Treating Consumer Data Like Oil: How Re-framing Digital Interactions Might Bolster the Federal Trade Commission's New Privacy Framework

Andrew Hasty*

TABLE OF CONTENTS

* J.D., The George Washington University Law School. Andy would like to thank his wife Isabelle and all of his friends within the FTC's Division of Privacy and Identity Protection for their patience and helpful feedback.

I. INTRODUCTION

Americans have grappled with consumer privacy concerns for a long time. More than 120 years have passed since Samuel Warren and Louis Brandeis—fearing that innovations such as "instantaneous photography" and "newspaper enterprise" would "proclaim[] from the house-tops" what "is whispered in the closet"—wrote their famous article calling for "the right 'to be let alone.'"[1] And yet, the same concern remains manifest in today's headlines.[2] More than a century later, solutions to the consumer privacy dilemma have not materialized.

Today's technologies enable unprecedented collection and analysis of consumer data, but mechanisms aimed at protecting consumer privacy have lagged.[3] When consumers use search engines to explore the web, exchange messages with friends, or download apps to their smartphones, these digital interactions are often tracked and monetized by a number of behind-the-scenes companies.[4] Yet, as business models centered on monetizing consumers' data and attention have taken off,[5] safeguarding consumer privacy in the United States remains the job of a motley assortment of protections.[6] Indeed, to the extent that regulations exist, they are "sectoral, with different laws regulating different industries and economic sectors."[7] This patchwork has created large gaps in coverage, making the Federal Trade Commission (FTC)—through enforcement of section 5 of the Federal Trade Commission Act ("Section 5")[8]—the United States' "regulator" of consumer privacy.[9]

Over the years, the FTC has skillfully leveraged its tools and experience to advance and enforce three different frameworks for

---

1. Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4. HARV. L. REV. 193, 195 (1890).

2. *See, e.g.*, Editorial, *The End of Privacy?*, N.Y. TIMES, July 15, 2012, at SR10, *available at* http://www.nytimes.com/2012/07/15/opinion/sunday/the-end-of-privacy.html; *see also* Bruce Schneier, *Will Giving the Internet Eyes and Ears Mean the End of Privacy?*, THE GUARDIAN (May 16, 2013, 7:26 AM), http://www.theguardian.com/technology/2013/may/16/internet-of-things-privacy-google.

3. *See, e.g.*, Paul Ohm, *Don't Build a Database of Ruin*, HARV. BUS. REV. (Aug. 23, 2012), https://hbr.org/2012/08/dont-build-a-database-of-ruin/.

4. *See* Julie Brill, *Data Industry Must Step Up to Protect Consumer Privacy*, AD AGE (Oct. 28 2013), http://adage.com/article/guest-columnists/data-industry-step-protect-consumer-privacy/244971/.

5. *See, e.g.* Ohm, *supra* note 3 ("Many businesses today find themselves locked in an arms race with competitors to see who can convert customer secrets into the most pennies.").

6. *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 587 (2014).

7. *Id.*

8. Section 5 of the FTC Act provides that "unfair or deceptive acts or practices in or affecting commerce . . . are . . . unlawful." Federal Trade Commission Act of 1914, ch. 311, § 5, 38 Stat. 719 (codified as amended at 15 U.S.C. § 45 (2012)).

9. Solove & Hartzog, *supra* note 6, at 587–88.

safeguarding consumer privacy, but it has so far been unable to create a regulatory model that keeps pace with rapidly evolving technologies.[10] Beginning in the 1990s, as consumers turned to the Internet to communicate, shop, and explore new possibilities, the FTC promulgated the first of its three privacy frameworks.[11] Widely referred to as the "notice and choice" framework, the FTC's initial attempt to grapple with the consumer privacy implications of connected digital technologies centered on encouraging companies to tell consumers how their data was handled so that consumers could choose which services to use.[12] Despite some early successes, the "notice and choice" approach quickly proved inadequate to deal with the "increasing convergence of online and offline data systems" ushered in by the new millennium.[13] Under its second framework—referred to as the FTC's "harm-based" approach—the FTC "targeted practices that caused or were likely to cause physical or economic harm, or 'unwarranted intrusions in [consumers'] daily lives,'" instead of "emphasizing potentially costly notice-and-choice requirements for all uses of information."[14]

Like the earlier "notice and choice" model, however, the harm-based framework also relied heavily on self-regulation, which developed too slowly to provide consumers with "adequate and meaningful protection" in light of technology's continued march forward.[15] In a recent effort to ensure that adequate and meaningful consumer privacy protections kept pace with technological change, the FTC set out to develop a third framework. In March 2012, after hosting a series of public roundtables and issuing a preliminary report for notice and comment,[16] the FTC released its latest framework for safeguarding consumer privacy.[17]

---

10. *See, e.g.*, *Hearing on "The FTC at 100: Views from the Academic Experts," Subcomm. on Commerce, Mfg., & Trade of the Comm. on Energy & Commerce*, 113th Cong. (2014) (statement of Paul Ohm, Professor, University of Colorado Law School) (praising the FTC for its prudent approach to privacy regulation but noting limitations that prevent the FTC from addressing privacy harms imposed by changing technologies), *available at* http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Ohm-CMT-FTC-100-Academic-Perspective-2014-2-28.pdf.

11. *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICY MAKERS 6–7 (2010), *available at* https://www.ftc.gov/sites/default/files/documents/ reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf .

12. *Id.* at iii.

13. *Id.* at 9.

14. *Id.* (internal citations omitted).

15. *Id.* at iii.

16. *Id.* at iii–v.

17. FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

Meanwhile, consumer technologies—and the privacy problems they raise—continue to evolve. Yesterday's desktop-based Internet technologies are paving the way for tomorrow's "Internet of Things," which seeks to give every device, from pacemakers, eyeglasses, and refrigerators to watches, cars, and HVAC systems, the ability to sense, remember, and communicate information with every other device.[18] Although these technologies promise to improve efficiency, lower costs, and create new products and services that enrich consumers' lives, they also raise serious privacy concerns by making consumers' every action potentially visible to anyone or anything with an Internet connection.[19] Already, as companies rush to extract information from consumers, the expression "data is the new oil" has become a tired cliché.[20] If consumer privacy regulation in the United States is to keep pace without restraining technological development, it must scale to meet complex and evolving challenges.

With the "Internet of Things" on the horizon, this Note asks how the United States' approach to consumer privacy regulation would change if the "digital oil" cliché were taken seriously. The Note proceeds by describing the consumer technology landscape as it currently exists, before turning to the FTC's role as the United States' primary privacy regulator. Through references to existing technologies and services, this Note argues that consumers' digital interactions should be recognized as the commercial exchanges of value that they are. Such a framing would substantiate the FTC's new privacy framework and could realistically be achieved through incremental implementation. After submitting the "data-as-oil" construct to public scrutiny for further refinement, the FTC could bring pilot cases to establish and stress test the theory in varying factual scenarios. This approach—matching the FTC's new privacy framework with the "data-as-oil" recognition—could ultimately be used to create a flexible regulatory solution to the complex privacy problems created by evolving technologies.

---

18. *See generally* Edith Ramirez, Chair, FTC., Opening Remarks at the FTC Public Workshop: The Internet of Things: Privacy and Security in a Connected World (Nov. 19, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/opening-remarks-ftc-chairwoman-edith-ramirez-federal-trade-commission-Internet-things-privacy/131119iotremarks.pdf.

19. *See, e.g.*, Maureen K. Ohlhausen, Comm'r, FTC., Remarks at the Consumer Electronics Show: Promoting an Internet of Inclusion: More Things AND More People, (Jan. 8, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/promoting-Internet-inclusion-more-things-more-people/140107ces-iot.pdf.

20. *See, e.g.*, John Naughton, *The Web Giants Pumping Us for Data*, THE GUARDIAN (Aug. 31, 2013, 7:06 PM), http://www.theguardian.com/technology/2013/sep/01/big-data-corporations-information.

II. THE MODERN DIGITAL ENVIRONMENT DEMANDS A NEW REGULATORY APPROACH

The modern digital environment requires a flexible regulatory structure capable of resolving complex consumer privacy dilemmas. As the number of transistors that can fit onto a square inch of silicon continues to double approximately every two years,[21] today's engineers continue to conceive and build products, services, and systems that solve problems and enrich lives. These developments also foster tremendous amounts of data collection, sharing, and use— raising difficult consumer privacy dilemmas that outstrip regulatory capacity. If consumers are to retain control over their information while harnessing the promise of tomorrow's technologies, the United States must implement a flexible regulatory solution that keeps pace with technological development.

A. Consumer Technologies Are Rapidly Evolving

What used to be confined to the creative minds of yesterday's science fiction writers is now the stuff of today's technological reality. Over the past few years, consumers have started carrying powerful personal computers at an astonishingly fast rate. Smartphone adoption has "outpaced the 1980s PC revolution, the 1990s Internet boom, and the social networking craze of the 'aughts,'"[22] and is reported to be "10 times that of what we might now perceive as the positively glacial pace of early personal computer adoption."[23] More than fifty-six percent of adults in the United States own smartphones[24] and spend a considerable amount of time using their devices to interact with the digital world.[25]

Possessing considerably more power than the guidance computers that first put astronauts on the moon,[26] today's ordinary smartphones are capable of identifying their user's every movement within inches and reporting these

---

21. *See, e.g.*, Mark Ward, *The Future of the Silicon Chip*, BBC NEWS (Sept. 27, 2011), http://www.bbc.com/news/technology-14880363.

22. Stephanie Mlot, *Smartphone Adoption Rate Fastest in Tech History*, PCMAG (Aug. 27, 2012, 2:27 PM), http://www.pcmag.com/article2/0,2817,2408960,00.asp.

23. *Id.*

24. Aaron Smith, *Smartphone Ownership 2013*, PEW RES. CENTER (June 5, 2013), http://www.pewinternet.org/2013/06/05/smartphone-ownership-2013/.

25. *See, e.g.* Maeve Duggan & Aaron Smith, *Cell Internet Use 2013*, PEW RES. CENTER (Sept. 16, 2013), http://www.pewInternet.org/Reports/2013/Cell-Internet.aspx.

26. *See, e.g.* Shaun Clayton, *8 Famous Computers with a Pathetic Amount of Power*, TOPLESS ROBOT (May 30, 2012, 8:03 AM), http://www.toplessrobot.com/2012/05/8_famous_computers_with_a_pathetic_amount_of_power.php (comparing the iPhone 4 to the Apollo Guidance Computer).

movements to anyone or anything with an Internet connection.[27] Brick and mortar retailers can combine their stores' video surveillance with facial recognition technologies to analyze customers' expressions (and, if any of those customers have the retailer's app on their phone, connect their customer's digital interactions with their physical ones).[28] Other examples abound. Bracelets worn around consumers' wrists help their wearers track steps taken, calories burned, and other physical activities.[29] Today's cars integrate sophisticated sensing and processing technologies to detect looming dangers and take preventive actions before the "driver" is even aware of an issue.[30] Many also take advantage of persistent data connections to keep the car in contact with service providers at all times.[31]

B. Information-Based Monetization Strategies Are Powering Technological Growth

The rapid development of technology, fueled by information-based monetization strategies, fosters a tremendous amount of data collection, use, and sharing. Aptly described as a "revolution,"[32] companies are rapidly adopting "big data" technologies, which promise to yield lucrative insights by mining unimaginably large data sets for previously undiscovered connections.[33] Behind the scenes of consumers' digital interactions, "[d]ata companies [scoop] up enormous amounts of information about almost every American. They sell information about whether you're pregnant or divorced or trying to lose weight, about how rich you are and what kinds of cars you have."[34] Today's companies "maintain[] vast troves of transactional data,

---

27. *See* Liat Clark, *Finnish Startup Can Locate You Indoors Using Magnetic Field Anomalies*, WIRED UK (July 9, 2012), http://www.wired.co.uk/news/archive/2012-07/09/indoor-smartphone-compass-locater.

28. *See* Megan Garber, *I Know What You Did Last Errand*, THE ATLANTIC (July 15, 2013), http://www.theatlantic.com/technology/archive/2013/07/i-know-what-you-did-last-errand/277785/.

29. *See, e.g.*, Barry Levine, *Wearable Bands Are Booming. Better Get in Shape for All That Fitness Tracking*, VENTURE BEAT (Feb. 12, 2014, 10:02 AM), http://venturebeat.com/2014/02/12/wearable-bands-are-booming-better-get-in-shape-for-all-that-fitness-tracking/.

30. *See, e.g.*, Nick Palmero, *6 Affordable Vehicles with Collision Warning Systems*, AUTOTRADER, http://www.autotrader.com/research/article/best-cars/188920/6-affordable-vehicles-with-collision-warning-systems.jsp (last visited Mar. 3, 2014).

31. *See, e.g.*, Keith Barry, *Can Your Car Be Hacked?*, CAR & DRIVER (July 2011), http://www.caranddriver.com/features/can-your-car-be-hacked-feature.

32. *See* Steve Lohr, *The Age of Big Data*, N.Y. TIMES (Feb. 11, 2012), http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html.

33. "Big Data" is "shorthand for advancing trends in technology that open the door to a new approach to understanding the world and making decisions." *Id.*

34. Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PRO PUBLICA (June 13, 2014, 1:59 PM), http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.

much of which is 'data exhaust,' or data created as a by-product of other transactions."[35] Some data, however, including the information derived from mobile devices, is particularly valuable since it can be associated with specific individuals.[36] This allows recipients of the data to "paint a picture about the needs and behavior of individual users rather than simply the population as a whole."[37] It is this promise—the ability to obtain a complete picture of each consumer's life—that is powering the growth of the digital world's most promising firms.[38]

Monetization strategies centered on advertising are not particularly new, nor is the use of data to persuade specific audiences.[39] What *is* new is the ability to use data about specific consumers to persuade those consumers to take desired actions, cheaply and on a wide scale.[40] Companies such as Google and Facebook have built empires by selling access to specific consumers, and many other firms are following their lead.[41] By targeting advertisements to particular individuals, firms employing ad-based monetization strategies compete to gather and analyze consumer-specific data in the hopes of commanding higher rents from companies wishing to reach specific audiences at specific times and in specific contexts.[42]

Instead of selling direct access to consumers, countless other firms profit from advertising-based monetization strategies by offering background services and infrastructure that facilitates the sale, publication,

---

35. WORLD ECON. FORUM, BIG DATA, BIG IMPACT: NEW POSSIBILITIES FOR INTERNATIONAL DEVELOPMENT 3 (2012), *available at* http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf.

36. *Id.* at 3.

37. *Id.* at 2.

38. *See* Lohr, *supra* note 32.

39. Understanding one's customers, and knowing how to influence them, has been viewed as "critical to advertising wisely" at least since 1904. *See* Walter D. Scott, *The Psychology of Advertising*, THE ATLANTIC (Jan. 1904), *available at* http://www.theatlantic.com/magazine/archive/1904/01/the-psychology-of-advertising/303465/.

40. *See, e.g.*, Elizabeth Dwoskin, *What Secrets Your Phone Is Sharing About You*, Wall St. J. (Jan. 13, 2014, 8:47 PM), http://online.wsj.com/news/articles/SB10001424052702303453004579290632128929194?mod=WSJ_hps_LEFTTopStories.

41. *See, e.g.*, *All The Facts You Need to Know About Mobile Marketing*, AD AGE (Aug. 19, 2013), http://adage.com/article/digital/mobile-fact-pack-2013-ad-age-s-guide-mobile-marketing/243696/. *See also* Billy Steele, *Facebook's Mobile Ads Now Account for Over Half of Its Revenue Thanks to 945 Million Monthly Users*, Engadget.com (Jan. 29, 2014), http://www.engadget.com/2014/01/29/facebook-mobile-ad-revenue-q4-2013/; Natasha Lomas, *Mobile Ad Market Spending to Hit $18BN in 2014, Rising to ~$42BN by 2017, Says Gartner*, Techcrunch.com (Jan. 21, 2014), http://techcrunch.com/2014/01/21/mobile-ad-market-forecast-to-2017/.

42. *See, e.g.*, J. HOWARD BEALES & JEFFREY A. EISENACH, NAVIGANT ECONOMICS, AN EMPIRICAL ANALYSIS OF THE VALUE OF INFORMATION SHARING IN THE MARKET FOR ONLINE CONTENT 1 (2014), *available at* http://www.aboutads.info/resource/fullvalueinfostudy.pdf.

and performance tracking of digital ads.[43] Still other firms seek to make money by collecting and packaging consumer information for secondary uses, such as research and targeting.[44] For example, many states' hospital systems make patients' records for sale to the general public.[45] Over the past decade, the number of third parties receiving this data has more than doubled,[46] and it is estimated that the market for medical data will surpass $10 billion over the next six years.[47] While states take a variety of steps to anonymize the data, it is often easy to re-identify and few states require purchasers not to do so.[48]

C. Technology's Benefits

It is unquestionable that advances in technology, especially when paired with the collection, sharing, and use of consumer data, have and will continue to produce tremendous benefits. Today, a blind German person (who knows no English) and a deaf American person (who knows no German) can communicate with each other *almost* in real time, thanks to wearable technology like Google Glass.[49] Questions about self-driving cars have shifted from feasibility to timing (when will they be for sale?), participants (which companies will sell them, and to whom?) and liability (who is at fault in a collision?).[50] Perhaps most promising are the

---

43. *See, e.g.*, Terence Kawaja, *Marketing Technology LUMAscape*, SLIDE SHARE (May 8, 2013), http://www.slideshare.net/tkawaja/marketing-technology-lumascape (last visited Jan. 15, 2014) (graphically presenting the firms that participate in digital advertising by grouping specific firms by functionality).

44. OFFICE OF OVERSIGHT & INVESTIGATIONS, S. COMM. ON COMMERCE, SCI., & TRANSP., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 29 (2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577.

45. *See* Jordan Robertson, *States' Hospital Data for Sale Puts Privacy in Jeopardy*, BLOOMBERG (June 5, 2013), http://www.bloomberg.com/news/2013-06-05/states-hospital-data-for-sale-puts-privacy-in-jeopardy.html.

46. *See* Jordan Robertson, *As Health Records Go Digital, Where They End Up Might Surprise You*, BLOOMBERG (June 5, 2012, 8:27 PM), http://go.bloomberg.com/tech-blog/2012-06-05-as-health-records-go-digital-where-they-end-up-might-surprise-you/.

47. *See* James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, MCKINSEY & COMPANY (May 2011), http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

48. *See* Robertson, *supra* note 45.

49. *See* Vint Cerf, Google, Remarks at FTC Workshop: Internet of Things - Privacy & Security in a Connected World 125-27 (Nov. 19, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.

50. *See, e.g.*, Doron Levin, *Just How Close to Commercial Reality Is a Self-Driving Car?*, FORTUNE (Jan. 10, 2014, 7:54 PM), http://features.blogs.fortune.cnn.com/2014/01/10/self-driving-car-google/.

opportunities in healthcare, where technology and data may be employed to reduce the costs of care and increase the quality of treatment.[51]

From an economist's perspective, the sharing of consumer information can reduce search costs, improving economic efficiency.[52] Indeed, consumers may "suffer privacy costs when too *little* personal information about them is being shared with third parties, rather than too much."[53] For example, buyers need to know where they can purchase which goods and at what prices, and sellers need to know which products to carry. Revealing buyers' tastes (without revealing buyers' maximum price) increases welfare for both sides, leaving everyone better off.[54]

D. Technology's Privacy Dilemmas

For all its benefits, changing technology also presents complex and evolving privacy dilemmas. For example, consumers struggle to understand the flow of their personal information when visiting websites on a desktop computer, let alone how they can take steps to control that flow.[55] These difficulties are exacerbated by smartphones, and "will be exponentially greater with the advent of the Internet of things, as the boundaries between the virtual and the physical worlds disappear."[56] From firms' tendency to change their information collection, use, and sharing practices over time in ways that undermine consumer privacy, to firms' use of "legalese" in key disclosures to maintain an illusion of transparency while obfuscating important information,[57] technology's march forward makes it very difficult to strike the right balance.

---

51. *See, e.g.*, Elaine Grant, *The Promise of Big Data*, HARV. PUB. HEALTH, Spring/Summer 2012, at 15 ("Petabytes of raw information could provide clues for everything from preventing TB to shrinking healthcare costs."), *available at* http://www.hsph.harvard.edu/news/magazine/spr12-big-data-tb-health-costs/.

52. *See* Hal R. Varian, *Economic Aspects of Personal Privacy* (U.C. Berkeley, 1996), *available at* http://people.ischool.berkeley.edu/~hal/Papers/privacy/.

53. Alessandro Acquisti, *The Economics of Personal Data and the Economics of Privacy* 4 (Org. for Econ. Co-operation & Dev., 2010), *available at* http://www.oecd.org/sti/ieconomy/46968784.pdf. (summarizing Varian, *supra* note 52).

54. *See* Varian, *supra* note 52.

55. *See, e.g.*, Edith Ramirez, FTC, Remarks at FTC Workshop: Internet of Things - Privacy & Security in a Connected World 10 (Nov. 19, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.

56. *Id.* at 10–11.

57. *See, e.g.*, Josh Constine, *Tech Companies, You're Killing Yourself with Scary Legalese. Put Policy Changes in Layman's Terms*, TECHCRUNCH (Dec. 18, 2012), http://techcrunch.com/2012/12/18/you-always-fear-what-you-dont-understand/ (calling on technology companies to "wise up and end the cycle of pushing policy updates, watching press and users alike panic and threaten to jump ship, and then issu[e] an apology and clarification").

1. Privacy's "Ratchet" and "Shrouding" Problems

In the midst of today's technological development, it seems as if consumers' ability to express preferences or exercise control over their information is only diminishing. The term "ratchet" is traditionally used to describe mechanisms which allow "effective motion in one direction only,"[58] and it provides a useful schema for understanding firms' tendency to undermine consumer privacy over time. Perhaps the most illustrative example of this behavior is that provided by Google's email service, Gmail.[59]

When Google's flagship email product launched in 2004, many were concerned about Google's plans "to scan the contents of [users'] email messages in order to display advertisements relevant to [users'] online conversations."[60] Of particular concern was the possibility that "users of Gmail, who must give Google their names to sign up, may have their names correlated with the search terms they type in when searching. This can be done through cookies and IP addresses."[61] Responding to such concerns, Google's Vice President of Engineering assured consumers that Google had "very strict policies" and did "not associate search clicks with a user's name or anything like that."[62] Eight years later, however, Google announced that it would begin "follow[ing] the activities of users across nearly all of its ubiquitous sites, including YouTube, Gmail, and its leading search engine."[63] As Google's Director of Privacy for Product and Engineering specifically told users:

> If you're signed in, we may combine information you've provided from one service with information from other services . . . . In short, we'll treat you as a single user across all our products, which will mean a simpler, more intuitive Google experience.[64]

---

58. *Ratchet Definition*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/ratchet (last visited Jan. 31, 2014).

59. Google is not the only Internet company contributing to privacy's "ratchet" problem. *See, e.g.*, Constine, *supra* note 57 ("Facebook has been through this ringer more times than anyone.").

60. Donna Wentworth, *Gmail: What's the Deal?*, ELECTRONIC FRONTIER FOUND. (Apr. 5, 2004), https://www.eff.org/deeplinks/2004/04/Gmail-whats-deal.

61. Janis Mara, *Google Responds to Gmail Privacy Concerns*, ClickZ (Apr. 2, 2004), http://www.clickz.com/clickz/news/1702090/google-responds-gmail-privacy-concerns (quoting Pam Dixon).

62. *Id.* (quoting Wayne Rosing).

63. Cecilia Kang, *Google Tracks Consumers' Online Activities Across Products, and Users Can't Opt Out*, WASH. POST (Jan. 24, 2012), http://articles.washingtonpost.com/2012-01-24/business/35440035_1_google-web-sites-privacy-policies.

64. *Id.* (quoting Alma Whitten, Google's Director of Privacy for Product and Engineering).

Thus, despite previously making express assurances that it would not connect Gmail users' accounts with their search queries, Google decided to do just that.

In addition to privacy's "ratchet," companies often obscure, or "shroud," their privacy practices. Consumers struggle to even identify the rights that companies reserve for themselves through their terms of use documents and privacy policies[65] (to the extent privacy policies are even available),[66] let alone to discern companies' actual data practices.[67] When Instagram—a popular photo-sharing service—announced that it was updating its terms of service to include language that many perceived as hostile to user rights, it faced "a major backlash from users" and quickly reverted to its old language.[68] The new terms provided that users "hereby agree that Instagram may place such advertising and promotions on the Service or on, about, or in conjunction with your Content."[69] Instagram users were outraged by the change, as it "would let advertisers pick and choose among user-posted photos for ads."[70] However, under the old terms, users had already granted

> Instagram a non-exclusive, fully paid and royalty-free, worldwide, limited license to use, modify, delete from, add to, publicly perform, publicly display, reproduce and translate such Content, including without limitation distributing part or all of

---

65. "The current privacy framework in the United States is based on companies' privacy practices and consumers' choices regarding how their information is used. In reality, we have learned that many consumers do not read, let alone understand such notices, limiting their ability to make informed choices." Comments of the FTC at 5, *Information Privacy and Innovation in the Internet Economy*, NTIA Docket No. 100402174-0175-01 (July 2, 2010) [hereinafter FTC Comments], *available at* https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-comment-department-commerce-national-telecommunications-and-information-administration/100623ntiacomments.pdf.

66. *See* FTC, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE 6 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf (surveying the practices of kids apps, and finding that "only 20% of the [400] apps reviewed disclosed any information about the app's privacy practices").

67. FTC Comments, *supra* note 65, at 6 (noting that "consumers generally do not understand data collection practices and are largely unaware that there may be companies collecting and analyzing their data for use by other companies").

68. Tomio Geron, *After Backlash, Instagram Changes Back to Original Terms of Service*, FORBES (Dec. 20, 2012, 7:39 PM), http://www.forbes.com/sites/tomiogeron/2012/12/20/after-backlash-instagram-changes-back-to-original-terms-of-service/.

69. INSTAGRAM, http://instagram.com/about/legal/terms/# (Policy effective as of Jan. 19, 2013).

70. Helen A.S. Popkin, *Instagram Responds to Outrage, Tweaks Privacy Policy to Limit Photo Use in Ads*, NBC NEWS (Dec. 18, 2012, 5:05 PM), https://web.archive.org/web/20131225031831/http://www.nbcnews.com/technology/instagram-responds-outrage-tweaks-privacy-policy-limit-photo-use-ads-1C7660196.

> the Site in any media formats through any media channels, except Content not shared publicly ("private") will not be distributed outside the Instagram Services.[71]

As Instagram noted in its blog post announcing the changes, "[n]othing has changed about [users'] photos' ownership or who can see them."[72] Thus, users were essentially outraged over cleaner language—not a change in Instagram's substantive rights under its terms of service or privacy policies.

2. Privacy Dilemmas Evolve with Changes in Technology

Grappling with dilemmas like privacy's "ratchet" and "shrouding" problems is further complicated by the evolving consumer technology landscape. Ushering in a major wave of change sweeping through the world today is the smartphone—a very personal computer that exacerbates many of the existing challenges to safeguarding consumer privacy. In addition to their high rates of adoption and use, these portable computers make it possible for anyone or anything with an Internet connection to collect a significant amount of consumer data while simultaneously introducing new hurdles for the regulatory environment.

Unlike laptop or desktop computers, "mobile devices are typically personal to an individual, almost always on, and with the user."[73] These "always on" and "always with the user" traits, combined with smartphones' ability to sense and analyze their environment, introduce new twists on existing problems. For example, the software that runs on these portable computers "can capture a broad range of user information from the device automatically—including the user's precise geolocation, phone number, list of contacts, call logs, unique device identifiers, and other information stored on the device—and can share this data with a large number of possible recipients."[74]

Unlike the world of traditional personal computers, where the overwhelming majority of consumers connect to the Internet through a web browser, smartphone users interact with the world through a host of non-

---

71. INSTAGRAM, http://instagram.com/about/legal/terms/before-january-19-2013/# (Policy before Jan. 19, 2013).

72. *Privacy and Terms of Service Changes on Instagram*, INSTAGRAM (Dec. 2012), http://blog.instagram.com/post/38143346554/privacy-and-terms-of-service-changes-on-instagram (last visited Jan. 15, 2014).

73. FTC, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 2 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

74. FTC, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING 1 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf.

browser applications. "[T]en years ago, the term 'app' had not entered common parlance; today, there are over 800,000 available in the Apple App Store and 700,000 on Google Play."[75] Oftentimes, smartphone users may not even realize that they are interacting with the online world or that the software they are using is collecting and reporting their private information.[76] Indeed, most consumers do not "realize how much data they implicitly give away, how that data might be used or even what is known about them."[77] And this is not a problem restricted to technology's novices—even experts in human computer interaction focused specifically on mobile privacy have acknowledged their own troubles with understanding information flows.[78]

As rapidly as smartphones have displaced the world of traditional computing, tomorrow's "Internet of Things" promises to arrive even quicker, posing even greater privacy questions. Already, many consumer product companies have begun making everyday objects "smart" by endowing them with "the ability to connect and transmit data through the use of embedded devices or sensors that connect with networks."[79] These smart "things" presently range "from household appliances to sophisticated business tools" and promise benefits like "greater efficiency, lower costs, improved services, [and] more accurate supply chain management."[80] However, they also raise privacy concerns that "could have widespread effects not only on business operations, but . . . on consumer trust and corporate reputation."[81] For example, the groceries one purchases and consumes may be logged and reported to health insurance companies. Car manufacturers could observe drivers' habits and tendencies, reporting law breakers to the police.[82] Employers could take productivity tracking to a whole new level, and meaningless correlations might be mistaken for significant causal relationships. If privacy safeguards are to keep pace with technology, they must be capable of reaching the complex privacy dilemmas raised by evolving technologies.

---

75. FTC, *supra* note 73, at 2.

76. Claire Cain Miller & Somini Sengupta, *Selling Secrets of Phone Users to Advertisers*, N.Y. TIMES (Oct. 5, 2013), http://www.nytimes.com/2013/10/06/technology/selling-secrets-of-phone-users-to-advertisers.html?_r=0.

77. WORLD ECON. FORUM, PERSONAL DATA: THE EMERGENCE OF A NEW ASSET CLASS 17 (2011), *available at* http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

78. *See* Miller & Sengupta, *supra* note 76.

79. ISACA, THE INTERNET OF THINGS: RISKS AND REWARDS OF THE INTERNET OF THINGS (2013), *available at* http://www.isaca.org/SiteCollectionDocuments/2013-Risk-Reward-Survey/2013-Global-Survey-Report.pdf.

80. *Id.* at 2.

81. *Id.* at 3.

82. *See, e.g.*, Jim Edwards, *Ford Exec: 'We Know Everyone Who Breaks the Law' Thanks to Our GPS in Your Car*, BUSINESS INSIDER (Jan. 8, 2014, 8:16 PM), http://www.businessinsider.com/ford-exec-gps-2014-1.

III. THE UNITED STATES' REGULATORY REGIME HAS NOT KEPT PACE WITH TECHNOLOGY

In the United States, there is no one law, or set of laws, specifically responsible for policing the data conduct of today's merchants, service providers, or other consumer-facing firms.[83] Nor is there a single entity tasked with across-the-board privacy enforcement.[84] While entities collect, share, analyze, and use massive amounts of consumer data for creativity-is-the-only-limit purposes, the job of ensuring that such practices strike an optimal balance is left to "a hodgepodge of various constitutional protections, federal and state statutes, common law tort, regulatory rules, and treaties."[85] Instead of a comprehensive, omnibus approach to dealing with technology's privacy dilemmas, the United States relies heavily upon the Federal Trade Commission to use its authority under section 5 of the FTC Act to challenge "unfair" or "deceptive" business acts or practices in order to "regulate" consumer privacy's competing interests.[86] While the FTC has played a role in privacy regulation since the dawn of the digital era, the extent to which the United States has relied on the FTC has increased over time. This section explores the United States' attempts to safeguard consumer privacy as digital and Internet technologies have emerged. From its use of the Fair Credit Reporting Act (FCRA)[87] and Fair Information Practice Principles in the pre-Internet digital age, to reliance on contract, self-regulation, and FTC enforcement in the Internet age, the United States has struggled to create a regulatory framework capable of keeping pace with changing technologies.[88]

A. The United States' Initial Approach to Consumer Privacy in the Digital Era

As early as 1969—nearly 80 years after Samuel Warren and Louis Brandeis called for action to protect one's "right to be let alone"[89]—a critical report demanded the Federal Trade Commission use its authority to address "[t]he information explosion, including increasing use of mass data-handling

---

83. Solove & Hartzog, *supra* note 6, at 587–88.

84. *See, e.g.*, Paul M. Schwartz, *Privacy and Preemption*, 118 Yale L.J. 902, 902 (2009) (arguing that "it would be a mistake for the United States to enact a comprehensive or omnibus federal privacy law for the private sector").

85. Solove & Hartzog, *supra* note 6, at 587.

86. *See id.* at 588-89.

87. 15 U.S.C. § 1681 (2012).

88. *See* The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (noting that the existing regulatory framework lacks the ability to address "consumer data privacy issues as they arise from technologies and business models").

89. Warren & Brandeis, *supra* note 1, at 196.

techniques to attack the privacy and autonomy of the consumer"—a "trend [that] has made possible social-psychological analysis of potential markets."[90] Shortly thereafter, the FTC began enforcing the FCRA[91]—then a recently enacted statute "govern[ing] the collection, assembly, and use of consumer report information" and "provid[ing] the framework for the credit reporting system in the United States."[92] While the FCRA has been amended over time, as originally enacted it "imposed requirements exclusively on [Credit Reporting Agencies] such as credit bureaus, except for those sections of the Act requiring users of consumer reports and other third parties to provide certain notices to consumers."[93] To address privacy problems outside the scope of the FCRA, the United States relied on industry adherence to "Fair Information Practice Principles."[94] Created through a series of "reports, guidelines, and model codes" issued by "government agencies in the United States, Canada, and Europe," the Fair Information Practice Principles "embody the important underlying concepts of transparency, consumer autonomy, and accountability."[95]

As the Internet emerged, augmenting the power of digital technologies to undermine consumer privacy, actors in the United States initially looked to tort and contract law for solutions. "Attempts to use the privacy torts to address problems with data collection and use ended in failure," but it appeared for a while as if contract law would play a significant role in privacy regulation thanks to the rapid emergence of privacy notices.[96] Partly to build goodwill, and partly to stave off formal regulation, many companies operating on the Internet began to post privacy notices, describing the companies' information practices.[97] Though the effort succeeded in preventing formal regulation,[98] it did not succeed in establishing contract law as the principle framework for safeguarding consumer privacy—"mainly because plaintiffs were not able to establish damages."[99] This suggests that

90. EDWARD F. COX ET AL., THE NADER REPORT ON THE FEDERAL TRADE COMMISSION 18 (1969).

91. 15 U.S.C. § 1681 (2012).

92. FTC, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT 1 (2011), *available at* https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf.

93. *Id.* at 1–2.

94. FTC, *supra* note 11, at 6–7.

95. *Id.* at 6–7.

96. Solove & Hartzog, *supra* note 6, at 590–97.

97. *Id.* at 593–94.

98. While Congress did enact a few sector-specific laws during this time frame, industry's self-regulatory efforts prevented the passage of comprehensive or omnibus federal privacy laws. *See id.* at 594.

99. *See id.* at 595–96 for a more detailed historical perspective. Though beyond the scope of this Note, given the numerous changes in technology and business models that have since come to fruition, perhaps private parties could adopt the framing advocated here in order to re-animate the contract-based approach.

practical limitations, as opposed to conceptual ones, have so-far prevented contract-based approaches from succeeding.

B. The Inadequacy of Existing Mechanisms Prompted the FTC to Step In

Originally established in 1914 to protect against "unfair methods of competition," the FTC's authority was expanded in 1938 to reach "unfair or deceptive acts or practices."[100] This authority—found in section 5 of the FTC Act[101]—is quite flexible and serves as the backbone of the agency's consumer protection role. Indeed, "Congress deliberately delegated broad power to the FTC under section 5 of the FTC Act to address unanticipated practices in a changing economy."[102] This flexibility has enabled the FTC to address consumer problems despite evolving markets and technologies.[103]

Taking advantage of this flexibility, the FTC extended Section 5 into the virtual world in 1994 when it brought its first Internet case, alleging that certain advertisements for credit repair kits sold through American Online were deceptive.[104] Shortly thereafter, at the behest of Congress, the FTC turned some if its attention to exploring Internet-related consumer privacy issues.[105] Since then, the FTC has employed three different frameworks (each designed to remedy the gaps of the prior approach), called for baseline privacy legislation to bolster its authority, and significantly ramped up the attention and resources that it devotes to safeguarding consumer privacy.

The FTC's first attempt to grapple with consumer privacy in the Internet era centered on a "notice and choice" framework that emphasized transparency. Under this framework, the FTC "encourage[ed] companies to develop privacy notices describing their information collection and use practices to consumers, so that consumers can make informed choices."[106] Because the FTC currently has no power to compel entities to make disclosures,[107] this approach relied more on policy efforts—such as public workshops, studies regarding website practices and disclosures, and

---

100. *See, e.g.*, FTC, 90TH ANNIVERSARY SYMPOSIUM PROGRAM 6-8 (2004), *available at* https://www.ftc.gov/sites/default/files/attachments/ftc-90-symposium/90thanniv_program.pdf.

101. Federal Trade Commission Act of 1914, ch. 311, § 5, 38 Stat. 719 (codified as amended at 15 U.S.C. § 45 (2012)).

102. Brief for FTC at 11, FTC v. Wyndham Worldwide Corp., Civil Action No. 2:13-CV-01887-ES-SCM (D.N.J. May 20, 2013) (citing FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 240 (1972)), *available at* https://www.manatt.com/uploadedFiles/Content/4_News_and_Events/Newsletters/AdvertisingLaw@manatt/FTC-v.-Wyndham.pdf.

103. *Id.* (summarizing historical use of § 5 to reach new issues).

104. Complaint of FTC, FTC v. Corzine, Case No. CIV-S-94-1446 (E.D. Cal. Sept. 12, 1994).

105. Solove & Hartzog, *supra* note 6, at 598–99.

106. FTC, *supra* note 11 at iii (internal citations omitted).

107. *See* Solove & Hartzog, *supra* note 6, at 599.

comments related to industry self-regulatory efforts—than it did on law enforcement.[108] Indeed, the FTC did not bring its first Internet *privacy* enforcement action until August 1998—three years after Congress requested the FTC get involved.[109] In addition to enforcement problems, and despite the model's emphasis on transparency, the notice and choice framework led to the creation of "long, incomprehensible privacy policies that consumers typically do not read, let alone understand."[110]

To address the shortcomings of its "notice and choice" approach, the FTC adopted a second framework focused on consumer harm. Specifically, the "harm-based" model sought to protect consumers from three types of injuries: physical harm; financial harm; and unwarranted intrusions into consumers' daily lives.[111] While this second framework enabled the agency to bring a number of enforcement actions,[112] its conception of harm was too narrow to reach all of privacy's myriad and evolving dilemmas:

> Just as a burn is an injury caused by heat, so is privacy harm a unique injury with specific boundaries and characteristics . . . . The subjective category of privacy harm is the perception of unwanted observation . . . . The objective category of privacy harm is the unanticipated or coerced use of information concerning a person against that person. These are negative, external actions justified by reference to personal information.[113]

Despite the various manifestations of privacy's problems, one must show harm that is "'cognizable,' 'actual,' 'specific,' 'material,' 'fundamental,' or 'special' before a court will consider awarding compensation."[114] These specific and narrow requirements ensured that the harm-based model—like the notice and choice approach—also depended on strong self-regulation in order to reach the problems beyond its scope.

---

108. FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 3 (2000), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

109. *See* GeoCities, *Decision and Order*, FTC No. 982 3015, Docket No. C-3849 (1999), *available at* https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015.do_.htm.

110. FTC, *supra* note 11, at iii (citations omitted).

111. *See id.*; *see also* Timothy J. Muris, Chairman, FTC, Protecting Consumers' Privacy: 2002 and Beyond, Remarks at The Privacy 2001 Conference (Oct. 4, 2001), *available at* https://www.ftc.gov/public-statements/2001/10/protecting-consumers-privacy-2002-and-beyond.

112. *See, e.g.*, Solove & Hartzog, *supra* note 6, at 627–48.

113. M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1131 (2011).

114. *Id.*at 1132 (internal citations omitted).

As the FTC has acknowledged, both the notice and choice and the harm-based frameworks "struggled to keep pace with the rapid growth of technologies and business models that enable companies to collect and use consumers' information in ways that are often invisible to consumers."[115] Because these two approaches were not sufficiently comprehensive to cover technology's evolving privacy dilemmas, and because industry self-regulatory efforts failed to close the gaps, the FTC set out to create a new privacy framework in 2010.[116]

The FTC began its quest by convening a series of public workshops composed of industry participants, academics, technologists, privacy experts, consumer advocates, and regulators.[117] After spending a year examining its privacy jurisprudence through these workshops, the FTC compiled and released a preliminary proposal for public comment.[118] Receiving more than 450 submissions, the agency revised its proposal and released its final report in March 2012.[119]

In order to contend with the challenges identified during the FTC's two-years-long re-think, and avoid stifling innovation, the FTC's new privacy framework centers on three core concepts—privacy by design, simplified choice, and transparency—along with a request for Congress to consider bolstering the agency's authority through additional legislation.[120] Specifically, the agency called for companies to "[b]uild in privacy at every stage of product development" and to "[g]ive consumers the ability to make decisions about their data at a relevant time and context . . . while reducing the burden on businesses of providing unnecessary choices."[121] The FTC also called on companies to "[m]ake information collection and use practices transparent," and asked Congress to consider enacting "flexible" and "technology neutral" privacy legislation that "provide[s] clear standards and appropriate incentives to ensure basic privacy protections across all industry sectors."[122]

IV. THE UNITED STATES SHOULD RECOGNIZE DIGITAL INTERACTIONS AS THE COMMERCIAL EXCHANGES OF VALUE THAT THEY ARE

It has been two years since the FTC released the final version of its new privacy framework. Industry self-regulatory efforts appear to be going

115. FTC, *supra* note 11, at iii (internal citations omitted).
116. *See, e.g.*, FTC, *supra* note 17, at i-v.
117. FTC, *supra* note 11, at iii–iv.
118. *Id.*
119. FTC, *supra* note 17, at i.
120. *Id.*
121. *Id.*
122. *Id.* at i, 12, 13.

nowhere,[123] Congress has taken no steps toward enacting baseline privacy legislation to bolster the FTC's enforcement work,[124] and the FTC's authority to act in the consumer privacy space is being challenged in the courts by defendants in two different enforcement actions.[125] While the FTC has been far from stagnant on the privacy front, its new framework does not appear to have moved the needle. If the United States' regulatory regime for consumer privacy is to keep up with today's emerging technologies, something needs to change.

A Google search for the phrase "data is the new oil" yields more than 700,000 results.[126] The expression "has achieved the status of an approved corporate cliché,"[127] and it has spurred a number of creative articles, but it has not been taken seriously by those studying or safeguarding the consumer privacy environment. This Note takes the expression seriously, arguing that such a framing fits neatly within the FTC's mandate, jurisdiction, and authority and could be employed to substantiate the FTC's new privacy framework—producing a flexible solution to complex and evolving consumer privacy dilemmas.

A. Digital Interactions Can Be Framed As Commercial Exchanges of Value

Article II of the Uniform Commercial Code,[128] though it only applies to sales of goods (expressly excluding sales of "information" from its scope),[129] provides a widely-adopted and useful framework for understanding what it means to have a commercial exchange of value.[130] "Sales" are defined as "the passing of title from the seller to the buyer for a

123. *See, e.g.*, Angelique Carson, *Did NTIA's Multi-Stakeholder Process Work? Depends on Whom You Ask.*, THE PRIVACY ADVISOR (Sept. 3, 2013), https://www.privacyassociation.org/publications/did_ntias_multi_stakeholder_process_work_depends_whom_you_ask.

124. *See, e.g.*, Allison Grande, *Groups Push Obama to Float 'Privacy Bill of Rights'*, LAW360 (Feb. 24, 2014, 4:30 PM), http://www.law360.com/technology/articles/512544/groups-push-obama-to-float-privacy-bill-of-rights-.

125. *See* FTC v. Wyndham Worldwide Corp., No. 12-1365 (D. Ariz. 2012); LabMD, Inc., FTC No. 102 3099, Docket No. 9357 (May 26, 2015).

126. Google.com search, executed Jan. 15, 2014.

127. Naughton, *supra* note 20.

128. The Uniform Commercial Code is a comprehensive model code written by experts in commercial law and approved by the National Conference on Commissioners on Uniform State Laws, who recommend that states adopt its provisions. Unless enacted by state legislature, the Code itself does not have legal effect. *See* Uniform Commercial Code Research Guide, DUKE LAW (May 2013), https://law.duke.edu/lib/researchguides/ucc/.

129. U.C.C. § 2-102 (2013); *see also id.* at § 2-103(1)(k) ("'Goods' means all things that are movable at the time of identification to a contract for sale . . . the term does not include information . . . . ").

130. Every state except for Louisiana has adopted some version of Article II of the UCC.

price," [131] where "price may be payable in money, goods, realty, or otherwise."[132] Thus, in the UCC's flexible framework, one party exchanges something of value (goods) for something else of value ("money, goods, realty, or otherwise").[133]

In the digital space, consumers' interactions *can* be viewed as commercial exchanges of value. When consumers execute Google searches, sign up for Facebook accounts, or download and use apps on their smart devices, they offer something in exchange for the digital provider's services.[134] Instead of dollars, consumers pay for their digital services with data and attention.[135] Thus, even where no money passes from a consumer to a service provider, value is exchanged and privacy questions become pricing questions—e.g., how much access and information does a consumer give up in exchange for which services?

Framing digital interactions as commercial exchanges of value is not a distorted way of viewing consumer-business interactions. Ginni Rometty, IBM's chief executive officer, made headlines last year when she encouraged business leaders and lawmakers to "think about data as the next natural resource:"[136]

> Just like oil was a natural resource powering the last industrial revolution, data is going to be the natural resource for this industrial revolution. Data is the core asset, and the core lubricant, for not just the entire economic models built around every single industry vertical but also the socioeconomic models.[137]

And IBM is not the only multi-national entity subscribing to such a view. The World Economic Forum—an independent, international organization—famous for its annual meeting in Davos to address the global

131. U.C.C. § 2-106(1).
132. U.C.C. § 2-304(1).
133. *Id.*
134. *See, e.g.*, Kirsten Martin, *Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online*, FIRST MONDAY, December 2013, at 3, *available at* http://firstmonday.org/ojs/index.php/fm/article/view/4838/3802.
135. *Id.*
136. Maria Deutscher, *IBM's CEO Says Big Data is Like Oil, Enterprises Need Help Extracting the Value*, SILICON ANGLE (Mar. 11, 2013), http://siliconangle.com/blog/2013/03/11/ibms-ceo-says-big-data-is-like-oil-enterprises-need-help-extracting-the-value/.
137. *Id.*

implications of technological change[138]—has already "declared data a new class of economic asset, like currency or gold."[139]

Such a framing has also begun appearing in academic contexts in the United States. In a recent article, James C. Cooper, the Director of Research and Policy at George Mason University School of Law's Law & Economics Center, noted that "in some regard, nothing is free online—we pay by revealing data that provides a picture of our likes and dislikes . . . [a]s the already-tired cliché goes, 'Data is the new currency.'" [140] Going further, Capital University Law School Professor Dennis Hirsch has suggested that policymakers look to environmental law's method for curbing oil pollution as a way to "reap big data's many benefits while reducing its negative impacts." [141] Going the furthest, scholars Chris Hoofnagle and Jan Whittington have applied transaction cost analysis to consumers' digital interactions, concluding that "information-intensive companies misuse 'free' to promote products and services that are packed with non-pecuniary costs" like consumers' personal information and attention.[142]

The "data-as-oil" framing has even begun appearing, at least implicitly, in comments and speeches made by FTC leadership. While announcing a recent settlement with an app developer for the deceptive collection of users' geolocation information, the director of the FTC's Bureau of Consumer Protection stated that "[w]hen consumers are given a real, informed choice, they can decide for themselves whether the benefit of a service is worth the information they must share to use it." [143] More explicitly, when FTC Commissioner Julie Brill called for technologists to think critically about solutions to complicated and evolving privacy dilemmas, she acknowledged that "[i]n a real sense, we are becoming the

---

138. *See, e.g.*, WORLD ECON. FORUM, WORLD ECONOMIC FORUM INSTITUTIONAL BROCHURE (2012), *available at* http://www3.weforum.org/docs/WEF_InstitutionalBrochure.pdf.

139. Lohr, *supra* note 32; *see also* WORLD ECON. FORUM, *supra* note 77, at 23 (noting that, "[w]hile direct personal data has an inherent value, secondary inferred data can often be mined and interpreted to produce new information of equal or greater value").

140. James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129, 1130–31 (2013) (internal citations omitted).

141. Dennis Hirsch, *The Glass House Effect: Why Big Data is the New Oil, and What to Do About It* 1-2 (Future of Privacy Forum, 2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/Hirsch-Glass-House-Effect1.pdf (paper submitted in advance of the Future of Privacy Forum and the Stanford Center for Internet & Society's "Big Data and Privacy: Making Ends Meet" workshop).

142. Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 609 (2014).

143. Associated Press, *FTC: Flashlight App Left Consumer in the Dark*, USA TODAY (Dec. 6, 2013, 10:35 AM), http://www.usatoday.com/story/tech/2013/12/06/ftc-flashlight-app/3889949/.

sum of our digital parts . . . [a]nd that rich vein of data is exactly the gold that data miners want to extract."[144]

Finally, even critics of the FTC's approach to privacy regulation have suggested framing digital interactions as commercial exchanges of value. When the agency was working to develop its new privacy framework, Adam Thierer, a senior research fellow at George Mason University's Mercatus Center, specifically encouraged the FTC to consider the "value exchange" behind consumers' digital interactions instead of pursuing a "top-down regulatory regime that seeks to micromanage the consent process."[145] Suggesting that "[o]nline advertisers and service providers could make th[e] value proposition/trade-off more explicit by putting a theoretical price tag on their content or services," Thierer went on to note that "a more open and experimental model of 'information as currency' and 'privacy bargaining' will ultimately better serve consumers and online content/service providers since it treats consent as context-sensitive matter and encourages beneficial experimentation and an ongoing learning process."[146]

B. Recognizing Digital Interactions as Commercial Exchanges of Value Synchronizes Well with the FTC's Mandate, Jurisdiction, and Authority

The FTC has no general powers in the privacy realm that authorize it to promulgate rules, levy fines, or ban specific conduct. While it enforces a handful of specific privacy-related regulations—the Fair Credit Reporting Act,[147] the Gramm-Leach-Bliley Act,[148] the Children's Online Privacy Protection Act[149]—along with the US-EU Safe Harbor Agreement,[150] the bulk of the FTC's authority used to safeguard consumer privacy flows from

144. Julie Brill, Comm'r, FTC, Lecture at Polytechnic Institute of NYU: A Call to Arms: The Role of Technologists in Protecting Privacy in the Age of Big Data, (Oct. 23, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/call-arms-role-technologists-protecting-privacy-age-big-data/131023nyupolysloanlecture.pdf.

145. Adam Thierer, Public Interest Comment on Federal Trade Commission Report, *Protecting Consumer Privacy in an Era or Rapid Change* (Feb. 18, 2011), http://www.ftc.gov/sites/default/files/documents/public_comments/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework/00320-57670.pdf, at 4-5.

146. *Id.* at 4-5.

147. Fair Credit Reporting Act §604(c), Pub. L. No. 91-508, 84 Stat. 1114-2 (1970) (codified as amended at 15 U.S.C. § 1681 (2012)).

148. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. § 6803 (2012)).

149. Children's Online Privacy Protection Act, Pub. L. No. 105-277, 112 Stat. 2681-728 (1998) (codified at 15 U.S.C. §§ 6501–06 (2012)).

150. *Welcome to the U.S.-EU Safe Harbor*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018365.asp (last visited Jan. 24 2014); *see also* Solove & Hartzog, *supra* note 6, at 603-04 (summarizing the FTC's authority to enforce the US-EU Safe Harbor Agreement).

its Section 5 enforcement power.[151] In section 5 of the FTC Act, Congress provided that "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful,"[152] and charged the FTC with ensuring that all but a few excepted for-profit commercial entities operating in the United States adhere to the law.[153] Congress chose to confer such broad enforcement powers on the FTC because it wanted the agency to be sufficiently equipped to safeguard consumers from developments in commercial practice that could not be fully anticipated in advance.[154]

Under Section 5, in order to establish that a practice is "deceptive," the FTC must show that "a representation, omission, or practice . . . is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[155] Likewise, in order to establish an "unfairness" claim, the FTC must show that "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[156] Thus, establishing that an act or practice is deceptive or unfair ultimately requires the FTC to prove that a misrepresentation was "material" to consumers or that an act caused consumer injury not offset by countervailing benefits, which is difficult to do in the realm of consumer privacy.

A number of factors complicate the FTC's ability to use Section 5 to safeguard consumer privacy. Firms are presently believed to have no regulatory obligation to provide privacy policies or otherwise explain their data practices to consumers.[157] Where companies provide privacy policies, the policies tend to be long[158] and written at reading levels requiring more

---

151. *See, e.g.*, Solove & Hartzog, *supra* note 6, at 599.

152. Federal Trade Commission Act of 1914, ch. 311, § 5(a)(1), 38 Stat. 719 (codified as amended at 15 U.S.C. § 45(a)(1) (2012)).

153. *See* 15 U.S.C. § 45(a)(2) (2012) (empowering the FTC to prevent "persons, partnerships, or corporations" from using "unfair or deceptive acts or practices in or affecting commerce," but exempting banks, credit unions, and common carriers from the FTC's jurisdiction).

154. FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 240 (1972) (noting that "Congress . . . explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' by tying the concept of unfairness to a common-law or statutory standard or by enumerating the particular practices to which it was intended to apply").

155. FTC Policy Statement on Deception, appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

156. 15 U.S.C. § 45(n) (2012) ("In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence" but "[s]uch public policy considerations may not serve as a primary basis for such determination"); *see also* FTC Policy Statement on Unfairness, appended to Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

157. *See* FTC, *supra* note 11.

158. One oft-cited study estimated the opportunity cost of reading privacy policies to be $781 billion. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP 543, 564 (2008).

than a high school diploma,[159] often using "vague and innocuous sounding terms to mask third-party information sharing."[160] And most consumers, including the current Chief Justice of the United States, do not read them.[161] Additionally, to show unfairness in the privacy realm, the FTC must connect a privacy issue to financial or physical injury.[162]

Considering these limitations, the FTC has been remarkably effective at using Section 5 to safeguard consumer privacy. Since 1997, it has levied over 170 privacy-related complaints, significantly ramping up its enforcement agenda as Internet-enabled technologies have transformed consumers' daily lives.[163] These efforts have enabled the agency to secure orders committing some of the largest technology companies to privacy audits for the near future and subjecting them to civil penalties for subsequent privacy-related missteps.[164] However, the FTC's privacy-related enforcement work has only produced one privacy-related judicial opinion,[165] and two different FTC defendants are presently challenging the agency's privacy jurisdiction in the courts.[166]

For the first time, FTC defendants, in two separate cases involving breaches of consumer data, are challenging the agency's power to enforce Section 5 for privacy-related offenses. In both cases, the defendants argue that "the FTC's enforcement action . . . should be dismissed because the Commission never provided the 'fair notice' that the Constitution and these cases require," since Section 5 generally prohibits unfair and deceptive business practices and "the FTC has published no rules or regulations at all explaining what data security practices a company must adopt to be in

---

159. George R. Milne, Mary J. Culnan, & Henry Greene, *A Longitudinal Assesment of Online Privacy Notice Readability*, 25 J. PUB. POL'Y & MARKETING 238, 243 (2006).

160. Chris Hoofnagle & Jan Whittington, *Unpacking Privacy's Price*, 90 N.C.L. REV. 1327, 1358 (2012).

161. *See, e.g.*, Debra Cassens Weiss, *Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print*, A.B.A. J. (Oct. 20, 2010, 12:17 PM), http://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print/.

162. *See* FTC, *supra* note 154 ("In most cases a substantial injury involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services… Unwarranted health and safety risks may also support a finding of unfairness").

163. *See* Solove & Hartzog, *supra* note 6, at 590, 600.

164. *See, e.g.*, Google, Inc., *Decision and Order*, FTC No.102 3136, Docket No. C-4336, (2011), http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf; *see also* Facebook, Inc., *Decision and Order*, FTC No. 092 3184, Docket No. C-4365, (2011), http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; Twitter, Inc., *Decision and Order*, FTC No. 092 3093, Docket No. C-4316 (2011), http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf.

165. FTC v. Accusearch, 570 F.3d 1187 (10th Cir. 2009). For a comprehensive review of the FTC's privacy-related enforcement actions, see Solove & Hartzog, *supra* note 6, at 18.

166. *See* FTC v. Wyndham Worldwide Corp., No. 12-1365 (D. Ariz. 2012); *see also* LabMD, Inc., FTC No. 102 3099, Docket No. 9357 (May 26, 2015).

compliance with the statute."[167] While the FTC almost certainly has the authority to use Section 5 to reach the conduct at issue in these cases,[168] it is notable that it has taken twenty-five years of privacy work in the digital era before facing such a challenge.

Treating consumer data as if it were oil—that is, recognizing digital interactions as commercial exchanges of value—would synchronize well with the FTC's authority and jurisdiction, ensuring that the agency remains sufficiently equipped to fulfill its mandate. Armed with such a framing, proving a deception theory would not require the FTC to perform a nuanced review of opaque privacy policies and convoluted data practices, but a showing that the "price" that consumers paid for a service (e.g., the data collection, use, and sharing rights consumers granted) was not consistent with what had been advertised.[169] Likewise, proving an unfairness theory would not require the agency to painstakingly connect specific consumer data to financial losses or physical intrusions borne by specific consumers in order to establish the requisite consumer harm. Instead, the FTC could establish harm by showing that the data collection, use, and sharing rights taken from consumers were more than the consumer had bargained for.[170]

C. Recognizing Digital Interactions as Commercial Exchanges of Value Would Substantiate the FTC's New Privacy Framework

The FTC has publicly acknowledged various limitations in its power to safeguard consumer privacy in the wake of rapidly evolving technological change.[171] Chief among these limitations is the agency's perceived inability to require firms to tell consumers how the firm collects, uses, and shares

---

167. Answers and Defenses at 7, LabMD, Inc., FTC No. 102 3099, Docket No. 9357 (June 6, 2012).

168. *See* Lab MD, Inc., *Order Denying Respondent LabMD's Motion to Dismiss*, FTC No. 102 3099, Docket No. 9357, at 2 (2014) (finding that Section 5 "applies to a company's failure to implement reasonable and appropriate data security measures"), *available at* http://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf.

169. *See, e.g.*, Findings of Fact and Conclusions of Law, FTC v. Lights of Am., Inc., File No. 0923145, Civil Action No. SACV10-1333 JVS (MLGx) 93 (C.D. Cal. Sept. 17, 2013) ("Information about a product's purpose, safety, efficacy, or cost is material") (citing FTC v. Direct Marketing Concepts, Inc., 569 F. Supp. 2d 285, 299 (D. Mass. 2008)); *see also* Guide Concerning Use of the Word "FREE" and Similar Representations, 16 C.F.R. § 251.1(c) (2014) ("When making 'Free' or similar offers all the terms, conditions and obligations upon which receipt and retention of the 'Free' item are contingent should be set forth clearly and conspicuously at the outset of the offer so as to leave no reasonable probability that the terms of the offer might be misunderstood.").

170. *See, e.g.*, FTC v. Grant Connect, LLC, 827 F. Supp. 2d 1199, 1224–25 (D. Nev. 2011) (finding that defendants' failure to clearly and conspicuously disclose a "recurring $39.95 per month fee" after advertising that "all [consumers] had to pay was a small activation fee, usually $2.78," constituted a deceptive practice in violation of section 5 of the FTC Act).

171. *See* FTC, *supra* note 17, at i.

consumer data.[172] This limitation has forced the FTC to rely on self-regulatory efforts and firms' goodwill to post privacy policies, inducing the FTC to repeatedly call for legislation strengthening its powers and enabling it to reach the privacy harms that have so-far been viewed as outside the scope of Section 5.[173]

Recognizing consumers' digital interactions as commercial exchanges of value—i.e., treating consumer data as if it were oil—could go a long way toward eliminating these limitations. Such a framing would create a mandate for firms to clearly and conspicuously tell consumers how much consumers must "pay" to use the firms' services before the consumer makes any commitment. This, in turn, could lead to simpler choices as firms compete with each other for consumers' data and attention by offering consumers better "prices." By "pricing" consumer privacy, such a framing might incentive firms to account for consumer privacy at each stage in the design of their digital products and services. Essentially, such a framing would substantiate the FTC's new privacy framework—equipping the agency with the tools necessary to ensure technology continues its march forward while safeguarding consumer privacy.

1. Transparency Would Have to Increase

In its new privacy framework, the FTC called on firms to take steps to increase transparency.[174] Specifically, the agency provided that "[p]rivacy notices should be clearer, shorter, and more standardized to enable better comprehension," and called for "some standardized elements, such as format and terminology, to allow consumers to compare the privacy practices of different companies and to encourage companies to compete on privacy."[175] But, because firms are currently incentivized to reduce transparency for fear that their statements could be used against them in a Section 5 "deception" action,[176] the agency's call for "clearer, shorter, and more standardized" privacy notices is unlikely to result in increased transparency unless something changes.

If consumers' digital interactions were treated as commercial exchanges of value, then transparency would have to improve because firms would have an affirmative obligation to clearly and conspicuously disclose their privacy practices—i.e., the "price" associated with use of their product. At this point, it is a "fundamental principle that any commercial entity, before billing customers, has an obligation to notify such customers of what they may be charged for and when, a principle that applies even to reputable

172. *See* FTC, *supra* note 11, at iii.
173. *See id.* at 21–23.
174. *See* FTC, *supra* note 17, at 60 ("Companies should increase the transparency of their data practices").
175. *Id.* at 61–62.
176. Hoofnagle & Whittington, *supra* note 160, at 1358.

and highly successful companies that offer many popular products and services."[177]

It is often argued that the information asymmetry that exists with regard to consumers' understanding of firms' data practices is so large and complicated that no amount of transparency will, practically speaking, provide a level playing field.[178] However, it seems incomprehensible that something so empowering as rapid technological change could improve virtually every aspect of consumers' lives yet fail to solve something as basic as adequate notice and meaningful consent. Not only do consumers regularly execute complicated financial transactions on a regular basis,[179] but many efforts have already identified methods that yield short, clear, and standardized privacy disclosures that could serve as model "price tags."[180] Firms have long dealt with these problems in the world of advertising disclosures,[181] and the FTC has convened public workshops[182] and produced guides [183] designed specifically to facilitate the efficient disclosure of required information in a variety of new and evolving contexts.

2. Consumers Would Encounter Simpler Choices as Firms Competed for Consumers' Data and Attention

The FTC's new privacy framework also calls for firms to "simplify consumer choice," recognizing that not every aspect of a firms' data

177. Apple, Inc., FTC No. 122-3108 (Jan. 15, 2014) (Comm'r. Ohlhausen, concurring) (settling "allegations that Apple Inc. engaged in unfair acts or practices by billing iTunes account holders for charges . . . without the account holders' express informed consent"), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/statement-commissioner-maureen-k.ohlhausen/140115applestatementohlhausen.pdf.

178. *See, e.g.*, Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1882 (2013).

179. In 2012, U.S. consumers made 26.2 billion credit card transactions. Federal Reserve, THE 2013 FEDERAL RESERVE PAYMENTS STUDY: RECENT AND LONG-TERM PAYMENT TRENDS IN THE UNITED STATES: 2003-2012, 7–8 (2013), *available at* http://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf.

180. *See, e.g.*, Patrick Gage Kelley et. al., *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach* (CMU CyLab, Paper No. 09-014, Jan. 12, 2010), *available at* https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf.

181. *See, e.g.*, FTC v. Colgate-Palmolive Co., 380 U.S. 374 (1965) ("It has long been considered a deceptive practice to state falsely that a product ordinarily sells for an inflated price but that it is being offered at a special reduced price").

182. *See, e.g.*, Workshop, FTC, *In Short: Advertising & Privacy Disclosures in a Digital World* (May 30, 2012, 9:00 AM), *available at* http://www.ftc.gov/news-events/events-calendar/2012/05/short-advertising-privacy-disclosures-digital-world.

183. *See, e.g.*, FTC, .COM DISCLOSURES: HOW TO MAKE EFFECTIVE DISCLOSURES IN DIGITAL ADVERTISING (2013), *available at* http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf; *see also* FTC, *supra* note 73.

practices ought to require express informed consent.[184] For practices where consumers should be given a choice, the agency's new framework provides that "companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data," obtaining "express affirmative consent before: (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data."[185] However, absent a material misrepresentation to consumers, the FTC currently has little power to ensure that firms offer consumers meaningful choice regarding consumer data practices.

Because recognizing consumers' digital interactions as commercial exchanges of value would force firms to increase the transparency of their data practices, all firms would begin having to justify their "price" to consumers. In traditional markets, firms compete over both price and quality.[186] However, by ignoring privacy costs, consumer-facing Internet-enabled services tend to compete only in terms of quality. If these firms were naturally incentivized to compete over "price"—i.e., over their consumer data practices—then such competition could create simplified choices for consumers. By requiring firms to conspicuously disclose material terms, recognizing digital interactions as commercial exchanges of value would place the burden of reducing the existing information asymmetry on firms, which are the cheapest cost avoiders.[187] As information asymmetry diminishes, and "prices" approach equilibrium, firms and consumers would gain transaction experience, and the terms over which they bargained would naturally be simplified. For example, rather than explain every aspect of a firm's data handling practices before every interaction, standards and baselines that could be efficiently communicated to consumers might emerge such that only deviations would have to be explained.

3. Firms Would Be Incentivized to Account for Consumer Privacy in the Design of Their Services

Finally, the FTC's new privacy framework calls on firms to practice "privacy by design."[188] Specifically, the agency has called for firms to "incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal policies, and data accuracy."[189] Again, this is a prescription that the agency has little

184. FTC, *supra* note 17, at 35–36.

185. *Id.* at 60.

186. *See, e.g.*, EINER ELHAUGE, UNITED STATES ANTITRUST LAW AND ECONOMICS 1 (2d ed. 2011).

187. *See* Hoofnagle & Whittington, *supra* note 160, at 1357–58 (comparing the "personal information transaction space" to the financial services context, where the "Schumer Box" shifted transaction costs from consumers onto the parties with the greatest incentives to obscure costs).

188. FTC, *supra* note 17, at 22.

189. *Id.* at 30.

power to support. In addition, it is not entirely clear how firms can "bake" privacy into the design of their products and services.[190]

However, if consumers' digital interactions were recognized as commercial exchanges of value, firms would naturally begin to consider consumer privacy at every stage of their design process. Firms are profit-seeking actors; they seek to minimize their costs while maximizing their revenues.[191] It is axiomatic that firms design their products and services in ways that maximize firms' competitive advantage. If collecting and handling consumers' data imposed costs on them beyond those of the underlying technologies used to gather, store and analyze the data (e.g., through lost revenues, as consumers turned to better priced competitors), then firms would inherently consider these costs as they engineered their products and services.

D. Implementing the Data-As-Oil Framing

Over time, as data continues to fuel technology's march forward, consumers' digital interactions may naturally be recognized as commercial exchanges of value. However, to ensure that the data-as-oil framing advocated by this Note becomes a reality within a useful time span, the FTC could submit the framing to public scrutiny before bringing a pilot case to test its merits.

Before taking significant regulatory action in a new domain, the FTC often invites the public to help the agency evaluate new issues and approaches. This is how the agency developed its existing privacy framework[192] and it generally reflects how the FTC grapples with the consumer protection issues of evolving technologies.[193] In order to refine the data-as-oil framing, and to notify those on the other side of consumers' digital interactions of a shift in approach, the FTC could host a public workshop exploring the framing's implications. In such a workshop, the FTC could call on attorneys, economists, consumers, and businesses to work through different hypothetical scenarios, examining how different disclosure and data handling practices complied or conflicted with Section 5's prohibition of unfair or deceptive practices.

---

190. *See, e.g.*, Ira S. Rubenstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1335 (2013) (noting that "despite the strong expressions of support for privacy by design, its meaning remains elusive").

191. *See. e.g.*, Herbert Hovenkamp, *Rationality in Law & Economics*, 60 GEO. WASH. L. REV. 293, 293 (1992) ("Economists assume that firms act rationally to maximize profits.").

192. *See* FTC, *supra* note 17, at 19–20.

193. *See, e.g.*, *News & Events*, FTC http://www.ftc.gov/news-events/commission-actions (filtered for "public event") (listing numerous FTC conferences addressing such topics as "Alternative Scoring Products", "Mobile Device Tracking", "Internet of Things", and "Mobile Security: Potential Threats and Solutions").

After running the data-as-oil framing through a gauntlet of public scrutiny, the FTC could then bring a pilot case to test the framing before an administrative law judge.[194] Such an enforcement action would enable the FTC to pick an ideal test defendant[195] and try the issue before an expert judge, familiar with the nuance of Section 5. Assuming the agency prevails in its test case, the FTC could then use the precedent to develop the framing by applying it in varying scenarios and courts.[196]

V. CONCLUSION

Rapidly evolving technology promises to continue bringing wonderful things to reality, but it also poses complex and evolving privacy dilemmas. This tendency creates a need for a flexible regulatory framework capable of scaling to meet technology's challenges without stifling innovation. The United States regime for safeguarding consumer privacy relies almost entirely on the FTC to enforce Section 5's broad prohibition of unfair or deceptive acts or practices, but the FTC has openly acknowledged limitations in its ability to carry out this mission—creating a new privacy framework and calling for baseline privacy legislation to bolster its authority.

The FTC's new privacy framework, however, ultimately depends on authority that the FTC does not believe it has. Recognizing digital interactions as commercial exchanges of value would ameliorate this problem. Such a framing would create a mandate for entities that collect data from consumers in exchange for digital products and services to disclose the bargain's material terms by requiring informed consent. This, in turn, might lead to simplified choice and "privacy by design" as companies competed over their consumer products' prices. Such a framing may not be able to solve all of privacy's problems, and more critical thinking needs to be devoted to the topic, but it could substantiate the FTC's new privacy framework—creating a flexible regulatory solution that scales to meet privacy's evolving problems.

---

194. "Under Section 5(b) of the FTC Act, the Commission may challenge "unfair or deceptive act[s] or practice[s]" . . . through maintenance of an administrative action." *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FTC (July 2008), http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last visited April 4, 2014) (quoting 15 U.S.C. § 45(b)).

195. The "ideal" defendant might consist of a well-funded company whose business centers on monetizing consumer data and attention—e.g., a profitable mobile app developer who offers consumers a valuable game or service monetized through the sale of targeted ads, and who only provides an opaque privacy policy. Such a fact pattern would make the value exchange between the consumer and developer as explicit as possible, since the developer's revenues could be directly apportion to individual consumers.

196. If the agency loses in an administrative action, staff may appeal the decision to the full Commission. *See* 15 U.S.C. § 45(b) (2012). Challenges to Commission decisions can be heard in federal appeals courts, 15 U.S.C. § 45(c), but the FTC's decision must be given administrative deference. *See* Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837 (1984).