but it is User X who supplied them. A corresponding issue affects the utility which users receive: User X may, whether directly or indirectly, benefit from the utility received by User Y. For the purpose of calculating ROD, should that utility be credited toward User X's utility or User Y's utility? This line of questioning is vital to unpacking precisely which personal data and what utility will be credited toward a particular individual's ROD score. To simplify the initial implementation of ROD, it would probably be prudent to calculate a user's data payment by reference only to the data that the user herself supplies and to calculate the corresponding utility by reference only to the utility that she herself receives, rather than by attempting to quantify the network effects and other positive externalities generated by other users.

Importantly, ROD varies not only across different individuals, but also over time. The scope of data collection and the utility of services are not fixed.[217] For example, an app may alter the scope of data it collects; a consumer may adjust an app's data collection permissions; an app's features may evolve; its performance may fluctuate; a consumer may change the way in which she uses an app and the value she attaches to its features or different types of personal data. Therefore, data price and utility cannot be fully computed in advance. The calculations which produce ROD scores must therefore be dynamic.[218]

Assessing ROD in real time is likely to require employing different metrics at different points in time. The *initial* ROD evaluation of a mobile app (upon installation or before it has been used) will need to rely on more generic, non-personal metrics, as the information required to produce personalized evaluations can only be sourced from a user's actual

216. This issue may turn on the legal question of who owns or holds rights in the data. *See* Victor, *supra* note 19.

217. *See* WEIGEND, *supra* note 3, at 3213–16.

218. *Cf. id.* at 5349–52 (arguing that frequent updates to the ROD metrics would make it difficult for consumers to conduct meaningful comparisons between different service providers.)

interaction with the app.[219] An app's default data permissions could be instructive, as could the average ROD of other users of the app. In addition, a user's interactions with other apps could shine light on the types of personal data and services she values, which would help predict the expected data price and utility of the app for that particular user. By contrast, *later* ROD evaluations (after the user has interacted with the app) could employ more personal metrics, based on a user's actual interaction with the app—including the scope of data collection actually occurring, app performance, and the user's engagement with different features of the app.

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. The implementation of ROD must be an iterative process. The methods for personalizing ROD scores and disaggregating personal data and utility among different users will need to be refined over time. 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[220]

3. It Takes Data to Evaluate ROD

Calculating ROD will be a data-intensive process. Information regarding both data collection and consumer behavior will be 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 . . . ."[221] As is the case for privacy tech

219. *See generally* Xuan Nhat Lam et al., *Addressing Cold-Start Problem in Recommendation Systems*, 2 PROC. INT'L CONF. ON UBIQUITOUS INFO. MGMT. & COMM. 208 (2008); Blerina Lika et al., *Facing the Cold Start Problem in Recommender Systems*, 41 EXPERT SYS. APPLICATIONS 2065 (2014); Andrew I. Schein et al., *Methods and Metrics for Cold-Start Recommendations*, 25 PROC. ACM SPECIAL INT. GROUP ON INFO. RETRIEVAL CONF. ON RES. & DEV. INFO. RETRIEVAL 253 (2002).

220. *See* WEIGEND, *supra* note 3, at 3234–3237; *see also* Strandburg, *supra* note 26, at 145.

221. WEIGEND, *supra* note 3, at 229–236; *see also id.* at 145. In addition, the title of Weigend's book is "Data *for* the People" (emphasis added). *See also* Busch, *supra* note [175], at 326; David A. Hoffman & Patricia A. Rimo, *It Takes Data to Protect Data*, *in* PRIVACY HANDBOOK, *supra* note 48, at 546; DATAWALLET,

and other personalized services and regulatory tools, data collection is a pre-requisite for generating ROD evaluations. It is the price of making data-for-services transactions more transparent.

Many data points are required to measure the data 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.[222] Clearly, measuring only the quantity of data collected is 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 must send an API request to the operating system.[223] For example, Skype sends 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.[224] In the case of Skype, for example, 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 consumers share with mobile apps.

Mobile apps owned by Google and Apple, such as Google Calendar and Apple Music, complicate ROD evaluations.[225] As explained, Google and Apple can, via API requests, indirectly access most data collected by mobile

---

https://app.datawallet.com/ [https://perma.cc/E8KK-KJWE] (for a commercial application of this philosophy).

222. The encryption and compression of outbound data may pose additional challenges.

223. *See generally* Jenn Chen, *What Is an API & Why Does It Matter?*, SPROUT SOC. (Jan. 31, 2018), https://sproutsocial.com/insights/what-is-an-api/ [https://perma.cc/C2FM-2JY8].

224. 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 60 (regarding passive data collection).

225. 23 of the 25 most-downloaded Android apps are owned by either Google or Facebook. *See Android Market History Data and Ranklists*, ANDROIDRANK, https://www.androidrank.org/ [https://perma.cc/8ZRP-F23N].

apps, including third party apps. Accordingly, monitoring the API requests sent by Google Calendar to Android (Google's own operating system) would not be instructive. That Google Calendar may, for example, collect location data is uninformative; Google *already* can, and perhaps already does, collect location data via the Android operating system or other Google apps, such as Google Maps. Seen in this light, users' data-for-services transactions involving apps owned by Google and Apple are part of much larger transactions with Google and Apple.[226] 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. To overcome this issue, ROD may need to be evaluated in relation to the proprietor of each app, rather than in relation to the app itself.[227]

Just as many data points are needed to assess the data price that consumers pay, so too are many data points needed to assess the utility that consumers gain. Exploring the best proxies for consumer utility and deciding what weight to place on each of them will be challenging. A significant number of the services that tech firms provide are "experience goods" or "credence goods," the quality of which is difficult for consumers to evaluate, even post-fact.[228] Consumer ratings of apps, app popularity and comparisons with competing apps may shed light on an app's utility.[229]

226. 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 204 (regarding Facebook's plans to consolidate the infrastructure of the various platforms which it owns).

227. 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*, 1 ACM INTERACTIVE MOBILE WEARABLE & UBIQUITOUS TECH., no. 3, 2017, at 42:1. Further, given that the infrastructure of certain tech firms (especially Google) is ubiquitous and the utility they provide spans many applications, the per-proprietor approach may also be problematic.

228. *See* Strandburg, *supra* note 26, at 131–32. *See generally* Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 AM. ECON. REV. 941 (1963); 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).

229. Some of these already feature in Google Play, Apple's App Store and third-party comparison sites. *See e.g., Snapchat vs. WhatsApp*, VERSUS,

Technical metrics, such as app performance, and personal metrics, such as frequency of use, are also informative.[230] As explained, the most illuminating insights into the benefits consumers receive will be gleaned from analyzing their actual interactions with services. Consider, for example, a navigation app that collects the equivalent data from two different users but where only one of those users takes advantage of the app's real-time traffic updates to alter their chosen route. All else being equal, the user who utilizes the real-time traffic updates will receive greater utility from the app, which will translate into the app delivering to them higher ROD than to the other user.

More subjective metrics, such as an individual's personal assessment of an app's features, could also be employed. But subjective metrics, whether relating to utility or data price, are difficult to quantify and encode.[231] How can one measure the value of forging a new relationship via a dating app or finding a dream job on LinkedIn?[232] How can one calculate an individual's personal sensitivity to certain types of data collection? Answering these questions—which touch upon some of the fundamental issues facing the growing personalization of law and policy[233]—is beyond the scope of this article. Nevertheless, to holistically reflect the data price consumers supply and the utility they gain, ROD evaluations will need to factor in certain subjective metrics, as elicited from the best available information on consumers' interactions with the services they use. Capturing these subtle insights is likely to require further access to personal data.

#### 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

---

https://versus.com/en/snapchat-vs-whatsapp [https://perma.cc/D6GA-HHXG].

230. *See* WEIGEND, *supra* note 3, at 3181–84. But simple measurements of screen time and data consumption are poor indicators of utility. While 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* Section V.A.4.

231. *See* WEIGEND, *supra* note 3, at 3140, 3176–79.

232. *Id.* at 2911–16.

233 *See generally* Anthony J. Casey & Anthony Niblett, *A Framework for the New Personalization of Law*, 86 U. CHI. L. REV. 86 (2019). *See also infra* note 214.

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 a consumer gains from one of these apps with another would not be instructive.[234] Apart from the nature of the services provided, data-for-services transactions that share in common other features may also lend themselves to ROD evaluations. For instance, services delivered in similar contexts (e.g., in-car apps) or to similar demographics (e.g., small business owners) may also be suitable use cases.

The key is to compare like with like. This will be easiest where the utility of the product is similar. For example, Skype, LINE and Viber all provide similar services, namely, voice and video calls. Therefore, comparing their respective sound and image quality, connection reliability, and user experience would be helpful. In each category of mobile apps competing apps offer similar services—music (e.g., Spotify and SoundCloud), podcasts (e.g., Stitcher and Podbean), storage (e.g., Dropbox and OneDrive), productivity (e.g., Quick PDF Scanner and CamScanner), and photo sharing (e.g., Flickr and Imgur).[235] There are also competing voice assistants—Alexa, Siri, and Google Assistant. Products and services in each of these categories are 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. 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 assess the utility and data price of similar services, which are most likely to draw consumer

234. 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), http://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf [https://perma.cc/XP73-MJSD] (regarding the benefits of network effects); *Rise of Data Capital*, *supra* note 54, at 7 (differentiating between direct and indirect network effects).

235. 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* Section V.A.1.

attention.[236] 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 decisions when choosing between competing service providers.

### *B. Nudging Return on Data*

Assessing ROD will not on its own enable consumers to navigate the tradeoffs inherent in data-for-services transactions. ROD scores must be actively communicated to consumers. As explained, consumers do not presently *experience* the transactional nature of their relationships with tech firms. Only if ROD is salient, will consumers tangibly experience the exchange underlying these transactions and, in turn, incorporate ROD into their decision-making.

Like with any transparency-enhancing technology, simplicity is key.[237] The average consumer should receive only the most essential ROD information. A clear snapshot of the data a consumer supplies to a service provider and the utility she receives in return will relieve her of the burden of conducting overly complex analysis and the associated cognitive overhead.[238] By providing palatable information, ROD will serve as a choice

236. *See* Xia et al., *supra* note 91, at 3–4 (explaining that consumers tend to pay greater attention to price discrepancies between similar products).

237. *See generally* Urs Gasser, *Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy*, 130 HARV. L. REV. F. 61, 65 (2016); Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1414 (2011); Christian Zimmermann, *A Categorization of Transparency-Enhancing Technologies*, AMSTERDAM PRIVACY CONF. 2015 (revised July 22, 2015), https://arxiv.org/abs/1507.04914 [https://perma.cc/DC7F-HUQY].

238. POSNER & WEYL, *supra* note 22, at 244–45. 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 or "decision fatigue." *See generally* Kathleen D. Vohs et al., *Making Choices Impairs Subsequent Self-Control: A Limited-Resource Account of Decision Making, Self-Regulation, and Active Initiative*, 94 J. PERSONALITY & SOC. PSYCH. 883, 895–96 (2008); Jonathan Levav et al., *Order in Product Customization Decisions: Evidence from Field Experiments*, 118 J. POL. ECON. 274, 296 (2010). But unlike in the case of micropayments, the imposition of transaction costs under ROD—much like the costs of developing the systems and infrastructure necessary to facilitate ROD—will be worthwhile as consumers will, it is hoped, ultimately receive greater utility in the form of better services.

engine encouraging consumers to reflect on the data prices they pay for the services they receive.[239] Consumers will be able to consider the merits of each data-for-services deal and make more deliberative decisions on how to spend the personal data they generate.[240]

Visualizing ROD could be particularly helpful in guiding consumers. Currently, several browsers employ visual symbols to communicate to users the security status of different websites.[241] Google Chrome, for example, uses different symbols to flag whether a website is secure, unsecure, or highly unsecure.[242] 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.[243] 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 fidelity calls. Apple's App Store and Google Play could then display the respective ROD scores in each app's profile, which would feature alongside other information, such as an app's rating and popularity. Alternatively, ROD scores could be displayed in the settings portals of a mobile operating system or as pop-ups within apps.[244]

---

239. *See generally* Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARV. BUS. REV. (Jan.–Feb. 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers [https://perma.cc/7GSR-NQ92].

240. *See generally* KAHNEMAN, *supra* note 77.

241. Adrienne Porter Felt et al., *Rethinking Connection Security Indicators*, 12 PROC. SOUPS 1 (2016); *What is an SSL Certificate?*, DIGICERT SYMANTEC, https://www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https?id=ssl-information-center# [https://perma.cc/NLH6-TN8N].

242. *Check If a Site's Connection Is Secure*, GOOGLE CHROME HELP, https://support.google.com/chrome/?p=ui_security_indicator [https://perma.cc/927J-WB2E].

243. *See* WEIGEND, *supra* note 3, at 3221–29 (likening the ROD scale to energy-efficiency ratings of appliances); KPMG, *supra* note 82, at 19.

244. *See* Rebecca Balebako et al., *The Impact of Timing on the Salience of Smartphone App Privacy Notices*, 5 PROC. ACM CONF. ON COMPUTER & COMM. SECURITY WORKSHOP ON SECURITY & PRIVACY IN SMARTPHONES & MOBILE DEVICES 63 (2015) (suggesting that consumers may pay greater attention to information

Importantly, personalized ROD dashboards, tailored to the needs, desires and characteristics of different consumers, would be more effective than a one-size-fits-all ROD interface.[245] For instance, some consumers may want more granular ROD insights. They may wish to understand the principles according to which ROD operates as well as the specific data points and metrics that ROD encodes. Customized user interfaces should be developed to convey this information.[246] In addition, the mechanics of ROD evaluations must themselves be transparent. Without disclosing the ROD algorithm, those conducting ROD evaluations could not be held accountable.[247] But the more transparent the ROD algorithm, the higher the chances that companies will successfully game it and configure services to have artificially high ROD scores.[248]

Making ROD salient in these ways and enabling consumers to experience the tradeoffs that characterize their relationships with data-driven companies 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,

---

provided within an app, compared with information available on an app store).

245 *See*, *e.g*, *Personalised Nudging for more Data Disclosure? On the Adaption of Data Usage Policies Format to Cognitive Styles* (2019), https://scholarspace.manoa.hawaii.edu/bitstream/10125/59877/1/0437.pdf; *Personalized Security Messaging: Nudges for Compliance with Browser Warnings* (2017) https://www.ndss-symposium.org/wp-content/uploads/2018/03/eurousec2017_08_Malkin_paper.pdf**!.**

246. *See, e.g.,* GHOSTERY, https://www.ghostery.com/ [https://perma.cc/A3LQ-Q264] (displaying both simple and detailed dashboards). These could be similar to "Schumer boxes," which outline to consumers the key terms of credit card agreements. *See* Fair Credit and Charge Card Disclosure Act of 1988, Pub. L. No. 100-583, § 2, 102 Stat. 2960 (1988); Hosea H. Harvey, *Opening Schumer's Box: The Empirical Foundations of Modern Consumer Finance Disclosure Law*, 48 U. MICH. J.L. REFORM 59, 60 (2014).

247. *See generally* PASQUALE, *supra* note 186, at ch. 5; Christian Sandvig et al., *Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms*, *in* 64 MEETING INT'L COMM. ASSOC. 1 (2014).

248. *See* JERRY MULLER, THE TYRANNY OF METRICS 3, 24, 77, 149 (2018); Hacker & Petkova, *supra* note 180, at 17*; 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).

status quo bias, and the information presented to or withheld from them.[249] The shaping of these factors is known as *choice architecture*.[250] 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.[251]

Put differently, every design choice is a *nudge*. Sunstein and Thaler define a nudge as any policy intervention designed to "alter[] people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives."[252] With the assistance of behavioral insights, choice architecture could be used to nudge consumers' decisions relating to personal data.[253]

249. *See* THALER & SUNSTEIN, *supra* note 86, at 3; Richard H. Thaler et al., *Choice Architecture* (Working Paper, 2010), http://papers.ssrn.com/abstract=1583509 [https://perma.cc/99CK-GHW5].

250. *Id.*

251. Acquisti et al., *supra* note 72, at 32–33; *see also* Idris Adjerid et al., *Choice Architecture, Framing, and Cascaded Privacy Choices*, 65 MANAG. SCI. 2267 (2018); Ron Hirschprung et al., *Analyzing and Optimizing Access Control Choice Architectures in Online Social Networks*, 8 ACM TRANSACTIONS ON INTELLIGENT SYST. & TECH., no. 4, 2017, at 57:1.

252. THALER & SUNSTEIN, *supra* note 86, 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).

253. *See* Serge Egelman et al., *Choice Architecture and Smartphone Privacy: There's a Price for That*, 2012 WORKSHOP ON ECON. INFO. SECURITY 211 (discussing a study in which 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.)

In recent years, several economists and computer scientists have proposed techniques for nudging consumers to protect their privacy.[254] They suggest that disclosing privacy risks will mitigate consumers' tendency to overlook and underestimate these risks.[255] 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.[256] However, these choice architecture proposals relate only to privacy.[257] They do not advocate comparing the data consumers supply with the utility they gain. Nor do these proposals seek to disclose ROD or prompt consumers to demand better deals from service providers. Like most of the legal frameworks and data platforms that have been discussed, choice architecture relating to personal data is also preoccupied with privacy. This need not be the case. *Choice architects can nudge ROD.*

Communicating ROD evaluations to consumers would frame their interactions with tech firms as a genuine exchange. If data-for-services deals were transparent, consumers would realize that the services they consume are not free but paid for with personal data. Nudging ROD in this way could tackle, and even harness, several cognitive and behavioral biases. If the data price were disclosed upfront, consumers would be less likely to overlook the longer-term costs of trading personal data. Upon seeing data collection as a price, consumers may become more selective in deciding which transactions to enter.[258] Although displaying ROD cannot guarantee that

254. *See, e.g.,* Hazim Almuhimedi et al., *Your Location Has Been Shared 5398 Times! A Field Study on Mobile Privacy Nudges*, 33 PROC. COMPUTER HUM. INTERACTION CONF. ON HUMAN FACTORS COMPUTING SYS. 787 (2015).

255. *See* Acquisti et al., *supra* note 72, at 13–14 (explaining how disclosing information about these risks may overcome the availability and overconfidence biases).

256. *See id.* at 17.

257. However, some tech firms 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 [https://perma.cc/A85M-ZT4J].

258. Yet, it need not altogether deter them from using data-driven services. *See, e.g.,* SALESFORCE, *supra* note 98, at 9 (indicating that consumers demand *both* personalized services and transparency around the use of personal data).

consumers will focus on the utility-to-data ratio of their exchanges with tech firms, it will at the very least equip consumers with a GPS-like tool to navigate the complex tradeoffs inherent in data-for-services transactions.[259] ROD would thus empower consumers and reduce their information asymmetry vis-à-vis tech firms.

ROD nudges could employ different degrees of forcefulness. A soft nudge might only provide information. For example, by simultaneously displaying the ROD of comparable mobile apps, app stores could nudge consumers toward selecting apps with higher ROD.[260] This would not impact consumers' ability to access apps with lower ROD. Meanwhile, 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*.[261] Yet, it would still not impose a particular choice. A consumer could nonetheless, after a longer search, opt for an app with lower ROD.[262] ROD nudges, by definition, leave consumers free to choose for themselves which services to purchase with the personal data they generate.[263] Nudging ROD would merely enable consumers to engage in a cost-benefit analysis and weigh the pros and cons of each transaction.

### *C. Pathways to Adopting Return on Data*

There are several potential routes to introducing ROD. Some involve mandatory regulation while others involve voluntary adoption by industry actors. To begin with, existing legal frameworks could be amended to

259. *See generally* CASS R. SUNSTEIN, ON FREEDOM (2019).

260. *See* Serge Egelman et al., 2009 *Timing Is Everything?: The Effects of Timing and Placement of Online Privacy Indicators*, PROC. COMPUTER HUM. INTERACTION CONF. ON HUMAN FACTORS COMPUTING SYS. 319 (explaining that nudges are most effective when introduced prior to consumers committing to particular choices).

261. *See* THALER & SUNSTEIN, *supra* note 86, at 6 ("Putting fruit at eye level counts as a nudge. Banning junk food does not."); Dan M. Kahan, *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem*, 67 U. CHI. L. REV. 607 (2000).

262. A consumer may do this because she trusts the app developer. *See generally* Morey et al., *supra* note 203 (explaining that consumers supply to companies they consider trustworthy more valuable data in exchange for comparable services).

263. *See* Acquisti et al., *supra* note 86, at 509–10; Adjerid et al., *supra* note 251, at 43.

incorporate ROD. For instance, the GDPR could institute the principle, already enshrined in the EU Directive, that personal data are the price consumers pay for many services. The rights of data subjects under the GDPR and other privacy law regimes, such as the CCPA, could be expanded to require that service providers monitor and disclose ROD to consumers. Mobile operating systems might, for example, be required to assess and communicate the ROD of third-party apps to consumers. Meanwhile, existing data protection authorities could oversee and enforce ROD regulation.

Alternatively, new legal frameworks could be developed to specifically institute and regulate ROD. Such frameworks might be more ambitious in their goals and methods. They could, for instance, mandate a minimum ROD in certain contexts, such as for particular types of platforms or for consumers with specific vulnerabilities. A specialized agency could be established to set standards for ROD and audit the ROD evaluations carried out by tech firms.[264]

Mandatory ROD regulation, whether in the form of amendments to existing legal frameworks or the establishment of new legal frameworks, may have many advantages. As an educational device,[265] ROD regulation could cultivate greater understanding of our interactions with service providers, much like the GDPR has increased awareness of privacy concerns. It could also jump-start the deployment of ROD nudges by mandating that service providers or intermediaries, such as app stores and operating systems, make ROD salient.[266] Thus, if properly designed and enforced, ROD regulation could ensure greater transparency around data-for-services transactions. The associated public scrutiny of such transactions might, in turn, drive companies to rethink the relationship between the personal data they collect and the services they provide, and even recalibrate the kind of deals they offer consumers.

However, some of these assumptions are tenuous. Apart from the likely political impediments to adopting ROD regulation, there is no guarantee that such regulation will successfully educate the public or meaningfully impact consumer behavior. It will be challenging to effect a paradigm shift toward ROD, especially given the entrenchment of the existing privacy-

264. *See* WEIGEND, *supra* note 3, at 3221–3229.

265. *See* CASS R. SUNSTEIN, HOW CHANGE HAPPENS 46 (2019) (regarding the expressive function of law in signaling social norms).

266. *See, e.g.,* Thaler & Tucker, *supra* note 239.

centric perspectives among companies and consumers alike.[267] In addition, it is notoriously difficult to regulate a moving target. Due to the complex and dynamic nature of the transactions that ROD seeks to evaluate, there is no straightforward way to craft legislation that properly captures and implements the principles of ROD and ensures the necessary transparency—let alone enforcement.

ROD regulation could also have unintended consequences. By demanding that companies comply with onerous requirements, such as ROD monitoring and disclosure, mandatory regulation could impose burdensome costs that stifle the technological innovation, risk-taking and investment that drive the data economy.[268] As mandatory regulation would not incentivize companies to embrace ROD but compel them to do so, companies' implementation of ROD would not necessarily align with their business interests. Companies would likely attempt to implement ROD as cheaply as possible, the outcome of which may be sub-optimal and even defeat the purposes of ROD. Ironically, mandatory regulation may also favor industry incumbents and disadvantage smaller companies with fewer resources available to absorb ROD compliance costs.[269]

---

267. *See generally* S. J. Liebowitz & Stephen E. Margolis, *The Fable of the Keys*, 33 J.L. & ECON. 1 (1990) (discussing the QWERTY keyboard, an archetypal case of path dependence); S. J. Liebowitz & Stephen E. Margolis, *Path Dependence, Lock-in, and History*, 11 J.L. ECON. & ORG. 205 (1995).

268. *See, e.g., Privacy Rights and Data Collection in a Digital Economy: Hearing before the S. Committee on Banking, Housing, and Urban Development*, 116th Cong. 6 (2019) (statement of Maciej Cegłowski, Founder, Pinboard), https://thrive.hyatt.com/en/thrive/human-rights.html [https://perma.cc/YK8A-SWSS] (regarding the compliance costs of GDPR); Jian Jia et al., *The Short-Run Effects of GDPR on Technology Venture Investment* (Nat'l Bureau of Econ. Res., Working Paper No. 25248, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278912 [https://perma.cc/YZ3P-VX7F]. *See generally* ADAM THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM (2014).

269. *See* Cegłowski, *supra* note 268; Leonid Bershidsky, *Europe's Privacy Rules Are Having Unintended Consequences*, BLOOMBERG (Nov. 14, 2018), https://www.bloomberg.com/opinion/articles/2018-11-14/facebook-and-google-aren-t-hurt-by-gdpr-but-smaller-firms-are [https://perma.cc/8FRP-FQP5]; Elizabeth Schulze, *Mark Zuckerberg Says He Wants Stricter European-Style Privacy Laws — But Some Experts Are Questioning His Motives*, CNBC (Apr. 1, 2019), https://www.cnbc.com/2019/04/01/facebook-ceo-zuckerbergs-call-for-gdpr-privacy-laws-raises-questions.html [https://perma.cc/LNQ5-5DGQ].

One alternative to mandatory regulation is self-regulation. Rather than mandate particular courses of action, self-regulation relies on companies voluntarily pursuing pro-social policies.[270] Under this approach, companies could themselves decide whether and how to assess ROD and engage consumers. Although self-regulation generally has several shortcomings[271]—including a lack of independence and external oversight, intrinsic conflicts of interest, and vulnerability to abuse—it also has distinct advantages. Under ROD self-regulation, service providers would not be burdened by external regulatory costs and additional barriers to entry, but would be given the opportunity to experiment with different approaches to ROD. The implementation of ROD in this context is likely to be more adaptive to changing user patterns and dynamic data-for-services business models. Instead of being constrained by regulatory standards, companies could design and deploy ROD mechanisms which align with their business vision and commercial interests.

But, in the absence of mandatory regulation, why would tech firms 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?[272] As a matter of fact, several major tech firms have publicly called for greater regulation of personal data.[273] If these companies are willing to support the imposition of

270. *See* Acquisti et al., *supra* note 50, at 479–81.

271. For criticism of privacy self-regulation, see Ira S. Rubinstein, *The Future of Self-Regulation Is Co-Regulation*, *in* PRIVACY HANDBOOK, *supra* note 49, at 503; Mark A. Lemley, *Private Property*, 52 STAN. L. REV. 1545, 1554–55 (2000); and Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1287 (2000).

272. *See* POSNER & WEYL, *supra* note 22, at 234; Acquisti et al., *supra* note 72, at 29.

273. *See* Jeff Horwitz & Deepa Seetharaman, *Facebook's Zuckerberg Backs Privacy Legislation*, WALL ST. J. (Jun. 26, 2019), https://www.wsj.com/articles/facebooks-zuckerberg-backs-privacy-legislation-11561589798 [https://perma.cc/KR3T-CFZG]; Sundar Pichai, *Privacy Should Not Be a Luxury Good*, N.Y. TIMES (May 7, 2019), https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html [https://perma.cc/K3VL-8FMQ]; Brad Smith, *Facial Recognition: It's Time for Action*, MICROSOFT (Dec. 6, 2018), https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/ [https://perma.cc/XD65-QPB2]; 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-

mandatory regulation that would force them to substantially alter their businesses, surely they would be willing to contemplate voluntarily adopting codes of conduct and practices that they can themselves design and implement.[274]

Tech firms are also facing a crisis of confidence, particularly in the wake of numerous high-profile privacy scandals.[275] They therefore want to be seen as proactively tackling concerns relating to personal data,[276] as norm entrepreneurs at the cutting edge of data policy.[277] Although public attention is largely focused on privacy protection, the notion that consumers deserve to receive more in return for the personal data they supply is gaining traction. If major tech firms were to self-regulate, they could improve their tarnished reputations and bolster trust among current and prospective customers.[278] And, the more companies that implement

privacy-laws-us-speech-brussels [https://perma.cc/7JN2-HZ9K]; Whittaker, *supra* note 7.

274. However, major tech firms may specifically support *mandatory* regulation because it tends to give them a comparative advantage over smaller firms. *See* Bershidsky, *supra* note 269; Schulze, *supra* note 269. In addition, mandatory regulation has the "advantage" of enabling companies to abrogate responsibility for questionable policy and practices, provided they comply with the regulation.

275. *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 [https://perma.cc/B2ZG-MRS7]; sources cited in *supra* note 116 (regarding the lack of trust in tech firms).

276. 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 deflect scrutiny away from Apple and Google. *See, e.g.,* Apple Inc. v. Pepper, 139 S. Ct. 1514 (2019) (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.,* Tripp Mickle, *Apple Touts New Privacy Features Amid Scrutiny of Tech Giants*, WALL ST. J. (June 3, 2019), https://www.wsj.com/articles/apple-touts-new-privacy-features-amid-scrutiny-of-tech-giants-11559589479 [https://perma.cc/BQ7W-JEEB]; 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 [https://perma.cc/8C86-NUU8].

277. *See* SUNSTEIN, *supra* note 265, at 45–46.

278. *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,

ROD, the stronger the ROD norm cascade, and the greater the reputational incentives for other companies to adopt ROD as well.[279]

ROD self-regulation may involve both technological and legal measures. Companies could develop tools to conduct ROD evaluations that they would communicate to customers. Companies could also more explicitly disclose that customers pay for services with personal data. For example, terms of service could grant customers a contractual right to know the ROD of a given service, even prior to accessing the service.

Another way to implement ROD is via a third-party organization that would monitor and publicize the ROD scores of different services.[280] There is a robust precedent for such a model: Net Promoter Scores (or NPS). NPS is a measure of customer satisfaction based on simple consumer surveys.[281] Although the derivation of NPS scores is controversial, NPS has been embraced by management across many industries, often as a predictor of growth, and plays an important role in the decision-making of many S&P 500 companies.[282] If a third-party company or industry watchdog were to track the ROD scores of competing services (generalized from the ROD of individual users) and consumers began to employ ROD in deciding which services to use, companies would turn to ROD as a proxy for customer satisfaction and even as a predictor of growth. Like NPS scores, ROD scores would enter boardrooms and impact the decision-making of major tech firms.

If consumers embraced ROD, data prices would over time become more elastic and better correlate with the utility of the services provided. Data collection would no longer be a flat fee that all consumers pay irrespective of how they wish to use a service. The relationship between the "give" and

---

2018), http://fortune.com/2018/11/08/mark-zuckerberg-facebook-reputation/ [https://perma.cc/7P5V-25Q2].

279. *See* SUNSTEIN, *supra* note 265, at 10–12.

280. *See, e.g.,* Smith, *supra* note 273 (proposing third-party testing of facial recognition); *see also* WEIGEND, *supra* note 3, at 3013.

281. *See* Frederick F. Reichheld, *The One Number You Need to Grow*, HARV. BUS. REV. (Dec. 2003), https://hbr.org/2003/12/the-one-number-you-need-to-grow [https://perma.cc/5MGW-9Z5K]; *What Is Net Promoter?*, NICE SATMETRIX, https://www.netpromoter.com/know/ [https://perma.cc/5P6T-VJWZ].

282. *See* Khadeeja Safdar & Inti Pacheco, *The Dubious Management Fad Sweeping Corporate America*, WALL ST. J. (May 15, 2019), https://www.wsj.com/articles/the-dubious-management-fad-sweeping-corporate-america-11557932084 [https://perma.cc/M75Q-WWU3]; *see also* WEIGEND, *supra* note 3, at 3203.

the "take" in data-for-services transactions would be better aligned. Tech firms would become accountable to consumers as they could no longer charge arbitrary data prices with impunity. Service providers would suffer adverse consequences if they unilaterally increased the data price without increasing the corresponding utility that consumers receive.

Put differently, as ROD becomes more prevalent, customer satisfaction and customer retention would increasingly hinge on ROD. In order to retain and attract ROD-sensitive consumers, service providers would have an incentive to carefully calibrate the scope of data collection they carry out. These developments would eliminate the moral hazard by which companies currently extract personal data at little or no cost (in terms of customer satisfaction and retention) and thereby correct the market failure that currently affects most data-for-services deals.

Ultimately, the more broadly ROD is adopted, the more ROD will interest consumers, as paying a higher data price—whether in terms of the quantity or quality of data—will actually buy them better services. The purchasing power of personal data will increase. By deciding which services to use based on ROD, consumers will signal their preferences to service providers, namely, lower data prices and higher-quality services. A critical mass of ROD-sensitive consumers demanding greater ROD will drive companies to respond by offering consumers greater ROD.[283] Companies will thus need to pay close attention to the ROD they offer consumers, as well as the relationship between the data collection they perform and the services they provide.

Once several major tech firms are onboard, others will have to follow or risk losing business. A competitive market will emerge. Companies will have an incentive to increase the ROD they offer consumers and will need to compete with one another to attract the business of consumers seeking higher ROD. By evaluating and communicating the ROD of competing services, third-parties and intermediaries (such as app stores and operating systems) will further stimulate this ROD-driven market. And, the more transparent and accessible ROD scores become, the more the market will thrive.

The introduction of ROD also presents exciting opportunities for startups. New market entrants, by offering consumers superior data-for-services deals, could draw business away from the tech giants.[284]

283. 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.

284. *See* SCHNEIER, *supra* note 2, at 206 (regarding the potential business opportunities if the costs of data collection were to increase). *See generally*

Companies that are early to adopt ROD will have a first-mover advantage. Consumers, aware of the transactional value of personal data, will be more inclined to share valuable data with companies offering more attractive ROD deals.[285] And the more consumers take interest in ROD, the steeper the ROD adoption curve among service providers. Startups that offer greater ROD will receive higher-quality and more relevant data from consumers, which will give them an edge over larger rivals. In particular, it will assist startups in performing consumer and product analytics and in developing and training AI.[286] ROD-driven competition could in the long run disperse market power among different service providers.[287] Entrepreneurs

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).

285. *See* POSNER & WEYL, *supra* note 22, at 231–2.

286. *Id.* at 220–21 (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); Arrieta-Ibarra et al., *supra* note 24, at 41. *But see* Dan Breznitz, *Balancing Privacy and Commercial Values Data and the Future of Growth: The Need for Strategic Data Policy*, CTR. FOR INT'L GOVERNANCE INNOVATION (Apr. 19, 2018), https://www.cigionline.org/articles/data-and-future-growth-need-strategic-data-policy [https://perma.cc/M3U5-GYT3] (suggesting that companies already benefit from increasing marginal returns on personal data).

287. *See* Stucke, *supra* note 64, at 303–07 (suggesting that Big Tech has 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 [https://perma.cc/YKX9-GLHL]; *see also* Kiran Stacey, *Senior Democrat Suggests 'Glass-Steagall' Law for Tech Companies*, FIN. TIMES (Mar. 4, 2019), https://www.ft.com/content/561b8546-355c-11e9-bd3a-8b2a211d90d5 [https://perma.cc/EPE2-ZTEN]; 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 [https://perma.cc/J9KP-DNYF] (advocating antitrust action with respect to Big Tech firms). By conveying the idea that consumers pay a price for services which are often depicted as free of charge, ROD scores could perhaps be considered under the consumer welfare standard in antitrust law. *See generally* Reiter v. Sonotone Corp., 442 U.S. 330 (1979).

attentive to emerging ROD norms and consumer expectations may have the potential to challenge the dominance of the Big Tech incumbents.[288]

## CONCLUSION

This Article has sought to advocate a new paradigm for analyzing data-for-services transactions. As we debate the future of data law and policy, including the introduction of federal privacy legislation, it is increasingly clear that privacy is not the only issue at stake. We must also consider what consumers receive in exchange for the data they share—that is, consumers' return on data (ROD). Most legal frameworks and many data platforms remain preoccupied with privacy and continue to overlook the transactional model that characterizes businesses in the data economy. This Article aims to buck that trend and challenge the reigning 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 that underpins data-for-services transactions.

To make data-for-services transactions more transparent, we need both to refine the methods for conducting personalized ROD evaluations and to effectively communicate the results to individual consumers. Consumers must understand and *experience* the transactional nature of their relationships with data-driven service providers. Showcasing the ROD scores of competing services will enable consumers to become conscious of the tradeoffs they routinely make. Equipped with a choice engine to better navigate the range of data-for-services deals on offer, consumers will be able to make more informed decisions regarding which deals to accept, and which to reject.

The implementation of ROD, like proposals for personalizing other areas of the law, clearly warrants further investigation. Who will develop and deploy practical tools for assessing ROD—government, startups, or major tech firms? Should regulation be introduced to jump-start or oversee the process? How can we mitigate the risk of ROD evaluations being manipulated or gamed? Notwithstanding these important questions, we can assume that if consumers begin to factor ROD into their decision-making at scale, service providers will need to respond. If consumers decide which

288. *See generally* 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); ZUBOFF, *supra* note 202; Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2016); Lina M. Khan, *The Separation of Platforms and Commerce*, 119 COLUM. L. REV. 973 (2019).

services to use even partly on the basis of ROD, market forces will incentivize tech firms to increase the ROD they offer. To compete for the business of ROD-sensitive 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, personalized legal frameworks and regulatory tools may herald new approaches. Consumers may begin to 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.