THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XVIII STLR.ORG FALL 2016

ARTICLE

A LAW AND ECONOMICS APPROACH TO PRIVACY POLICY MISSTATEMENTS: CONSIDERING THE NEED FOR A COST-BENEFITS ANALYSIS IN THE FTC'S DECEPTION FRAMEWORK†

Shawn A. Johnson*

* J.D., C.P.A., and Law Clerk to the Honorable Justice Paul W. Green, Supreme Court of Texas.

I. INTRODUCTION

It is said that today's world is "shaped by technology and fueled by information."[1] Technological innovations such as mobile phones, audio and video recording devices, and computers, as well as the Internet and the rise of Big Data, have revolutionized our ability to capture, analyze, and share information.[2] Further, information is undoubtedly critical to the economy. When readily available, consumer information enables businesses to "deliver the right products and services to the right customers, at the right time, more effectively and at a lower cost."[3] It also enhances customer convenience, improves service quality, and allows businesses to target those likely to be interested in the goods and services they offer, reducing waste and the need for mass advertising.[4] Indeed, information about consumer needs and preferences is said to be "the cornerstone of any system that allocates goods and services within an economy."[5] As more information about consumers becomes available, the economy can more accurately and efficiently meet their needs and preferences.[6] As former Federal Reserve Board Chairman Alan Greenspan wrote in 1998:

> A critical component of our ever more finely hewn competitive market has been the plethora of information on

---

1. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1 (5th ed. 2015).

2. *See id.*

3. Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 882 (2000) (quoting Fred L. Smith, Jr., *Better to Share Information*, DESERET NEWS, Oct. 14, 1999, at A22).

4. *See* FRED H. CATE, PRIVACY IN PERSPECTIVE 12–14 (2001). According to Cate, information sharing also promotes competition and innovation, and "is especially critical for new and smaller businesses, which lack extensive customer lists . . . or the resources to engage in mass marketing . . . ." *Id.* at 14.

5. Cate, *supra* note 3, at 882 (quoting *Financial Privacy, Hearings Before the Subcomm. on Fin. Insts. and Consumer Credit of the H. Comm. on Banking and Fin. Servs.*, 106th Cong. (1999) (statement of Edward M. Gramlich, Member, Board of Governors of the Federal Reserve System)). A report in 2011 estimated that Big Data and analytics could yield potential gains in the overall economy by up to $610 billion in annual productivity and cost savings. Thomas M. Lenard & Paul H. Rubin, *Big Data, Privacy and the Familiar Solutions*, 11 J.L. ECON. & POL'Y 1, 6 (2015) (citing SUSAN LUND, ET. AL., GAME CHANGERS: FIVE OPPORTUNITIES FOR US GROWTH AND RENEWAL 66, (McKinsey Global Institute 2013), http://www.mckinsey.com/global-themes/americas/us-game-changers.

6. Cate, *supra* note 3.

> the characteristics of customers both businesses and individuals. Such information has enabled producers and marketers to fine tune production schedules to the ever greater demands of our consuming public for diversity and individuality of products and services.[7]

But many privacy advocates argue that the technological revolution that started in the twentieth century and continues today has caused a rapid erosion of personal privacy.[8] Without a doubt, more personal information is readily available to both public and private sector entities today than at any other point in mankind's history. One proposal to stop this erosion is "to stop the avalanche of technology and commercial opportunity responsible for [it] . . . . by intervening in the market for privacy [by] increas[ing] the cost of consuming other people's privacy and lower[ing] the profits of voluntarily giving up one's own privacy."[9] Others argue for a less paternalistic approach, such as an increased emphasis on privacy-enabling technologies like encryption[10] or a greater effort to obtain prior informed consent from consumers.[11] Irrespective of the framing of the issue and the various proposed solutions, most privacy scholars agree that "the collection and use of personal data by businesses and government is spinning out of control."[12]

While merchants that collect, use, store, and share consumer information are not specifically regulated under federal law, they are nevertheless regulated by the Federal Trade Commission (FTC),

---

7. Letter from Chairman Alan Greenspan, Fed. Reserve Bd., to Rep. Edward J. Markey, U.S. H.R., July 28, 1998, at 1, http://assets.complianceexpert.com/fileserver/file/4780/filename/6-99G-LFP-Appendix6.1.pdf.

8. *See, e.g.*, Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 729 (1999); Jonathan Shaw, *The Erosion of Privacy in the Internet Era*, HARV. MAG., Sept.–Oct. 2009, at 38, *available at* http://harvardmagazine.com/2009/09/privacy-erosion-in-internet-era; *see also* Abraham R. Wagner & Paul Finkelman, *Security, Privacy, and Technology Development: The Impact on National Security*, 2 TEX. A&M L. REV. 597, 611–15 (2015) ("For most of history people have had very little to keep private. Literacy was limited, communications were costly and even more limited, and there was no Big Data.").

9. Allen, *supra* note 8, at 733-34.

10. *See About EFF*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/about (last visited Feb. 5, 2016).

11. *See* CATE, *supra* note 4, at 17.

12. Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 359.

which has power under Section 5 of the Federal Trade Commission Act to sanction businesses that engage in deceptive or unfair acts or practices in relation to their collection and use of consumer data.[13] But some have called into question the FTC's method for determining whether to bring a Section 5 enforcement action, arguing for "a deeper integration of economics and cost-benefit analysis" into the FTC's consumer protection framework.[14] They argue that "[a]n economic approach to privacy regulation [should be] guided by the tradeoff between the consumer welfare benefits of new and enhanced products and services against the potential harm to consumers, both of which arise from the same free flow and exchange of data."[15]

This Article examines calls for the integration of economic considerations into the FTC's Section 5 framework. It does so by applying law and economics analysis to the FTC's recent enforcement action against Nomi Technologies, a retail analytics provider, for a privacy policy misstatement. In Part II, the Article sets the stage by providing a brief summary of the current state of consumer privacy law and explaining how the FTC became the predominant consumer privacy watchdog in the United States. Part III cites calls for increased economic considerations to temper the FTC's power and distinguishes the two methods through which the FTC may sanction privacy violations—unfairness and deception. Part IV discusses Nomi's data collection practices and its settlement with the FTC. The Article proceeds to the law and economics analysis in Part V, using both rational and behavioral models to determine whether the FTC's deception framework produces economically efficient outcomes in the context of privacy policy misstatements and to recommend efficiency-promoting improvements to that framework. A summary of the Article and its conclusions are set out in Part VI.

II. THE STATE OF U.S. CONSUMER PRIVACY LAW

---

13. *See* 15 U.S.C. § 45 (2012); *see also infra* text accompanying notes 44–63.

14. Joshua D. Wright, The FTC and Privacy Regulation: The Missing Role of Economics 2 (Nov. 12, 2015), http://masonlec.org/site/rte_uploads/files/Wright_PRIVACYSPEECH_FINALv2_PRINT.pdf.

15. *Id.* at 5; *see also id.* at 7.

The concept of "privacy" is amorphous.[16] In Warren and Brandeis' famous 1890 law review article, *The Right to Privacy*, privacy was defined as the "general right of the individual to be let alone."[17] In recent decades, legal scholars and privacy advocates have refined this definition and, though far from reaching universal consensus, generally agree that privacy is "a right of personhood, intimacy, secrecy, limited access to the self, and control over information."[18] More specifically, they define *informational privacy* as the right to control "the collection, use and disclosure of personal information."[19] Today, these rights arise from and are protected by "an interrelated web of tort law, federal and state constitutional law, federal and state statutory law, evidentiary privileges, property law, contract law, and criminal law."[20]

In the United States, consumer privacy is regulated by "sectoral" laws that focus on various segments of the economy.[21] While Europe uses an omnibus approach in which one overarching statute regulates personal information use irrespective of the entities or industries that wish to process it, in a sectoral approach, different laws regulate different industries, economic sectors, and types of information.[22] For example, the Health Insurance Portability and Accountability Act (HIPAA) protects health data,[23] while financial

---

16. *See generally* CATE, *supra* note 4, at 3–4 (listing some common definitions, including individual autonomy, solitude and intimacy, confidentiality, anonymity, security, freedom from intrusion, and control of information about oneself).

17. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890).

18. SOLOVE & SCHWARTZ, *supra* note 1, at 45; *see also* ALAN WESTIN, PRIVACY AND FREEDOM (1967) ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."); Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("Privacy is . . . the *control* we have over information about ourselves.").

19. SOLOVE & SCHWARTZ, *supra* note 1, at 2.

20. *Id.*

21. *Id.* at 790; *see also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014).

22. SOLOVE & SCHWARTZ, *supra* note 1, at 790; *see also* Solove & Hartzog, *supra* note 21, at 587.

23. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered titles of U.S.C.). Medical and health information is also protected in tort through breach of confidentiality and public disclosure of private facts and through the

data is regulated by statutes such as the Gramm-Leach-Bliley Act[24] and the Fair Credit Reporting Act.[25] There are different statutes for entertainment records[26] and marketing,[27] and there are statutes protecting the privacy of certain classes.[28] And one cannot forget the various state law protections that are generally sectoral as well.[29] In short, "it is fair to say that U.S. privacy law regulates only specific types of data when collected and used by specific types of entities."[30]

Currently, no federal statute specifically regulates consumer information contained in merchant records.[31] Instead, merchants are largely self-regulated. With respect to the collection, use, or disclosure of this information, the principal approach taken by most businesses is "notice and choice."[32] In one form of notice and choice, businesses provide take-it-or-leave-it privacy policies (or "privacy notices") that describe the methods in which personal data will be collected, used, or disclosed.[33] Consumers are said to have a "choice" because they can decide *whether or not* to purchase goods or services from a given business. Others provide a privacy policy containing a statement that consumers may "opt out" of all forms of data collection, usually by filling out an online form. Some

---

Constitution by the constitutional right to information privacy and the Fourth Amendment.

24. Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered titles of U.S.C.).

25. Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1936 (codified as amended in scattered titles of U.S.C.).

26. *See* Cable Communications Policy Act of 1984 (as amended), 47 U.S.C. ch. 5, subch. V–A (2012) (amending the Communications Act of 1934); Video Privacy Protection Act of 1988 (as amended), 18 U.S.C. § 2710 (2012)).

27. *See* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C. ch. 5); Telephone Consumer Protection Act of 1991 (as amended), 47 U.S.C. § 227 (2012)); CAN-SPAM Act of 2003, 15 U.S.C. ch. 103 (2012).

28. *See* Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-728 (codified as amended in scattered sections of 15 U.S.C.).

29. *See, e.g.*, California's Privacy Rights for California Minors in the Digital World Act of 2015, CALIF. BUS. & PROF. CODE §§ 22580–22582 (West Supp. 2015); California Online Privacy Protection Act of 2003 (as amended), CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2014). Privacy is also protected by some state constitutions.

30. Solove & Hartzog, *supra* note 21, at 587.

31. SOLOVE & SCHWARTZ, *supra* note 1, at 790–91; Solove & Hartzog, *supra* note 21, at 587–88.

32. Solove & Hartzog, *supra* note 21, at 593.

33. Solove & Hartzog, *supra* note 21, at 592.

companies go further, offering consumers choices through provisions granting them the ability to opt out of certain data uses or disclosures. But consumer assent is the default under an opt-out regime—consumer information will be processed unless an affirmative step is taken to indicate a desire to the contrary.[34] Thus, many privacy advocates argue that opt-out is effectively information collection without consent and call for an opt-in approach—in which consumers must affirmatively consent to information collection and use before such activities can occur.[35]

By contrast, "free-flow advocates" argue that opt-out and opt-in approaches offer consumers the same protection but caution that an opt-in approach "imposes significantly higher costs on consumers, businesses, and the economy as a whole because of the difficulty contacting consumers one by one to obtain their affirmative consent . . . ."[36] To those in the free-flow camp, an opt-in regime establishes "no information flow" as the default rule because of the high transaction costs of an opt-in regime on both businesses and consumers. Free-flow advocates argue that the high transaction costs neutralize the efficiency gained through advanced data collection techniques and restrict "the information lifeblood on which today's economic activity depends."[37]

Further complicating the protection of consumer information privacy, consumer behavior suggests a general disinterest in the matter. In fact, very few consumers actually read privacy policies or take advantage of privacy-enabling technologies.[38] But a primary reason that consumers do not read privacy policies is that they are too costly to read. According to a study conducted in 2009, "the cost to the economy of the time spent reading Internet privacy notices would be $781 billion per year" (or 53.8 billion hours per year).[39]

---

34. *Id.*; *see also* SOLOVE & SCHWARTZ, *supra* note 1, at 828.

35. CATE, *supra* note 4, at 34-35.

36. *Id.* at 35.

37. Michael E Staten & Fred H. Cate, *The Impact of Opt-In Privacy Rules on Retail Markets: A Case Study of MBNA*, 52 DUKE L.J. 745, 766 (2003).

38. Eric Goldman, *The Privacy Hoax*, FORBES (Oct. 14, 2002), http://www.forbes.com/forbes/2002/1014/042.html; Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 J.L. & POL'Y INFO. SOC'Y 425, 428 (2011). The better argument seems to be that privacy policies enable privacy watchdogs to inform the public as well as legislatures about the realities of data-collection and use practices and of the causal connection between privacy and data-collection activities. *See* Steven Hetcher, *Changing the Social Meaning of Privacy in Cyberspace*, 15 HARV. J.L. & TECH. 149, 161–62 (2001).

39. MacCarthy, *supra* note 38, at 428, 436 (citing Aleecia McDonald & Laurie Faith Cranor, *The Cost of*

One reason for this, however, is that privacy policies often contain misstatements or are riddled with legalese drafted by attorneys—such that consumers are unable to make informed decisions even if they take the time to read the posted policy.

Consumer behavior also indicates that most consumers do not place a high value on information privacy, as they routinely "sell" their personal information at very low prices.[40] For instance, studies show that although consumers will express in surveys that they are very concerned about privacy, they will gladly reveal detailed personal information in exchange for small product discounts.[41] A similar study found that an overwhelming number of consumers would give personal information to a new online store for the opportunity to enter into a $100 sweepstakes.[42] In an attempt to estimate the price that U.S. consumers would pay to protect their information, two well-known studies found that most consumers value their information from only a few cents to just over $30.[43]

But legal safeguards are in place to protect consumers: although merchants that collect customer information are not specifically regulated under federal law, they often fall under the FTC's Section 5 jurisdiction because they have a privacy policy, and privacy policies are enforced by the FTC.[44] In fact, through this power, the

---

Reading Privacy Policies, 4 J.L. & POL'Y INFO. SOC'Y 543 (2008) (estimating that reading privacy policies carries costs in time of over 200 hours a year, worth about $3,534 annually, per U.S. Internet user)).

40. Alessandro Acquisti et al., *What Is Privacy Worth?*, 42 J. LEGAL STUD. 249, 250 (2013) (identifying empirical studies attempting to quantify individual privacy valuations); *see also* PAUL H. RUBIN & THOMAS M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION 83 (2002) (applying the economic principle of revealed preferences to conclude that society does not place much value on privacy).

41. Goldman, *supra* note 38; Sarah Spiekermann, Jen Grossklags & Bettina Berendt, *E-Privacy in Second Generation E-Commerce: Privacy Preferences Versus Actual Behavior*, *in* PROCEEDINGS OF THE THIRD ACM CONFERENCE ON ELECTRONIC COMMERCE 38 (Michael P. Wellman & Yoav Shoham, eds., 2001).

42. Goldman, *supra* note 38.

43. Acquisti et al., *supra* note 40, at 254 (citing Hal R. Varian, Fredrik Wallenberg & Glenn Woroch, *The Demographics of the Do-Not-Call List*, 3 IEEE SECURITY & PRIVACY 34-39 (2005); Ivan P. L. Png, *On the Value of Privacy from Telemarketing: Evidence from the "Do Not Call" Registry* (Nat'l Univ. of Sing. Working Paper, 2007)). Similar studies have found a range of $30 to $45. *Id.* at 255–56 (citing Il-Horn Hann et al., *Overcoming Information Privacy Concerns: An Information Processing Theory Approach*, 24 J. MGMT. INFO. SYS. 13-42 (2007)).

44. Solove & Hartzog, *supra* note 21, at 588; *see also id.* at 594 ("[T]oday, whether for online or offline activities, most established companies in nearly all

FTC has become the nation's chief information privacy regulator. As Professors Daniel J. Solove and Woodrow Hartzog have explained:

> Since the late 1990s, the Federal Trade Commission (FTC) has been enforcing companies' privacy policies through its authority to police unfair and deceptive trade practices. . . . The cases have nearly all resulted in settlement agreements. Nevertheless, companies look to these agreements to guide their privacy practices. Thus, in practice, FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States—more so than nearly any privacy statute or any common law tort.[45]

Because the FTC is authorized to sanction deceptive or unfair acts or practices, such as a business's non-compliance with its own privacy policy, the FTC has enjoyed expansive jurisdiction to protect consumer privacy, in addition to the statutory jurisdiction Congress has granted it through sectoral legislation.[46] In fact, because many companies fall outside the purview of sectoral privacy laws, in many instances the FTC is the primary source of regulation—making it "the largest and arguably the most important component of the U.S. privacy regulatory system."[47]

For context, a brief history lesson is in order. Congress established the FTC in 1914 to ensure fair competition in commerce.[48] In 1938, the Wheeler-Lea Act amended Section 5 to extend the FTC's jurisdiction to proscribe "unfair or deceptive acts or practices" and "unfair methods of competition," charging the

---

industries have a privacy policy.") (citing and discussing Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN. ST. L. REV. 587, 593–94 (2007); FTC, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress 10 (2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf)).

45. Solove & Hartzog, *supra* note 21, at 583. The FTC also has some enforcement power over the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Children's Online Privacy Protection Act, among others. *See id.* at 602.

46. *Id.* at 588.

47. *Id.*

48. *Id.* at 598 (citing *About the Federal Trade Commission*, FTC, https://www.ftc.gov/about-ftc (last visited Jan. 27, 2016)).

FTC with protecting consumers directly.[49] In 1995, Congress requested that the FTC become involved with consumer privacy issues, using its existing powers.[50]

Since 1998, the FTC has held the position that the "use or dissemination of personal information in a manner contrary to a posted privacy policy is a deceptive trade practice" under Section 5.[51] Through the use of its Section 5 authority to sanction deceptive or unfair privacy practices, the FTC has gained jurisdiction (i.e., power) over the privacy arena.[52] Although the FTC essentially lacks rulemaking authority under Section 5,[53] "through a common law-like process, the FTC's [enforcement] actions have developed into a rich jurisprudence that is effectively the law of the land for businesses that deal in personal information."[54]

The FTC also has relatively limited enforcement power in relation to information privacy practices, but the agency has utilized its power quite effectively. The FTC Act does not create a private right of action, so only the FTC can enforce it. Although the FTC can obtain injunctive remedies, it does not have power to issue punitive fines under Section 5.[55] Instead, the FTC can generally issue such fines only when a company violates a "consent decree" previously entered into for a Section 5 violation.[56] Companies that

---

49. *Id.* (discussing the passage of the Wheeler-Lea Act of 1938 (as amended), 15 U.S.C. § 45 (2012).

50. *Id.* (citing FTC, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress 3–5 (2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf).

51. SOLOVE & SCHWARTZ, *supra* note 1, at 848. The FTC's unfairness and deception frameworks do not require ownership of personal data. *See* Hetcher, *supra* note 38, at 171 n.82.

52. Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041 (2000).

53. SOLOVE & SCHWARTZ, *supra* note 1, at 849. The FTC has Magnuson-Moss rulemaking authority requiring the FTC to conduct "an industry-wide investigation, prepare draft reports, propose a rule, and engage in a series of public hearings . . . . These processes are so burdensome that the FTC has not engaged in Magnuson-Moss rule-making in 32 years.". *Id.* (quoting Beth DeSimone & Amy Mudge, *Is Congress Putting the FTC on Steroids?*, Seller Beware Blog, Arnold & Porter (Apr. 26, 2010), http://www.consumeradvertisinglawblog.com/2010/04/is-congress-putting-the-ftc-on-steroids.html)

54. Solove & Hartzog, *supra* note 21, at 589.

55. SOLOVE & SCHWARTZ, *supra* note 1, at 849.

56. *Id.* According to Professors Solove and Hartzog, "When the FTC does include fines, they are often quite small in relation to the gravity of the violations and the overall net profit of the violators. This is because any fines issued by the

violate a consent decree are liable for a civil penalty of up to $16,000 per violation, which could be on a per-user or per-record basis. It is from these consent decrees that a "common law of privacy" emerges.[57] Even though they function more like contracts than binding precedent, "companies look to these agreements to guide their decisions regarding privacy practices."[58] As Professors Solove and Hartzog aptly describe, "[t]he FTC has codified certain norms and best practices and has developed some baseline privacy protections. Standards have become so specific they resemble rules."[59]

In addition to the risk of fines for non-compliance, the FTC's settlement provisions can impose other significant costs on a company. These additional costs give teeth to the FTC's Section 5 authority. According to Professors Solove and Hartzog:

> Businesses fear the length of the FTC's auditing process—twenty years in more than fifty percent of the cases. The auditing process is exhaustive and demanding. A typical assessment requires the specific detailing of the agreed-upon safeguards to protect consumer information; an explanation of "how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered device functionality or covered information"; an explanation of "how the safeguards that have been implemented meet or exceed the protections" agreed upon in the consent order; and a certification of the effectiveness of the company's protections by "a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession."[60]

From 1997 to 2015, the FTC issued more than 200 privacy-related complaints,[61] and the number of complaints issued per year

---

FTC must reflect the amount of consumer loss." Solove & Hartzog, *supra* note 21, at 605.

57. Solove & Hartzog, *supra* note 21, at 589.

58. *Id.* at 585, 607.

59. *Id.* at 583.

60. *Id.* at 606 (citations omitted).

61. *See Legal Resources*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/legal-resources?title=&type=case&field_consumer_protection_topics_tid=245&field_industry_tid=All&field_date_value%5Bmin%5D%5Bdate%5D=&field_date_value%5Bmax%5D%5Bdate%5D=&sort_by=field_date_value

is on the rise. For example, the FTC brought seven privacy-related complaints in 2002, thirteen in 2012, and twenty-five in 2015.[62] The majority of these complaints resulted in consent decrees, adding to the ever-growing "common law" of consumer information privacy.[63]

III. THE NEED FOR LAW AND ECONOMICS AT THE FTC

Many have argued that the FTC should incorporate an economic analysis into its Section 5 framework as it relates to consumer privacy issues. Most recently, former FTC Commissioner Joshua D. Wright argued at a November 2015 conference that the FTC can and should employ "a deeper integration of economics and cost-benefit analysis" into its privacy framework.[64] According to Commissioner Wright, as in antitrust regulation, privacy regulation will have to integrate "the insights from economics, such as how firms compete with respect to privacy protections, the effect of privacy regulation on consumer welfare and competition, and consumer preferences for privacy."[65]

Commissioner Wright advocates for an economic approach "guided by the tradeoff between the consumer welfare benefits of new and enhanced products and services against the potential harm to consumers."[66] He cautions that "[i]f the benefits of these welfare-enhancing business practices are not weighed correctly against the harms they present to consumers, we run the risk of squelching innovation and depriving consumers of these benefits."[67] In fact, Commissioner Wright suggests that the FTC frequently fails to evaluate these tradeoffs properly, identifying two critical flaws in its current analytical framework.[68] First, he argues that the FTC tends to discount the benefits of new technologies that may pose threats to consumer privacy.[69] Second, he believes that current FTC practices "place[] far too much emphasis on speculative and anecdotal risks

---

&=Apply (last visited Feb. 4, 2016) (filtering on Type: Case and Topic: Privacy and Security).

62. *See id.*; *see also* Solove & Hartzog, *supra* note 21, at 610 (providing figures from 1997 to 2014).

63. *See Legal Resources*, *supra* note 61; *see also* Solove & Hartzog, *supra* note 21, at 610.

64. Wright, *supra* note 14, at 2.

65. *Id.* at 2–3.

66. *Id.* at 5; *see also id.* at 7.

67. *Id.* at 6.

68. *Id.*

69. *Id.*

without adequately assessing whether the benefits of these new technologies outweigh the concerns."[70] The result, according to Commissioner Wright, is that "[s]ometimes . . . the direction the FTC is going in terms of consumer protection enforcement does not make economic sense."[71]

Commissioner Wright is not the first to call for economics at the FTC. For example, in 2000, then-Commissioner Orson Swindle responded to the FTC's recommendation for online privacy regulation, arguing:

> [T]he Privacy Report fails to pose and to answer basic questions that all regulators and lawmakers should consider before embarking on extensive regulation that could severely stifle the New Economy. Shockingly, there is absolutely no consideration of the costs and benefits of regulation; nor the effects on competition and consumer choice; nor the experience to date with government regulation of privacy; nor constitutional implications and concerns; nor how this vague and vast mandate will be enforced.[72]

Before proceeding to the law and economics analysis of the FTC's action against Nomi, it is important to understand the existing constraints on the FTC's power to sanction companies for privacy violations. Thus, the remaining two Sections of this Part describe and differentiate Section 5's unfairness and deception liability theories.

A. Unfairness

---

70. *Id.* (adding that other times the FTC "simply asserts that consumer benefits do not exist").

71. *Id.* at 17.

72. Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress, Dissenting Statement of Commissioner Orson Swindle 16 (May 25, 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/swindledissent.pdf; *see also* J. Howard Beales, III & Timothy J. Muris, *FTC Consumer Protection at 100: 1970s Redux or Protecting Markets to Protect Consumers?*, 83 GEO. WASH. L. REV. 2157, 2204 (2015); *see also* Richard Craswell, *Regulating Deceptive Advertising: The Role of Cost-Benefit Analysis*, 64 S. CAL. L. REV. 549, 552 (1991).

Amendments to the FTC Act require a balancing of interests when the FTC pursues an "unfair" act or practice claim. Specifically, in 1994, Congress amended the Act to incorporate the FTC's Unfairness Policy Statement[73] to ensure that the FTC would follow an objective methodology when evaluating fairness rather than focusing exclusively on public policy considerations.[74] The 1994 amendment added subsection (n), which states:

> The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless 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*. 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. Such public policy considerations may not serve as a primary basis for such determination.[75]

Thus, the FTC Act already requires that the FTC conduct a cost-benefit analysis in some cases: a practice will be deemed unfair only if it causes substantial injury to consumers[76] that they cannot

---

73. According to the FTC's Statement on Unfairness, injury to a consumer caused by an unfair practice "must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces." FTC Policy Statement on Unfairness, appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [hereinafter FTC Policy Statement on Unfairness]. Under this policy the FTC "will not find that a practice unfairly injures consumers unless it is injurious in its net effects," considering "the costs to the parties directly before the agency, the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters." *Id.*

74. Winston J. Maxwell, *The Notion of 'Fair Processing' in Data Privacy Law*, *in* QUELLE PROTECTION DES DONNÉES PERSONNELLES EN EUROPE? (Céline Castets-Renard, ed., 2015), http://ssrn.com/abstract=2544623.

75. Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312, 108 Stat. 1691, § 9 (codified at 15 U.S.C. § 45(n) (2012)) (emphasis added).

76. Substantial injury "cannot be trivial or speculative, but ordinarily consists of 'monetary, economic or other tangible harm.' Emotional distress, mental anguish, loss of dignity and other harms are not ruled out by this criterion, but they must be effects that all or most reasonable persons would

reasonably avoid[77] and the aggregate injury is not offset by corresponding aggregate consumer benefits.[78] The last step in the unfairness test requires that the FTC evaluate countervailing benefits, which means the FTC must inquire whether the practice generates new valuable services or lower prices for consumers. In this connection, the FTC must compare the situation that would exist in the absence of any regulation by the FTC to the situation that would exist if the practice were stopped or regulated.[79] The difference represents the costs associated with the FTC's own regulatory action, and conversely, the benefits associated with leaving the practice unregulated.[80] In short, the FTC can bring an unfairness claim only when regulation will result in a net increase in social welfare.

B. Deception

The FTC's approach to deceptive acts or practices is embodied in its 1984 Policy Statement on Deception.[81] The FTC will find deception if there has been a material representation, omission, or practice that is likely to mislead consumers acting reasonably under the circumstances, to the detriment of consumers.[82] For present purposes, only the element of materiality is relevant. "The basic question is whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service."[83]

According to Commissioner Wright, "The materiality inquiry is critical because the [FTC's] construct of 'deception' uses materiality as an evidentiary proxy for consumer injury: '[i]njury exists if consumers would have chosen differently but for the deception. If

---

construe as genuine harms." MacCarthy, *supra* note 38, at 483 (footnote omitted).

77. Including the ability to decline to participate in the activity. *Id.* at 486.

78. This is about net social welfare. "The compensating benefit need not be distributed to the same individuals who experience the harm." *Id.* at 487.

79. *See* Maxwell, *supra* note 74.

80. *See id.*

81. FTC Policy Statement on Deception, appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception [hereinafter FTC Policy Statement on Deception].

82. *Id.*; *see also* GEOFFREY A. MANNE ET AL., IN THE MATTER OF NOMI TECHNOLOGIES, INC.: THE DARK SIDE OF THE FTC'S LATEST FEEL-GOOD CASE 5 (2015).

83. FTC Policy Statement on Deception, *supra* note 81.

different choices are likely, the claim is material, and injury is likely as well.'"[84] He believes that the requisite link between materiality and consumer injury ensures that the agency's authority is employed to deter only conduct that is likely to harm consumers and will not deter conduct that improves consumer welfare. However, the materiality test lacks a requirement that the FTC evaluate countervailing consumer benefits, which means it need not inquire whether its action in a particular case will increase social welfare.

Thus, the FTC's framework for determining whether an act or practice is deceptive is quite different from its test for unfairness. Most importantly, a cost-benefit analysis is not required in order for the FTC to establish that an act or practice is deceptive.[85] Where a company has not broken its promises (and therefore not deceived consumers), the FTC would have to couch the practice as "unfair," requiring a cost-benefits analysis.[86] But where, for instance, a company violates an express statement in its online privacy policy, the FTC can charge the company with deceiving consumers without conducting a cost-benefit analysis. This results in a form of strict liability for deceptive acts or practices.

IV. IN THE MATTER OF NOMI TECHNOLOGIES

Nomi Technologies' "Listen" service provides retail analytics to brick-and-mortars based on data collected from mobile device tracking technology.[87] Commissioner Wright succinctly described Nomi's service at the November 2015 conference:

> Nomi uses sensors placed in its clients' retail locations or its clients' existing WiFi access points to detect the media access control (MAC) address broadcast by a consumer's mobile device when it searches for WiFi networks. Nomi passed MAC addresses through a cryptographic hash function before collection and created a persistent unique identifier for the mobile device. Nomi did not "unhash" this identifier

---

84. Dissenting Statement of Commissioner Joshua D. Wright at 2, In the Matter of Nomi Technologies, Inc., FTC File No. 132 3251 (Apr. 23, 2015), https://www.ftc.gov/system/files/documents/public_statements/638371/150423nomiwrightstatement.pdf (dissenting to the Commission's decision to accept for public comment a consent order with Nomi) [hereinafter Dissenting Statement of Commissioner Wright].

85. *See* Maxwell, *supra* note 74.

86. *See id.*

87. Wright, *supra* note 14, at 9.

> to retrieve the MAC addresses and Nomi did not store the MAC addresses . . . .[88]

A brief explanation of Wi-Fi technology is necessary for context.[89] Wi-Fi functions using the same principle as other wireless devices—using radio frequencies to send signals between devices. Many devices utilize Wi-Fi, including laptops, tablets, and smartphones. Using Wi-Fi, these devices can connect to public and private networks through a wireless network access point. When a Wi-Fi client (e.g., a smartphone or laptop) is looking to connect to a network, there are two approaches it can take. The first technique, which is used by laptops and non-smartphone devices, involves scanning for Beacon Frames (packets broadcast by wireless access devices in order to advertise their presence),[90] waiting for a network that the client has previously connected to, and initiating a connection with it. The second technique, which is used primarily by smartphones, involves periodically broadcasting packets called Probe Requests,[91] which contain the client's unique MAC address. The advantage of the second technique is that by actively scanning for nearby wireless access devices, a smartphone can initiate a wireless connection faster than if it waits for the devices to send out a Beacon Frame. While this certainly makes it more convenient to join a network, it also makes indiscriminate data collection possible. The key takeaway, however, is that Nomi was not conducting invasive data collection: mobile phones send unsolicited Probe Requests by design, and Nomi simply configured its wireless access devices to log the details of any Probe Requests received.

---

88. *Id.* A MAC address is a twelve-digit identifier that is unique to a particular device. Compl. at ¶ 4, In the Matter of Nomi Technologies, Inc., FTC File No. 132 3251 (Sept. 3, 2015), https://www.ftc.gov/system/files/documents/cases/150423nomicmpt.pdf.

89. For a thorough discussion of many widely used mobile device tracking technologies, see generally Ashkan Soltani, *Privacy Trade-Offs in Retail Tracking*, FED. TRADE COMMISSION (Apr. 30, 2015, 11:59 AM), https://www.ftc.gov/news-events/blogs/techftc/2015/04/privacy-trade-offs-retail-tracking.

90. *See* Benjamin D. Kern, *Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 101, 104 (2004)

91. *See* Brendan O'Connor, *Whoops! How Your "Convenience" Broadcasts Your Secrets*, A.B.A. SCITECH LAW, Winter 2014, at 26, 27, *available at http://www.americanbar.org/content/dam/aba/publications/scitech_lawyer/2014/winter/whoops_convenience_broadcasts_your_secrets.authcheckdam.pdf.*

By logging incoming Probe Requests, Nomi obtains: (1) a unique hash value of a device's MAC address (a scrambled value that uniquely identifies the device); (2) the device's manufacturer; (3) the Wi-Fi signal strength; and (4) the dates, times, and locations that the device is observed.[92] According to the FTC's complaint, Nomi collected information about approximately nine million devices between January 2013 and September 2013.[93] Nomi uses this information to provide its clients with "aggregate analytics about consumer traffic patterns, such as the percentage of individuals passing by the store who do not enter, the length of consumer visits, the percentage of repeat customers, [and] the number of consumers visiting other locations within a chain . . . ."[94] From this aggregate data, Nomi's clients can also glean information such as what product displays are popular and how long customers stand in checkout lines.[95] It also allows them "to measure how different retail promotions, product offerings, displays, and services impact consumers. In short, these insights help retailers optimize consumers' shopping experiences, inform staffing coverage for their stores, and improve store layouts."[96]

However, Nomi is just one of many retail analytics providers. A growing number of brick-and-mortars use mobile device signals in order to improve customer experiences and better understand

---

92. Nomi derived the manufacturer of a device from its MAC address and the precise location of a device from its proximity to the sensor observing it. Compl. at ¶ 5, In the Matter of Nomi Technologies, Inc., FTC File No. 132 3251 (Sept. 3, 2015), https://www.ftc.gov/system/files/documents/cases/150423nomicmpt.pdf; *see also* Sarah Kessler, *Here's What Brick-and-Mortar Stores See when They Track You*, FASTCOMPANY (Aug.1, 2013, 8:00 AM) , http://www.fastcompany.com/3015060/heres-what-brick-and-mortar-stores-see-when-they-track-you (providing examples of the information gathered by retail analytics providers). 2

93. Compl. at ¶ 6, In the Matter of Nomi Technologies, Inc., FTC File No. 132 3251 (Sept. 3, 2015), https://www.ftc.gov/system/files/documents/cases/150423nomicmpt.pdf.

94. Thomas C. Bell et al., *FTC Ramps Up Scrutiny of Retail Location Analytics*, 20 CYBERSPACE LAW., June 2015 (citing Compl. at ¶ 7, In the Matter of Nomi Technologies, Inc., FTC File No. 132 3251 (Sept. 3, 2015), https://www.ftc.gov/system/files/documents/cases/150423nomicmpt.pdf).

95. Ashkan Soltani, Remarks at the Federal Trade Commission Seminar: Spring Privacy Series, Mobile Device Tracking 16 (Feb. 19, 2014) (transcript available at https://www.ftc.gov/system/files/documents/public_events/182251/140219mobiledevicetranscript.pdf) [hereinafter Soltani].

96. Dissenting Statement of Commissioner Wright, *supra* note 84, at 1 (footnote omitted).

customer movements and interactions within the business.[97] In fact, this is not much different from the use of information about consumer browsing behavior by online retailers—brick-and-mortars merely seek to generate similar information from physical stores.[98] Even more, the services offered by Nomi are arguably less intrusive than alternatives employed by some brick-and-mortars, such as video cameras coupled with facial recognition software.[99]

Without question, the growing use of location-based retail analytics is motivated by the desire to better understand consumer needs and preferences and improve customer satisfaction.[100] Because the information generated through retail analytics helps brick-and-mortars better understand how to improve customer satisfaction and business operations, it helps them compete more effectively amidst the growth of e-commerce.[101] For example, retailers use information about customer traffic patterns or "heat maps" at a micro level to optimize store environments[102] and at a macro level to determine ideal business locations—by identifying where consumers actually travel.[103] Information about the number of shoppers that enter a particular department and the average time spent therein enables store management to enhance customer service by providing appropriate staffing levels at a particular time and ensuring proper product placement.[104] Tracking technologies also help retailers to reduce customer wait time—ensuring that customers do not spend too long waiting in customer service or checkout lines.[105] Finally, such technologies allow retailers to assess

---

97. Bell et al., *supra* note 94; *see also* Soltani, *supra* note 95, at 8–9.

98. Bell et al., *supra* note 94.

99. *See* Dissenting Statement of Commissioner Wright, *supra* note 82, at 4 n.17 (citing Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES (July 14, 2013), http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html).

100. *See* Ilana Westerman, CEO, Create With Context; James Riesenbach, CEO, iInside; and Glenn Tinley, Founder, Mexia, Remarks at the Federal Trade Commission Seminar: Spring Privacy Series, Mobile Device Tracking 28 (Feb. 19, 2014) (transcript available at https://www.ftc.gov/system/files/documents/public_events/182251/140219mobiledevicetranscript.pdf).

101. *Id.* at 28–29.

102. *Id.* at 34.

103. *Id.*

104. *Id.* at 34, 37–38.

105. *Id.* at 35.

customer loyalty and satisfaction by identifying repeat customers.[106] As one CEO has said: "[T]hese are decisions that affect millions of dollars, in terms of real estate, in terms of leasing, product selection, product mix, and these are the decisions that this data is helping companies to make."[107]

Of course, the misuse of certain types of consumer information can have serious consequences such as identity theft and fraud and cause an array of emotional injuries. Despite the fact that the FTC considers precise geolocation data to be sensitive personal information,[108] the risk of concrete harm does not arise in the case of Nomi's tracking practices. First, no personally identifiable information was acquired, as Nomi applied a cryptographic hashing process to each MAC address to generate a unique, obfuscated number to identify each device.[109] Second, while it is possible for the hashing process to be reversed,[110] doing so would require the cryptographic algorithm—something that only Nomi employees have access to. Moreover, even assuming that someone did reverse the process, they would only have a MAC address and the associated data—information that cannot be used to identify an individual when taken alone. For the information to be matched with an individual, one would have to acquire a record from some other source, such as the mobile phone company, to tie an individual to the de-hashed MAC address. And after taking all of these steps, one would merely know that a person walked through a particular retail establishment at certain dates and times—making it unlikely that financial or emotional harm would result from the data security breach absent extraordinary circumstances.

The true harm implicated in *Nomi* is the market failure that occurs when consumers are deprived of accurate information with which to make informed choices. This issue arose because Nomi's online privacy policy stated that consumers could opt out of tracking

---

106. *Id.*

107. *Id.* at 37.

108. *FTC Testifies on Geolocation Privacy*, FED. TRADE COMMISSION (June 4, 2014), https://www.ftc.gov/news-events/press-releases/2014/06/ftc-testifies-geolocation-privacy.

109. Dissenting Statement of Commissioner Wright, *supra* note 84 at 1.

110. Statement of Chairwoman Ramirez, Commissioner Brill, and Commissioner McSweeny at 1, In the Matter of Nomi Technologies, Inc., FTC File No. 132 3251 (Apr. 23, 2015), https://www.ftc.gov/system/files/documents/public_statements/638351/150423nomicommissionstatement.pdf [hereinafter Statement of Chairwoman Ramirez].

on its website *or at its client's retail locations*.[111] The relevant portion of the policy read:

> With privacy being our number one concern, Nomi pledges to:
>
> 1. Keep each customer's data secure and private.
>
> 2. Never tie any personally identifiable consumer data to a specific device or behavior.
>
> 3. Always allow consumers to opt out of Nomi's service on its website as well as at any retailer using Nomi's technology.
>
> Ultimately, this is all about the consumer. With Nomi, retailers are able to get continuous feedback on the in-store experience and optimize it for consumers.
>
> Click here to opt out of the service.[112]

Nomi's third promise became the focus of the FTC's complaint.[113] The FTC charged that this representation was false or misleading in violation of Section 5 because, while consumers could opt out on Nomi's website, no opt-out was available at its clients' retail locations.[114] The FTC alleged further that the same provision indirectly represented that consumers would be given notice when a retailer was utilizing Nomi's service—that consumers would be told if they were at a store where the tracking technology was in use.[115] This was problematic in part because Nomi's Listen service had approximately forty-five clients at the time of the FTC's complaint,

---

111. Bell et al., *supra* note 94. Nomi's online opt-out process was straightforward: Once a consumer had entered their device's MAC address into Nomi's online opt-out, Nomi would add it to a "blacklist" of MAC addresses for which information would not be stored. Compl. at ¶ 11, In the Matter of Nomi Technologies, Inc., FTC File No. 132 3251 (Sept. 3, 2015), https://www.ftc.gov/system/files/documents/cases/150423nomicmpt.pdf. This was the only way to opt out of tracking. *Id.*

112. Compl. at Ex. A, In the Matter of Nomi Technologies, Inc., FTC File No. 132 3251 (Sept. 3, 2015), https://www.ftc.gov/system/files/documents/cases/150902nomitechexhibitsa-c.pdf.

113. Compl. at ¶¶ 11–13, In the Matter of Nomi Technologies, Inc., FTC File No. 132 3251 (Sept. 3, 2015), https://www.ftc.gov/system/files/documents/cases/150423nomicmpt.pdf.

114. *Id.* at ¶¶ 14–15.

115. *Id.* at ¶¶ 16–17.

but Nomi had not published or otherwise made available to consumers a list of the retailers that use or used the service.[116] Nomi also did not require its clients to post disclosures or otherwise notify customers about their use of Nomi's Listen service—and most clients did not do so.[117]

Thus, as Commissioner Wright explained in his dissenting statement, "The FTC's case against Nomi rested on a single line within its privacy policy."[118] Although Nomi promised that consumers could opt out both online and in stores, Nomi only allowed consumers to opt out of its tracking service online. And by promising that consumers could opt out in stores, Nomi implicitly promised that consumers would be given notice when a retailer was utilizing its services, but Nomi failed to ensure that this occurred.

Although this appears to be a simple case at first glance, the details highlight the challenges faced by retail analytics providers like Nomi. First, Nomi, a small startup company trying to gain a competitive client base, merely contracts to provide its Listen service to retailers and has no control over clients' premises.[119] Thus, it is unlikely that Nomi could effectuate an in-store notice and opt-out requirement.[120] Second, Nomi's assertion that consumers could opt out at retail locations is not entirely false: consumers can "opt out" of Probe Request logging on their own devices by disabling Wi-Fi, turning the device off, or not carrying the devices with them while shopping. Of course, the fact that consumers lacked information about Nomi's client base makes this ability effectively impossible: it would be entirely reasonable for a privacy-conscientious consumer to enter a store with his device and assume that the business did not use Nomi's services in the absence of a posted in-store notice—satisfying the "materiality" requirement of the FTC's test for

---

116. *Id.* at ¶¶ 8–9.

117. *Id.* at ¶ 10.

118. Wright, *supra* note 14, at 9.

119. Dissenting Statement of Commissioner Maureen K. Ohlhausen, In the Matter of Nomi Technologies,
Inc., FTC File No. 132 3251 (Apr. 23, 2015), https://www.ftc.gov/system/files/documents/public_statements/638361/150423nomiohlhausenstatement.pdf (dissenting to the Commission's decision to accept for public comment a consent order with Nomi) ("At the time covered by the complaint, the majority of Nomi's customers were trialing this startup service in a few stores, at most.") [hereinafter Dissenting Statement of Commissioner Ohlhausen 1].

120. *See* Dissenting Statement of Commissioner Wright, *supra* note 84, at 4.

deception.[121] At the same time, Nomi's 3.8% opt-out rate was "significantly higher than the opt-out rate for other online activities," reflecting the effectiveness of Nomi's online opt-out mechanism.[122] In fact, Nomi's Listen service had appeared in a widely publicized story on the front page of *The New York Times* in July 2013,[123] which might have been a factor in its above average opt-out rate.[124] Nevertheless, the success of the online opt-out option and the existence of the technological ability to opt out in stores does not change the possibility that consumers might have been deceived by the privacy policy's language. But this highlights a challenge most businesses face: How can a business provide consumers with a useful (i.e., clear, concise, and complete) privacy policy—and thus provide them real data privacy choices—when utilizing complex technologies?[125]

What is most interesting about this case is that no law required Nomi to develop or publish a privacy policy at all.[126] Because Nomi was acting as a third-party service provider and did not collect personally identifiable information, it had no obligation to post a privacy policy or provide consumers with an opportunity to opt out of the tracking whatsoever.[127] Thus, Nomi could have avoided FTC sanctions by not posting the policy in the first place.

In settlement with the FTC, Nomi agreed to a twenty-year consent order that prohibits it from misrepresenting:

> the options through which . . . consumers can exercise control over the collection, use, disclosure, or sharing of information collected from or about them or their computers

---

121. *See supra* text accompanying notes 81–86 (describing the FTC's test for deceptive acts or practices).

122. Wright, *supra* note 14, at 14.

123. Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. TIMES (July 14, 2013), http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted=all&_r=0.

124. Dissenting Statement of Commissioner Wright, *supra* note 84, at 4 ("Nomi's website received 3,840 unique visitors during the relevant timeframe and received 146 opt outs—an opt-out rate of 3.8% of site visitors. This opt-out rate is significantly higher than the opt-out rate for other online activities.").

125. *See* Hetcher, *supra* note 38, at 177–78; *see also id.* at 186 ("If the notice is too detailed, the reader may become lost or distracted, and if the notice is too pithy, the reader may not receive adequate information.").

126. Wright, *supra* note 14, at 13.

127. Dissenting Statement of Commissioner Ohlhausen 1, *supra* note 119.

> or devices . . . or . . . the extent to which consumers will be provided notice about how data from or about a particular consumer, computer, or device is collected, used, disclosed, or shared.[128]

The consent order also requires that, for five years, Nomi maintain and make available to the FTC upon request information regarding its compliance with the order and all consumer complaints that relate to conduct prohibited by the order.[129]

In the statement of the commissioners in the majority accompanying the consent order, the majority recognized that tracking services such as Nomi's Listen service benefit businesses and consumers by enabling retailers "to improve store layouts and reduce customer wait times."[130] However, the majority went on to explain that such services also raise privacy "concerns" "because they rely on the collection and use of consumers' precise location data."[131] According to the majority:

> consumers visiting stores that used Nomi's services would have reasonably concluded, in the absence of signage and the promised opt-outs, that these stores did not use Nomi's services. Nomi's express representations regarding how consumers may opt out of its location tracking services go to the very heart of consumers' ability to make decisions about whether to participate in these services.[132]

Commissioner Wright disagreed with the FTC's actions on both legal and policy grounds.[133] With respect to the legal grounds, he believed that the element of materiality required in a Section 5 deception claim was lacking given the availability of Nomi's opt-out

---

128. Agreement Containing Consent Order at 2–3, In the Matter of Nomi Technologies, Inc., FTC File No. 132 3251 (Apr. 23, 2015), https://www.ftc.gov/system/files/documents/cases/150423nomiorder.pdf.

129. *Id.* at 3.

130. Statement of Chairwoman Ramirez, *supra* note 110, at 1.

131. *Id.*; *see also* Prepared Statement of the Federal Trade Commission on S. 2171 Before the Subcomm. for Privacy, Technology, and the Law of the S. Comm. on the Judiciary 2 (June 4, 2014), https://www.ftc.gov/system/files/documents/public_statements/313671/140604locationprivacyact.pdf (explaining that the use of sensitive geolocation information "can raise privacy concerns" and providing examples of what "could" occur without providing any examples of actual consumer harm).

132. Statement of Chairwoman Ramirez, *supra* note 110, at 2.

133. Dissenting Statement of Commissioner Wright, *supra* note 84.

mechanism and evidence that it was highly utilized by consumers.[134] Commissioner Ohlhausen agreed with this reasoning, explaining that the evidence "suggests that the privacy policy's partially inaccurate statement harmed no consumers."[135]

According to Commissioner Wright, the FTC's action was also inappropriate in this case in light of the fact that the market seemed to be functioning properly on its own. As he explained in his dissent:

> [M]arket forces already appear to be responding to consumer preferences related to tracking technology. For example, in response to potential consumer discomfort some retailers have discontinued or changed the methods by which they track visitors to their physical stores. Technological innovation has also responded to incentives to provide a better consumer experience, including a Bluetooth technology that provides not only an opt-in choice for consumers, but also gives retailers the opportunity to provide their consumers with a more robust shopping experience. Notably, Nomi itself has responded to these market changes and no longer offers the MAC address tracking technology to any retailer other than its legacy customers.[136]

---

134. *Id.* at 2–4. *See also id.* at 4 ("To presume the materiality of a representation in a privacy policy concerning the availability of an additional, in-store opt-out mechanism requires one to accept the proposition that the privacy-sensitive consumer would be more likely to bypass the easier and immediate route (the online opt out) in favor of waiting until she had the opportunity to opt out in a physical location.").

135. Dissenting Statement of Commissioner Ohlhausen 1, *supra* note 119.

136. Dissenting Statement of Commissioner Wright, *supra* note 84, at 4–5 (citing Amy Hollyfield, *Philz to Stop Tracking Customers via Smartphones*, ABC 7 NEWS (May 29, 2014), http://abc7news.com/business/philz-to-stop-tracking-customers-via-smartphones/83943; Peter Cohan, *How Nordstrom Uses WiFi to Spy on Shoppers*, FORBES (May 9, 2013), http://www.forbes.com/sites/petercohan/2013/05/09/how-nordstrom-and-home-depot-use-wifi-to-spy-on-shoppers; Siraj Datoo, *High Street Shops Are Studying Shopper Behaviour by Tracking Their Smartphones or Movement*, THE GUARDIAN (Oct. 3, 2013), http://www.theguardian.com/news/datablog/2013/oct/03/analytics-amazon-retailers-physical-cookies-high-street; Jess Bolluyt, *What's So Bad About In-Store Tracking?*, CHEAT SHEET (Nov. 27, 2014), http://www.cheatsheet.com/technology/whats-so-bad-about-in-store-tracking.html/?a=viewall; Greg Petro, *How Proximity Marketing Is Driving Retail Sales*, FORBES (Oct. 8, 2014), http://www.forbes.com/sites/gregpetro/2014/10/08/how-proximity-marketing-is-driving-retail-sales).

Both Commissioners Wright and Ohlhausen were most concerned that the FTC's enforcement action against Nomi undermines the agency's own goals to promote consumer information and choice. According to Commissioner Wright, "aggressive prosecution of this sort will inevitably deter industry participants like Nomi from engaging in voluntary practices that promote consumer choice and transparency—the very principles that lie at the heart of the Commission's consumer protection mission."[137] He predicts the FTC's action against Nomi will have the unintended consequence of incentivizing service providers like Nomi to take down their voluntary privacy policies, leaving "consumers and privacy watchdogs with even less information."[138] Commissioner Ohlhausen agreed on this point, citing numerous comments from the public supporting the conclusion that the FTC's application of "a *de facto* strict liability deception standard absent any evidence of consumer harm"[139] "encourages companies to do only the bare minimum on privacy, ultimately leaving consumers worse off."[140]

In fact, subsequent events give credence to the notion that consumers are worse off because of the FTC's action against Nomi. Just as Commissioners Wright and Ohlhausen cautioned, Nomi responded by altering the relevant portion of its privacy policy to read:

> Opt Out of Nomi's Services: You can opt out of having Nomi collect data from your device by clicking here and inserting your MAC address. If you provide us with your MAC address to opt out of our services, we will retain that MAC

---

137. *Id.* at 4.

138. Wright, *supra* note 14, at 15. Wright poses the following rhetorical question: "[I]f a company might face legal action for incorrectly yet harmlessly describe an opt-out feature they did not need to provide in the first place, then why bother?" *Id.* at 16. *See generally* Hetcher, *supra* note 38, at 171 ("When websites take up the FTC's suggestion and seek to implement the fair information practices via privacy policies, the FTC's regulatory grasp is enhanced. Once websites make representations to consumers regarding their practices, the FTC has a claim to jurisdiction if the websites behave differently.").

139. Dissenting Statement of Commissioner Maureen K. Ohlhausen at 1, In the Matter of Nomi Technologies, Inc., FTC File No. 132 3251 (Aug. 28, 2015), https://www.ftc.gov/system/files/documents/public_statements/638361/150423nomiohlhausenstatement.pdf (dissenting to the final consent order) [hereinafter Dissenting Statement of Commissioner Ohlhausen 2].

140. Dissenting Statement of Commissioner Ohlhausen 1, *supra* note 119.

> address indefinitely in order to continue to effectuate your opt-out. For instructions on how to locate your MAC address, see below.[141]

Rather than take the action that the FTC probably intended to induce—adding a requirement that its clients post in-store notices[142]—Nomi simply removed the statement regarding the in-store opt-out option. This leaves consumers in nearly the same position as if the FTC had done nothing at all with respect to Nomi and worse off as to companies not under a twenty-year consent decree, which can choose to post inflexible, take-it-or-leave privacy notices or not post a privacy policy at all.

Having established the legal background, policy considerations, and facts of the FTC's Section 5 action against Nomi, the Article will embark on its law and economics analysis by first providing a brief introduction of pertinent general law and economics principles and then using those principles to analyze the FTC's action against Nomi.

V. LAW AND ECONOMICS ANALYSIS: RATIONAL AND BEHAVIORAL MODELS

Legal rules affect the incentives that businesses and consumers have to engage in various activities, similar to the way that prices impact behavior. In that vein, law and economics applies

---

141. *Our Privacy Policy*, NOMI, http://www.nomi.com/homepage/privacy/.

142. A majority of the commissioners at the FTC, along with FTC staff, have overwhelmingly bought in to the consent model argued for by privacy advocates. For instance, a recent FTC report on The Internet of Things openly minimized the consumer benefits of emerging technologies and made industry recommendations without any cost-benefit analysis. FEDERAL TRADE COMMISSION, INTERNET OF THINGS:
PRIVACY & SECURITY IN A CONNECTED WORLD (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. As one participant in a recent FTC seminar explained, "the privacy community . . . has a consent model where the distinction is consent. And the default for the privacy community is that people don't know sensitive personal information about you, unless you decide to share it with them for purposes that you understand." *See, e.g.*, Seth Schoen, Electronic Frontier Foundation, Remarks at the Federal Trade Commission Seminar: Spring Privacy Series, Mobile Device Tracking 82 (Feb. 19, 2014)
(transcript available at https://www.ftc.gov/system/files/documents/public_events/182251/140219mobiledevicetranscript.pdf). Mr. Schoen went on to express his belief that stores utilizing in-store tracking should put up a sign "to warn people and to give people an opt-out." *Id.* at 93.

microeconomic principles to the analysis of legal rules.[143] It has both positive and normative applications: in a positive application, economic analysis is used to explain the existing legal system and determine whether a particular legal rule produces economically efficient outcomes—whether the legal rule incentivizes conduct that maximizes social welfare.[144] In a normative application, economic analysis is used prescriptively to recommend improvements to the legal system to promote efficiency—promoting policies that maximize social benefits net of social costs.

In order to make normative predictions, law and economics analysis requires the use of assumptions about how individuals react to and change their behavior as a result of changes in law. To satisfy this need, early law and economics scholars imported from economics a series of assumptions about how people respond to incentives, generally known as Rational Choice Theory ("Rational Choice").[145] Rational Choice typically assumes that decision makers have perfect perceptual and computational ability, meaning that they understand the consequences of the alternatives and cannot be fooled by the way options are presented or framed and that they can evaluate complex alternatives accurately and effortlessly.[146] It is also assumed that decision makers have a complete and accurate picture of their environment and practice dynamic coherence, meaning that they act in accordance with an overall optimal strategy, where

---

143. Russel B. Korobokin & Thomas S. Ulen, *Law and Behavioral Science: Removing the Rationality Assumption from Law and Economics*, 88 CAL. L. REV. 1051, 1053 (2000).

144. "Efficiency" refers to the relationship between the aggregate benefits and costs of a situation. A. MITCHELL POLINSKY, AN INTRODUCTION TO LAW AND ECONOMICS 7 (4th ed., 2011). Economists traditionally concentrate on how to maximize efficiency—how to produce the highest level of social welfare. Law and economics is not concerned with equity—the distribution of benefits among individuals; it is concerned with maximizing the welfare of society as a whole. *Id.* at 7 n.5. Throughout this Article, the term "efficiency" is synonymous with Pareto optimality, meaning that no party is made worse off by a social-welfare maximizing outcome and that any movement from that allocation would make at least one party worse off. *Id.* at 7 n.4.

145. Korobokin & Ulen, *supra* note 143, at 1055. Expected utility theory is the most widely used variation of Rational Choice. This theory assumes that decision makers will conduct a cost-benefit analysis when deciding between competing alternatives and select the alternative that maximizes their expected utility—the alternative that produces the greatest expected benefit net of expected costs. *Id.* at 1062–63; *see also* Matthew A. Edwards, *The FTC and New Paternalism*, 60 ADMIN. L. REV. 323, 326–27 (2008).

146. David M. Kreps, *Bounded Rationality*, *in* 1 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 168, 169 (Peter Newman ed., 1998).

optimality is measured according to their fixed and unwavering preferences and in full appreciation of their strategic options.[147] Rational Choice also assumes that decision makers are risk neutral, meaning that they care only about the expected value of a risky situation[148] and are thus indifferent between alternatives with the same expected gain or loss. Finally, it is generally assumed in traditional models that transaction costs—the costs of identifying the parties with whom to bargain, of meeting and bargaining with them, and of enforcing any bargain reached—do not exist such that parties can costlessly negotiate with one another.[149] As these examples indicate, Rational Choice assumes that individual decision making is extraordinarily rational and that individuals will make decisions that maximize their own expected utility.[150] As law and economics developed, however, these standard assumptions became subject to criticism for oversimplifying the factors influencing individual decision making,[151] giving rise to behavioral law and economics.[152]

Behavioral law and economics retains the positive and normative applications of law and economics but loosens the behavioral assumptions employed under Rational Choice. Specifically, it substitutes the assumption that decision makers are extraordinarily rational with a more refined and context-dependent view of how decision makers choose behaviors and actions based on empirical studies of behavior.[153] This movement has led many to substitute Rational Choice with the concept of bounded rationality—the idea that in making decisions, the rationality of individuals is limited by the information they have, the cognitive limitations of their minds, and the finite amount of time they have to make a decision. This approach is reinforced by studies suggesting that individuals often make decisions based on heuristics, or rules of thumb, rather than on "rational" cost-benefit calculations and that

147. *Id.*

148. Expected value represents the magnitude of a potential loss or gain multiplied by the probability of its occurrence. POLINSKY, *supra* note 144, at 31.

149. *Id.* at 13–16. That said, because transaction costs are not low with respect to data collection for retail analytics purposes, the efficient solution is to give the legal right to the party who values it most. In this case, that party is the business or retail analytics provider—meaning that opt-out will generally produce a more efficient outcome than opt in. *See* RUBIN & LENARD, *supra* note 40, at 73.

150. Kreps, *supra* note 146, at 168.

151. Korobokin & Ulen, *supra* note 143, at 1056.

152. *See id.*

153. Edwards, *supra* note 145, at 324.

these different cognitive approaches can lead to different behavior. Such research leads behavioral law and economics scholars to be less confident about the ability of decision makers to make judgments about the world that will enable them to maximize their expected utility. When this occurs, the effect of legal rules can deviate from those identified under Rational Choice, altering positive and normative conclusions. As a result, behavioral law and economics scholars rely on studies demonstrating how cognitive defects lead individuals to make choices contrary to their best interests to support the notion that the law may be legitimately used paternalistically to protect people from themselves.[154]

This Part breaks its analysis of the FTC's enforcement action against Nomi into two sections. The first Section uses traditional Rational Choice. The next Section considers how behavioral considerations, such as the concept of bounded rationality, affect the conclusions that flow from the rational model. However, before doing so, it is helpful to highlight a few overarching concepts that arise throughout the analysis, many of which have been informally discussed already.

Information Privacy and Law and Economics. Law and economics scholars focus primarily on three economic concepts when analyzing privacy law, whether it be the common law of privacy or statutory privacy protections. These concepts are the economics of information, the economics of reputation, and the economics of contracting.[155] A critical concept to law and economics analysis of privacy law is the right of individuals to control the dissemination of personal information.[156] Individuals often seek to conceal discrediting information about themselves, which can deprive the public of information necessary to prevent crime and fraud and ensure that economic resources are allocated efficiently.[157] But individuals also seek to protect embarrassing facts about themselves that offer no benefit in economic transactions and do not prevent crime and fraud. Thus, privacy laws must be designed to limit the ability of individuals to conceal discrediting or economically valuable information about themselves while allowing

---

154. ADAM DEVLIN, FUNDAMENTAL PRINCIPLES OF LAW AND ECONOMICS 397 (2015) (citing Richard Thaler & Cass Sunstein, *Libertarian Paternalism Is Not an Oxymoron*, 70 U. CHI. L. REV. 1159 (2003)).

155. Richard A. Posner, *Privacy*, *in* 3 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 103, 103 (Peter Newman ed., 1998).

156. *Id.* at 104.

157. *Id.* at 105.

the concealment of information that does not yield efficient outcomes when readily available to decision makers. At the same time, information is said to be a "public good" in the sense that once collected it can be used multiple times at almost no cost and without any decrease in value.[158] This "public good" characteristic creates positive externalities because, while data collected about one consumer benefits many others, individual consumers will internalize only the benefits and costs of data collection with respect to themselves.[159] "Thus, at its core, the economics of privacy concerns the tradeoffs associated with the balancing of public and private spheres between individuals, organizations, and governments."[160] Unlike most areas of law analyzed using economic principles, however, there is no unequivocal impact of privacy regulation on social welfare—in some instances, the right to restrict information access will increase welfare; in others, social welfare will increase only if the right to restrict access is denied.[161]

Regulation and Law and Economics. Regulation is one method of controlling harmful behavior—mandating that potential injurers take certain precautions to reduce the risk or extent of harm while allocating residual harms to victims.[162] Public interest theory holds that regulators should pursue maximum economic efficiency, intervening only if there is a market failure—when economies of scale or indivisibilities create a natural monopoly or non-sustainable equilibrium, or if there are externalities or imperfect consumer information.[163] However, regulators face the risk of capture by special interests, which can lead them to enact rules that promote rather than prevent market failures.[164] Therefore, regulation will result in efficient precautionary measures by potential injurers only when tailored to address the specific harmful activity and adequately

---

158. RUBIN & LENARD, *supra* note 40, at xiii, 11.

159. *Id.* at xv.

160. Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy* (Mar. 8, 2016), http://ssrn.com/abstract=2580411.

161. *Id.* at 8; *see also* Posner, *supra* note 155, at 104.

162. POLINSKY, *supra* note 144, at 147–48.

163. Theodore E. Keeler & Stephen E. Foreman, *Regulation and Deregulation*, *in* 3 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 213, 213 (Peter Newman ed., 1998).

164. *See id.* at 213–14. While traditional regulatory capture theory involves agency capture by members of the regulated industry, the FTC's recent enforcement actions suggests that the agency may have been captured by privacy advocates rather than by the entities it regulates. *See supra* note 139.

enforced.[165] That said, even when regulations are correctly fashioned, they will result in excessive participation in the harmful activity by injurers because residual harms are borne by victims—meaning that the price of the underlying good or service will not reflect its full cost to society and too much of it will be consumed.[166] However, because victims bear the cost of any remaining harm, they are motivated to take steps to reduce the likelihood and extent of harm.[167]

Consumer Protection and Law and Economics. Law and economics has played a significant role in the development of consumer protection law.[168] Law and economics scholars emphasize information failure as the primary rationale for regulation and focus on promoting consumer sovereignty.[169] As a result, consumer protection law has traditionally dealt with problems such as fraudulent or deceptive business practices[170] and is designed to level the playing field, so to speak, by putting businesses and consumers in positions of equal bargaining power.[171] Rational Choice holds that consumer protection laws are not necessary absent exceptional circumstances because consumers obtain perfect information at no cost, and rational consumers can perfectly interpret that information.[172] In a non-traditional model, however, not only is accurate information costly for consumers to obtain, it is vulnerable to consumer misinterpretation.[173] For instance, the way that choices are framed may result in irrational consumer behavior.[174] Furthermore, consumers limited by their own bounded rationality will not analyze all information possessed or consider all possible

---

165. POLINSKY, *supra* note 144, at 147.

166. *Id.* at 148.

167. *Id.*

168. Iain Ramsay, *Consumer Protection*, *in* 1 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 410, 410 (Peter Newman ed., 1998).

169. *Id.* (explaining that law and economics scholars generally abhor consumer protection regulation based on distributional goals or paternalism).

170. Peter H. Huang, The Law and Economics of Consumer Privacy Versus Data Mining 2 (May 27, 1998), http://ssrn.com/abstract=94041; *see also* Ramsay, *supra* note 168, at 410 ("The normative goal of consumer sovereignty is the central economic rationale for consumer protection.").

171. Ramsay, *supra* note 168, at 410.

172. *See id.* at 411.

173. *See id.*

174. *Id.* at 412. For instance, consumers are more willing to accept a choice framed as foregoing a gain rather than avoiding a loss. *Id.*

effects of that information.[175] At the same time, "it is often very difficult to distinguish between situations where governments are responding to problems which prevent individuals from reaching a rational judgment and those where government is overruling individual preferences and substituting its own judgment."[176]

Using these concepts, the next two Sections analyze the FTC's enforcement action against Nomi. The goal of the analysis is to determine whether the FTC's test for deceptive acts or practices in the context of privacy policy misstatements produces economically efficient outcomes and to recommend efficiency-promoting improvements to the FTC's framework.

A. A. Rational Model

This Article's law and economics analysis starts with the key economic assumption that a perfectly competitive market exists. In a perfectly competitive market, brick-and-mortars, as well as the companies like Nomi that support their operations, will over time earn zero profits—just enough profit to justify remaining in business rather than shifting capital to other ventures. If stores earn less than this amount, they leave the market. If they earn more, new competitors will enter the market and drive out excess profits.[177]

The outcome of in-store tracking by brick-and-mortars in a perfectly competitive market under Rational Choice is easy to demonstrate. As summarized in Table 1 below, assume that in-store tracking provides a benefit to brick-and-mortars because they can lower prices by an average of $20 per customer, attracting more business through competitive prices and increasing its average margin on sales by $10. Also assume that its highly privacy conscientious customer base would be willing to pay an additional $30 to frequent brick-and-mortars that do not utilize in-store tracking technologies because they would not be subject to location-based data collection.[178] This means that a given consumer has a $20

---

175. *See id.* at 411–12 (citing M.A. Eisenberg, *The Limits of Cognition and the Limits of Contract*, 47 STANFORD L. REV. 211 (1995)).

176. *Id.* at 411.

177. *See* Russell Korobkin, *A "Traditional" and "Behavioral" Law-and-Economics Analysis of Williams v. Walker-Thomas Furniture Company*, 26 U. HAW. L. REV. 441, 448–49 (2004) (citing MICHAEL PARKIN, MICROECONOMICS 240 (6th ed. 2003)).

178. The $30 amount that consumers would be willing to pay to avoid the tracking is not an arbitrary figure. Using the theory of revealed preferences, an individual's willingness to pay is equated with preference, serving as a rough proxy for utility or value. *See* DEVLIN, *supra* note 154. As explained earlier,

expected gain (by realizing lower prices) but a $30 expected loss, yielding a net expected loss of $10. In these circumstances, competitors would operate without utilizing tracking technologies at prices $20 to $30 higher than the original business, and customers would prefer to transact with the competitor, forcing the original business to discontinue its use of the tracking service.

Table 1: Rational Example

Consumer Privacy Sensitivity Level	Retailer's Net Gain	Consumer's Gain	Consumer's Loss	Consumer's Net Gain (Loss)
High	$10	$20	$30	($10)
Moderate	$10	$20	$10	$10
Low	$10	$20	$0	$20

By contrast, suppose that that the business's customers are moderately privacy conscientious and would only be willing to pay an extra $10 to frequent brick-and-mortars that do not utilize in-store tracking technologies and that, as in the last scenario, use of the technology allows the brick-and-mortars to lower prices by $20 per customer. This time, consumers would prefer to transact with the business that utilizes location-based retail analytics to those that do not because doing so increases each consumer's expected utility by $10. In this situation, businesses would certainly continue (or begin) to track consumers' movements throughout their stores because doing so would adhere to their preferences and facilitate continued business operations.

As these two examples highlight, in a world where consumers have perfect information, as Rational Choice assumes, the fact that growing numbers of businesses utilize tracking technologies is evidence that consumers prefer the combination of lower prices and discreet privacy invasions relative to other possible combinations of price and privacy. Further, firms that violate consumer privacy expectations, once this fact is known, will suffer losses of reputation and consumer trust, leading to substantial declines in market share.[179] Thus, in a functioning market, firms will compete by offering better privacy policies or better data collection practices—

many empirical studies have concluded that consumers generally do not value informational privacy more than $30. *See supra* note 43 and accompanying text.

179. RUBIN & LENARD, *supra* note 40, at xvi, 39–43.

assuming that information privacy is a product attribute about which consumers care.[180]

This outcome frequently occurs in the market. On a number of occasions, retailers have discontinued the use of retail tracking technologies, without any government action, following consumer reactions to the practice.[181] Indeed, in response to the New York Times article about Nomi's Listen service, Nomi discontinued that service, which allowed for surreptitious tracking, in favor of a new service utilizing Bluetooth Low Energy that does not track consumers unless they explicitly authorize data collection.[182] Similarly, to ease consumer privacy concerns, industry associations such as the Direct Marketing Association have developed tools[183] that enable consumers to opt out of unsolicited mail advertisements and issue reports about members who are being disciplined for violating the association's code of conduct.[184] Likewise, a growing number of mobile analytics services participate in the Future of Privacy Forum's SmartPlaces tool, which allows consumers to opt out of many services that utilize passive Wi-Fi tracking technologies.[185] Additionally, third-party self-regulatory organizations like TRUSTe and the Better Business Bureau's BBBOnline program rate websites according to how well they protect consumer privacy and permit those that provide sufficient privacy protection to display these privacy-signaling markers online.[186] These results indicate that the market is functioning

---

180. Lenard & Rubin, *supra* note 5, at 20 ("The fact that firms compete less on the basis of privacy than we might expect suggests that consumers are less concerned about privacy practices than other firm attributes.").

181. *See supra* note 135 and accompanying text; *see also* Soltani, *supra* note 89 (describing the industry's move to Bluetooth Low Energy); RUBIN & LENARD, *supra* note 40, at 40–42 (discussing half a dozen instances in which businesses have changed collection and use practices following consumer unrest).

182. *See* Soltani, *supra* note 89.

183. DMACHOICE.ORG, https://dmachoice.thedma.org/index.php (last visited Mar. 25, 2016).

184. CATE, *supra* note 4, at 25.

185. *Opt Out Here*, SMART PLACE PRIVACY, https://optout.smart-places.org/ (last visited Mar. 25, 2016). Future of Privacy Forum has also issued a self-regulatory framework for location-based mobile analytics service providers. *Mobile Location Analytics Code of Conduct*, FUTURE OF PRIVACY FORUM (Oct. 22, 2013), http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf.

186. CATE, *supra* note 4, at 26.

properly, leading to the conclusion that regulation of consumer privacy might not be necessary.

Now consider the effect of imperfect information on the part of consumers. For example, assume that the brick-and-mortar uses a retail analytics provider that has a privacy policy containing a misstatement, meaning that consumers do not have perfect information but instead suffer from information asymmetry.[187] If the consumer frequents the business, he will enjoy the same gain as above—a $20 savings on goods purchased. He is moderately concerned about privacy, but would be willing to pay only $10 more for an option in which his location remains private. In this case, an efficient outcome results despite the market failure caused by his inability to make an informed decision: Knowing that he will save $20 by shopping at the business, he would most certainly do so. However, an efficient outcome does not result in the case of the consumer that values his privacy more highly: Although he enjoys a $20 savings on the goods purchased, he unknowingly loses the $30 value that he attaches to his privacy.

Of course, the retail analytics provider could have avoided the privacy policy misstatement by conducting an annual audit of its policy. But assume that the service provider would pass the audit costs on to its clients, causing the business to forgo the $10 increase in its margin on sales. Because law and economics presumes that both the service provider and the business earn just enough profit to justify continuing operations, the business would likely find a less expensive (but perhaps more invasive) way to understand consumer behavior and preferences before agreeing to pay the service provider's increased rate. In fact, given that the service provider is not legally obligated to maintain a privacy policy,[188] it would probably remove the posted policy in order to keep its client's business—also causing information asymmetry because consumers could not understand the service provider's data collection and use practices.[189]

Thus, the question becomes whether consumers prefer to pay lower prices at stores utilizing retail analytics providers that maintain incomplete and inaccurate privacy policies or, instead, prefer to pay higher prices or suffer from more invasive tracking techniques, such

---

187. RUBIN & LENARD, *supra* note 40, at xv ("Asymmetric information is a form of market failure that occurs when one party to a transaction has more information than the other.").

188. *See supra* notes 126–27 and accompanying text.

189. *See* RUBIN & LENARD, *supra* note 40, at 31.

as being asked personal questions during checkout or being identified through the use of facial recognition software. Although we cannot read consumers' minds, Rational Choice instructs that the answer must be the former; otherwise, brick-and-mortars would increase prices or find new ways to track their customers on their own initiative, and the rapid growth of online shopping would not have occurred.

Finally, assume that the retail analytics provider could not simply remove its posted privacy policy—as would have been the case if the Location Privacy Protection Act of 2015 had become law.[190] This means that the FTC would now have jurisdiction over the service provider and could sanction it for any explicit or implied misstatements contained in the policy (no matter how trivial) through its power to proscribe deceptive acts or practices. While resolving the information asymmetry problem, this time the brick-and-mortar would be forced to raise its prices by $20 to compensate for the inability to utilize the service or pass on to customers the additional $10 it must now pay the service provider to ensure that its privacy policy is free of misstatements. In the case of moderately privacy conscientious consumers, the result would be that: (1) overall social welfare would be reduced because businesses are required to do something that costs them more than the offsetting benefit to consumers; (2) marginal consumers (those for whom it used to be barely worth it to buy the goods and services) will no longer purchase the goods and services and will be worse off because they will enjoy no consumer surplus (value to the consumer less the price paid) rather than some surplus; and (3) brick-and-mortars in a perfectly competitive market will continue to earn "zero profits" per transaction, but fewer transactions will occur, making them worse off. Here, the FTC's consumer-protection efforts ultimately result in reduced consumer welfare.

However, this inefficient outcome would be avoided if the FTC's power were limited to sanctioning unfair methods of competition. In this case, the FTC would be required to show that the act or practice causes (or is likely to cause) substantial injury to consumers that they themselves cannot reasonably avoid and, most importantly, that the

---

190. The Location Privacy Protection Act would have required companies that collect location data from more than 1,000 devices per year to maintain a public website describing the nature of the location information, the purposes for which the information is used and disclosed, the specific entities to which the information is disclosed, and how individual might revoke consent to such collection and disclosure. Location Privacy Protection Act, S. 2270, 114th Cong. (2015).

injury is not outweighed by countervailing benefits to consumers or competition.[191]

For example, again assume that the retail analytics provider could not simply remove its privacy policy. The FTC has discovered a trivial misstatement in the privacy policy that could have been avoided had the service provider conducted the annual policy audit described above. But this time, the FTC would be required to conduct a cost-benefit analysis before bringing an enforcement action, and it would find that consumers who value their privacy moderately would be worse off if action is taken (because of increased prices) but continue to enjoy a $10 net benefit if the status quo persists. Thus, in the case of a moderately privacy conscientious consumer, the FTC could not establish an essential element of an unfairness claim and would be precluded from bringing an action. The retailer would keep prices low and the efficient outcome would result.

This Article will proceed by modifying some of the assumptions used in the examples above and examine how those modifications impact the initial conclusions. Specifically, the following Subsections will consider the role of risk, the incentive problem, and risk shifting. The conclusions of these modifications are summarized at the end of this Section.

1. The Role of Risk

Up to this point it has been assumed that consumers are risk neutral, meaning that "they care only about the expected value of a risky situation—that is, the magnitude of a potential loss or gain multiplied by the probability of the loss or gain occurring."[192] A risk-neutral person is indifferent between scenarios with the same expected gain.[193] In the case of in-store tracking for retail analytics purposes, such risks might include: (1) the use of personal information for purposes other than those for which it was collected; (2) unauthorized sharing of personal information with third parties; (3) misappropriation of personal information; or (4) the collection and use of inaccurate information—denying consumers the benefits they would otherwise enjoy.[194] Expected benefits might include

---

191. *See supra* text accompanying notes 73–80 (describing the FTC's test for unfair methods of competition).

192. POLINSKY, *supra* note 144, at 31.

193. *Id.*

194. *See generally* CATE, *supra* note 4, at 6–7. It is important to recognize that the risks related to Nomi's retail tracking services are quite obscure given

reduced prices, decreased checkout times, or improved customer service.[195]

To illustrate the outcome in the case of a risk-neutral consumer, assume there is a 100% chance that a consumer will pay higher prices by patronizing a business that does not utilize in-store tracking. This yields an expected loss of $20 (100% multiplied by $20). Alternatively, if the consumer shops at a store that utilizes in-store tracking, he faces a 1% chance that his MAC address will be recovered and matched to the retailer's data, resulting in a $2,000 harm. Because this option also yields an expected loss of $20 (1% multiplied by $2,000), a risk-neutral consumer would be indifferent between these choices. Because the retailer obtains a higher margin on sales by utilizing retail analytics, social welfare is maximized if the consumer patronizes the retailer that tracks his movement in the store.

To complicate the analysis, consider the degree to which risk aversion affects the result. Unlike a risk-neutral consumer, a risk-averse consumer cares not only about the expected value of a risky situation but also about the absolute magnitude of the risk.[196] For instance, a risk-averse consumer, unlike a risk-neutral one, would not be indifferent between the certainty of a $20 injury and a 1% chance of suffering a $2,000 injury. Instead, the risk-averse consumer would prefer to suffer the $20 injury with certainty, and in this case, would patronize retailers that do not track his movements within the store, creating an inefficient result from a social welfare standpoint.

In fact, a risk-averse person might be willing to pay more than the expected value of the risk as a premium to avoid the greater potential harm.[197] To demonstrate the effect of a risk premium, assume that a risk-averse consumer is willing to pay $30 to frequent a retailer that will not track his movement to avoid the $20 potential harm from tracking. Here, the benefit of eliminating the risk is $10—the difference between the expected value of the risk and the premium the consumer will pay to avoid it. In this case, the

---

that a consumer's MAC address is stored as an obfuscated hash value. Even if a hacker or disgruntled employee acquired the secret algorithm used to "hash" the MAC address, the hacker or employee would still need to find a way to tie a person to the recovered MAC addresses. *See generally* Lenard & Rubin, *supra* note 5, at 8 (reviewing the concerns raised by privacy advocates, scholars, and public officials over the potential privacy threats of Big Data and concluding that there is no evidence that any of those threats have materialized at this point).

195. *See supra* text accompanying notes 94–107.

196. POLINSKY, *supra* note 144, at 57.

197. *Id.* at 57–79, 83.

consumer's aversion to risk will also lead to an inefficient result. And if enough of the business's customers are risk averse, it would stop using retail analytics because doing so would adhere to consumer preferences and facilitate continued business operations.

Opt-out provisions can help prevent the inefficiency resulting from consumer risk aversion because the ability to opt out of data collection offers risk-averse consumers an alternative to patronizing retailers that do not track their movements within stores. For instance, following the facts from the scenarios above, the ability to opt out will allow risk-averse consumers to enjoy the $20 decrease in prices but avoid the potential $2,000 loss altogether. Of course, if the service provider's privacy policy has a misstatement that renders the consumer's ability to opt out ineffective, then the same information asymmetry problem described earlier will result.[198] However, an accurate privacy policy containing an opt-out provision can also create a new problem: If too many consumers opt out, the retailer will not acquire enough data that, in the aggregate, will help it understand consumer behavior.[199] So again, if enough consumers are risk averse, the retailer will discontinue its tracking practice because it will not be worthwhile to do so, creating an inefficient result.

The last example highlights how opt-out provisions can create market failures because consumers do not internalize enough of the positive externalities to induce optimal consumer decision making.[200] As explained earlier, information collected about one consumer benefits many others, but an individual consumer will only internalize the benefits and costs of tracking with respect to himself.[201] While this problem is not isolated to risk-averse consumers or situations in which the ability to opt out of information collection is available, these factors exacerbate the positive externalities existing in the market. Because consumers will not consider the full social benefits of location-based retail analytics, they will consent to too little data collection, if any, creating an inefficient outcome.

---

198. *See supra* text accompanying note 187.

199. This is precisely why opt-out provisions are preferable to opt-in provisions: Having "do not track" as the default provision means that the business cannot acquire enough data to obtain reliable results unless it first invests in getting a substantial number of consumers to consent to data collection.

200. RUBIN & LENARD, *supra* note 40, at 32.

201. *See supra* text accompanying note 159.

Risk aversion can also affect retail analytics providers—especially with respect to the decision of whether to post a privacy policy. For these parties, such risks include the possibility that too many consumers will opt out or that it will make a misstatement in its privacy policy, impacting consumer trust and risking sanctions by the FTC. The benefits include earning consumer trust through candor, while still acquiring enough data to make meaningful analysis possible. A detailed analysis of risk aversion by retail analytics providers is beyond the scope of this Article, but it is important to note that the FTC's action against Nomi will likely lead risk-averse service providers to remove their privacy policy altogether for the reasons described above.[202]

Another solution to the inefficiency resulting from risk aversion is insurance, which would eliminate the risk in exchange for an insurance premium.[203] Specifically, either the business or the consumer might pay to be completely protected from the $2,000 potential future harm (i.e., the $20 expected future harm). But this may create a moral hazard problem. Specifically, consumers, now protected against any harm that could result from misuse of their MAC address and location data, will have less incentive to take precautions. This means that they will patronize businesses that collect this data more frequently, increasing the probability of loss. Alternatively, the consumer might be willing to allow the business to collect more detailed information, increasing the size of the loss.[204] This leads to the next modification—the incentive problem.

2. The Incentive Problem

The incentive problem for legal rules asks whether and how a law induces decision makers to account for the effects of their behavior on others.[205] In general, the incentive aspect of efficiency will encompass both a care and activity-level decision, and legal rules should be evaluated with respect to their effects on both.[206] Our primary focus—the care decision—refers to behavior "that affects costs and benefits [of others], aside from . . . [the] level of

---

202. *See supra* text accompanying notes 187–191.

203. POLINSKY, *supra* note 144, at 60–61.

204. The same would be true if the business was insured against data breaches: the business would be willing to collect more information from consumers, increasing the monetary harm caused by a security breach.

205. POLINSKY, *supra* note 144, at 165.

206. *Id.*

participation in the [underlying] activity."[207] In the setting of in-store tracking, the legal system must be evaluated in terms of whether it creates incentives for individuals or firms to take the appropriate amount of care with respect to: (1) what type of information is collected; (2) how it is used and stored; (3) whether privacy-conscientious consumers have the ability to opt out of tracking and actually do so; and (4) whether the business's privacy policy is free of untrue or deceptive statements. By contrast, the activity-level decision refers to "the number of individuals or firms that choose to participate in the activity" and the "extent of [their] participation in such an activity."[208] For example, a retailer's activity level corresponds to the number of consumers for which it gathers information. The consumer's activity level corresponds to how many businesses he or she visits and whether he or she exercises the right to opt out of (or opt in to) tracking. Accordingly, the legal system must also be evaluated to determine whether it creates incentives for the parties to engage in the activity to an appropriate extent.[209]

Consider incentives in relation to privacy policies: we know most businesses that collect consumer information post privacy policies stating what they can and cannot do with the information. But if there is no legal enforcement of these policies, businesses have little incentive to comply with them, and they become false promises upon which consumers rely—assuming that violating the policy does not otherwise impact profits by causing, for example, loss of reputation and consumer trust.[210] Naturally, strong penalties for privacy policy violations encourage compliance, but excessive penalties might also discourage beneficial data collection or the posting of a privacy policy in the first place.

For example, assume that the FTC will commence an enforcement action against any business that posts a privacy policy containing a misstatement. The business will take precautions to avoid intentional or unintentional misstatements—presumably by having internal controls ensuring that its data collection and use practices align with statements in the policy. At the same time, however, if the business is not legally obligated to post a privacy policy, then it also has an incentive not to post the policy from the outset.[211] It will collect information without notifying consumers,

---

207. *Id.*

208. *Id.*

209. *Id.* at 166.

210. *See generally* Hetcher, *supra* note 38.

211. *See supra* text accompanying notes 187–88.

meaning that consumers cannot determine whether visiting that business maximizes their own utility because they will be unable to assess the expected loss accurately. Furthermore, the business can (and probably will) collect more information—both qualitatively and quantitatively—because consumer preferences will not influence its decision.

Instead, assume that retail analytics providers are legally required to post a privacy policy before collecting consumer information. This solves the information asymmetry problem described above[212] while maintaining the business's incentive to maintain an accurate privacy policy. But now, businesses must determine whether the cost of maintaining a misstatement-free policy is worth the benefits derived from information collection. For example, as summarized below in Table 2, assume that a business receives $4 million in benefits from analyzing consumer information. It must incur $2 million in costs to ensure that the policy has no misstatements, $1 million to ensure that there are no misstatements that will injure consumer welfare, or no compliance costs whatsoever.[213] Assume further that consumers will enjoy a $2 million net gain if data collection and analysis occurs but that half of all compliance costs will be passed on to consumers. Finally, consumers will suffer $1.5 million in losses if the policy has a harmful misstatement.

Table 2: Effect of Business Compliance Efforts

	Business's Gross Gain	Compliance Cost	Business's Net Gain (Loss)*	Consumer's Net Gain (Loss)**	Net Social Gain (Loss)
No misstatements	$4M	$2M	$3M	$1M	$4M
No harmful misstatements	$4M	$1M	$3.5M	$1.5M	$5M

212. *See supra* text accompanying note 187.

213. These figures are supported by the Gramm-Leach-Bliley Act's privacy notice requirement, for which it was estimated that the "average compliance costs was $1.37 per customer, with total estimated compliance costs per bank ranging . . . from as little as $1,000 to more than $2 million." *Examination of the Gramm-Leach-Bliley Act Five Years After Its Passage Before the H. Comm. on Banking, Hous., and Urban Affairs*, 108th Cong. 46 (2004) (Statement of Harry P. Doherty, Vice Chairman of the Board, Independence Cmty. Bank Corp.). The total costs of that legislation "has been estimated at between $2 and $5 billion per year." MacCarthy, *supra* note 38, at 435.

Multiple harmful misstatements	$4M	$0	$4M	$500,000	$4.5M
No privacy policy	$0M	$0	$0	$0	$0
* Calculated by subtracting 50% of the compliance costs from the business's original gain. ** Calculated by subtracting 50% of the compliance costs from the consumer's original net gain.					

In this case, because the FTC will bring an enforcement action to proscribe the deceptive act or practice regardless of the impact on consumer or social welfare, the business must incur the $2 million compliance expenditure to avoid strict liability—creating an inefficient result. Alternatively, brick-and-mortars will avoid the use of retail analytics altogether, also leading to an inefficient result.

By contrast, consider the outcome if the FTC's power was limited to sanctioning unfair acts or practices. Because the FTC would be required to balance the costs and benefits of sanctions before bringing an action, it would be precluded from doing so for trivial misstatements or omissions.[214] Now, the business would choose to incur the $1 million expenditure to ensure that no potentially harmful misstatements exist in its privacy policy but continue to collect consumer information, leading to an efficient result. This leads to the conclusion that the FTC should utilize its Section 5 authority only when a business makes a harmful misstatement in its privacy policy and should consider whether its actions create an environment incentivizing inefficient market outcomes.[215]

3. Risk Shifting

The risk-allocation question asks whether a particular legal rule distributes risk efficiently among the relevant individuals or firms.[216] Law and economics holds that, "if the risk cannot be (or is not)

---

214. *See supra* text accompanying notes 73–80 (describing the FTC's test for unfair acts or practices).

215. It is important to consider this conclusion alongside the facts of *Nomi*: Nomi had a higher-than-average 3.8% opt-out rate, supporting the conclusion that very few consumers, if any, were actually impacted by the misstatement in its privacy policy because most consumers who wanted to opt out did so online after reading the policy. Further, any consumers affected by the misstatement will suffer harm only if a data breach occurs and the MAC addresses are tied to their identities.

216. POLINSKY, *supra* note 144, at 166.

eliminated, then it should be allocated among the relevant individuals or firms according to their relative aversion to risk."[217] This might mean that the risk should be shared among the parties or shifted entirely to one of them.[218] In short, the legal system should be evaluated in terms of how well it promotes the optimal allocation of risk.

In the case of consumer information and the risk of data misuse, companies face many post-breach exposure points, such as fines and class-action lawsuits. In addition to numerous federal laws and regulations, most states have liability schemes to sanction and hold accountable businesses that mishandle consumer information.[219] Even more, the FTC has acted on numerous occasions to penalize companies that fail to take reasonable measures to protect customer data.[220] For instance, the FTC might sanction a company with inadequate data security for engaging in an unfair or deceptive act or practice under Section 5.[221] Even more, companies that fail to care for consumer information properly will suffer losses of consumer trust and reputation, affecting the bottom line, and possible discipline by trade associations and self-regulatory organizations.[222] However, consumers also face a magnitude of post-

---

217. *Id.* at 166–67.

218. Other theories propose that "liability should attach to the 'cheapest cost avoider'—the party best suited to make the cost-benefit analysis between accident costs and accident avoidance costs and to act on that analysis." Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 284 (2007) (quoting Guido Calabresi & Jon T. Hirschoff, *Toward a Test for Strict Liability in Torts,* 81 YALE L.J. 1055, 1060 (1972)). Under a "cheapest-cost avoider" strategy, businesses constitute the cheapest cost avoiders compared to consumers whose information might be collected. *Id.* Businesses have distinct informational advantages about its data collection and use practices while consumers cannot identify misstatements in a privacy policy. Thus, businesses are in the best position to make decisions about the costs and benefits of data-collection practices and the accuracy of their privacy policies.

219. Today, forty-seven states have a breach-notification law. SOLOVE & SCHWARTZ, *supra* note 1, at 952.

220. *Id.* at 975. There are several sources of authority that the FTC uses to regulate data security, including the Gramm-Leach-Bliley Act (and the FTC's Safeguard's Rule), FTC Section 5, the Children's Online Privacy Protection Act, and the Fair Credit Reporting Act. *Id.* at 975-76.

221. *Id.* at 975. Although early FTC enforcement actions involved companies that failed to live up to promises made about data security in privacy policies, the FTC has more recently found certain data security practices to be "unfair" regardless of the statements made in privacy policies. *Id.*

222. *See supra* text accompanying notes 181–86.

breach costs, such as identity theft.[223] Other costs might include emotional distress, loss of credit, or the expenditure of time and money to prevent future fraud.[224] In fact, 18% of online Americans have been victims of a data breach.[225] Approximately one-quarter of these records are used to commit fraud.[226] At the same time, it is critical to understand that businesses will usually suffer the more severe financial injury following a data breach[227] and that other laws are in place to protect consumers from and compensate them for concrete injuries suffered.[228]

In the case of preventing the unauthorized collection and use of consumer data, one might think that consumers are more risk averse than businesses. If this were the case, however, why wouldn't a larger percentage of consumers read privacy policies? Perhaps this counterintuitive result occurs because, under the FTC's seemingly strict liability regime in which any misstatement in a privacy policy is actionable as a deceptive act or practice, the risk is placed upon the business rather than the consumer. In other words, the threat of a Section 5 enforcement action shifts the risk of harm resulting from a privacy policy misstatement to the business, which can face liability even if no consumers rely on it, no actual harm results, and the benefits to consumers outweigh the harm it causes. But taking this with the fact that consumers have adequate redress through other laws in the event of harm gives rise to a moral hazard problem: consumers have very little incentive to take precautions, meaning they will more frequently transact with retailers that collect

---

223. *See generally* SOLOVE & SCHWARTZ, *supra* note 1, at 949 (chapter on data security).

224. *Id.* at 968; *see also* Daniel J. Solove, *Privacy and Data Security Violations: What's the Harm?*, TEACHPRIVACY (July 2, 2014), https://www.teachprivacy.com/privacy-data-security-violations-whats-harm.

225. SOLOVE & SCHWARTZ, *supra* note 1, at 950 (citing Mary Madden, *More Online Americans Say They've Experienced a Personal Data Breach*, PEW RES. CTR. (Apr. 14, 2014), http://www.pewresearch.org/fact-tank/2014/04/14/more-online-americans-say-theyve-experienced-a-personal-data-breach/).

226. *Id.* (citing LEXISNEXIS TRUE COST OF FRAUD STUDY: MERCHANTS STRUGGLE AGAINST AN ONSLAUGHT OF HIGH-COST IDENTITY FRAUD AND ONLINE FRAUD 6 (2013)).

227. *Id.* at 950–51 (discussing the costs of data breaches on companies: ChoicePoint ($15 million in FTC fines alone); LifeLock ($12 million in FTC fines alone); and Sony ($15 million class-action settlement and $171 million in overall costs)).

228. RUBIN & LENARD, *supra* note 40, at 8, 34; *see also* Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 121–25 (2002).

information about them, increasing the probability of loss, and they will unknowingly allow businesses to collect more detailed information, increasing the size of the loss.[229]

By contrast, if businesses were held responsible only for misrepresentations that could cause real consumer harm or that satisfied the cost-benefit test used in unfairness claims, more of the risk of retail tracking would be placed upon consumers. In this case, consumers would have proper incentive to understand a business's privacy practices and select the economically efficient choice to opt out of overly invasive tracking or avoid businesses that engage in such practices. Such a system does not place all of the risk on consumers but avoids the moral hazard problem and fosters an efficient outcome.

4. Summary of the Rational Model

The conclusions flowing from the rational model can be summarized as follows: In a competitive market where all decision makers have all the relevant information and can effortlessly and perfectly analyze that information in the decision-making process, FTC regulation is not necessary. In this case, consumers understand all of the potential harms and benefits, meaning that companies have an incentive to properly balance consumer privacy expectations with the benefits of data collection. If they fail to do so, consumers will be drawn to competing businesses that achieve the proper balance. In fact, a rational model leads to the conclusion that unnecessary regulation, or regulation that is not justified by a cost-benefits analysis, will produce economic inefficiencies. Further, inefficient outcomes will result from the FTC's deceptive act or practice regime when the agency sanctions a business for trivial privacy policy misstatements where individual consumer harm is not shown and the net social gains of data collection are greater than the net social losses. Thus, the rational model has also demonstrated that irrespective of information asymmetry on the part of consumers, a cost-benefits prerequisite to all Section 5 claims is more likely to generate economically efficient outcomes when compared to the FTC's current strict liability regime for deceptive acts or practices. This is particularly true given the positive externalities that exist with respect to location-based retail analytics coupled with the potential for consumer risk aversion.[230] While individual consumers will not

---

229. *See also supra* text accompanying note 204.

230. Normatively, regulators like the FTC should be cognizant of the positive externalities affecting consumers when analyzing consumer privacy

include the benefits that the disclosure of their personal information provides to others, the FTC is well suited to perform a complete cost-benefits analysis.

Based on this, it is highly unlikely that the FTC's deception claim against Nomi produced an efficient outcome from a social welfare standpoint. Apart from the theoretical and speculative harms identified by the FTC, there was no showing that the misstatement in Nomi's policy created a risk of consumer injury.[231] Further, though the misstatement created an information asymmetry problem, the evidence of Nomi's above average opt-out rate following the highly publicized *New York Times* article detailing its practices and its decision to move to a more privacy enabling tracking technology indicates that the market is functioning properly.[232] In fact, because retail analytics providers like Nomi are not legally required to maintain a privacy policy, service providers not under a twenty-year FTC consent decree are now motivated to remove their posted policy rather than internalize the high compliance costs necessary to avoid the FTC's strict liability regime. Others might leave the market completely. Thus, overall social welfare is likely to have been reduced rather than improved because businesses are required to do something that costs them more than the offsetting benefit to consumers.

To prevent outcomes like *Nomi*, the FTC should add a cost-benefit analysis to its deception framework. As demonstrated earlier, the FTC's current framework will produce inefficient outcomes in some cases—particularly where the harm to consumers is non-existent or inconsequential or the benefits to consumers are substantial. The FTC plays a critical role in reducing the information asymmetry problem and ensuring that companies live up to the promises they make in their privacy policies. However, because the market can adequately handle those that fail to meet consumer privacy expectations, the FTC's best role is that of a "privacy watchdog" that can inform the public as well as state and federal lawmakers about the realities of data collection and use practices

---

issues. Specifically, the agency should not rely exclusively on consumer surveys when making consumer privacy decisions because many consumers will undervalue the societal benefits of data analytics. A failure to account for this externality will cause the FTC underestimate consumer losses and take action not called for by the economic realities of the situation. But businesses and data aggregators can help overcome this challenge by working to inform consumers and the FTC about the wide-ranging benefits of data analytics.

231. *See supra* text accompanying notes 109–111.

232. *See supra* text accompanying notes 181–86.

and of the causal connection between privacy and data collection. Instead, the FTC's overzealous response to Nomi's privacy policy misstatement is likely to reduce the availability of information about business data collection and use practices, preventing watchdogs such as the FTC from alerting the market of bad actors. Adding a cost-benefit test like the one used in the agency's unfairness framework will prevent these negative outcomes but ensure businesses have sufficient incentive to avoid conduct that risks concrete consumer injuries that are not outweighed by countervailing benefits to consumers or competition.

B. Behavioral Model

The conclusions in the last Section's traditional analysis depend on the assumption that the parties have all the information necessary to make a decision. They also depend on the assumption that the parties will properly evaluate all of that information in the decision-making process to make the choice that maximizes their expected utility. For example, consumers are assumed to have a reasonable opportunity to discover and understand the tracking technology, the service provider's privacy policy, and the method to opt out of tracking in order to determine the marginal value of transacting with a business that does not utilize location-based retail analytics. If a competing business were to offer goods or services without utilizing in-store tracking at a correspondingly higher price, it was assumed that consumers would choose the price–term combination that will maximize their expected utility. The same was expected if competitors offer goods and services without in-store tracking but instead utilize some other data collection method or charge higher prices.

However, many people do not approach decisions with the scrupulousness and caution achieved by considering all relevant information and comparing the trade-offs of various choices.[233] Instead, behavioral studies have revealed several forms of deviations from rationality that affect decision making. For instance, most people use an ad hoc decision-making process that economizes time and effort—focusing on the most important benefits and risks and the associated probabilities of those attributes.[234] In fact, studies show that people generally do not consider many more than five factors

---

233. Korobkin, *supra* note 177, at 459 (citing JOHN W. PAYNE ET AL., THE ADAPTIVE DECISION MAKER 29–30 (1993)).

234. *Id.*

when making a decision.[235] Further, even if a person has complete information to allow him to calculate the expected utility of a particular decision, he might misinterpret that information because of cognitive limitations, biases, or limited opportunism.

For instance, the predictions and conclusions of the rational model are severely undermined if consumers do not account for in-store tracking when deciding whether to patronize one store versus another. If this occurs, businesses will not face market pressure to discontinue the practice if it is inefficient because it will not drive away customers and discontinuing it will not attract new customers. Further, businesses would face market pressure to utilize some form of in-store tracking even if it reduced social welfare because its competitors would do so, reduce costs, and gain a competitive advantage by using those savings to lower prices or provide other services that consumers would account for when making decisions.

To understand the reasoning that leads to this conclusion, as in the rational model, assume that a complete and accurate disclosure regime would increase the cost of providing goods and services to brick-and-mortars by $10 per customer. This time, however, assume that consumers are ignorant of the practices (whether or not this ignorance is intentional or otherwise attributable to the consumer) and that the expected loss to a consumer for giving up his information is $30. This time, even if competitors offered services without utilizing location-based retail analytics, consumers would still prefer to patronize the business that collects their location data, even though the decision does not maximize their expected utility. As a result, businesses would choose to collect consumer location data because doing so will improve rather than hinder continued business operations.

By contrast, assume that the decision to not collect consumer location data would increase the business's costs by $10 per transaction and that a consumer is ignorant of the data collection and the associated $30 expected loss. This time, however, also assume that the FTC asserted that the practice was unfair or deceptive—perhaps because the retail analytics provider has a misstatement in its privacy policy. This time, the retailer would be forced to raise prices to compensate for the inability to utilize the tracking technology or to ensure that the service provider's privacy policy is free of harmful misstatements, but the $30 harm is prevented. Because consumers are not ignorant of price, they would

---

235. Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203, 1227–29 (2003).

include this in their decision-making process and patronize the business that provides the most value at the lowest price, avoiding an economically inefficient outcome. Therefore, as this example demonstrates, when lawmakers can detect behavioral characteristics that affect the accuracy of the results flowing from the rational model, they may be able to enact laws that induce or require decision makers to act in a better way.

The remainder of this Section expands on these principles by considering four behaviors that can cause consumers to depart from utility-maximizing decision making in order to analyze the efficiency of the FTC's enforcement action against Nomi. Specifically, it considers hyperbolic discounting, cognitive biases, limited opportunism, and the zero price effect. A summary of the conclusions flowing from these behaviors is provided at the end of the Section.

1. Hyperbolic Discounting

Even where individuals have access to complete information and can successfully calculate optimization strategies for their decisions, they might still deviate from the utility-maximizing strategy. One problem that can cause the rational model to generate inaccurate predictions is hyperbolic discounting—a scenario in which an individual prefers immediate benefits to delayed benefits.[236] Research in psychology, for example, has shown that some individuals incorrectly predict their future preferences and often suffer from self-control problems such as the tendency to trade off costs and benefits in ways that damage their future utility in favor of instant gratification.[237] For instance, when offered the choice between $100 now and $200 a year from now, many people will choose the immediate $100. However, given the choice between $100 in five years and $200 in six years, nearly all people will choose $200 in six years, even though that is the same choice seen at five years' greater distance.

To demonstrate how this might occur in the case of location-based retail analytics, assume that data collection will provide a $15 net gain to the consumer whereas seclusion will provide a $20 net gain. Depending on how long the consumer must wait to realize the benefits of seclusion, the consumer might prefer the immediate

---

236. Christine Jolls et al., *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471, 1539 (1998).

237. Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Decision Making*, 3 IEEE SECURITY & PRIVACY 26 (2005).

satisfaction of lower prices and decreased checkout times fostered by data collection over the long-term benefits of seclusion. As a result, the consumer will not make the rational, utility-maximizing choice.

This outcome is quite relevant in the case of Nomi's privacy policy misstatement. Specifically, assume that Nomi's clients had posted notices about the in-store tracking and allowed consumers to opt out at retail locations. Would consumers have used this opt-out option? Behavioral studies on hyperbolic discounting suggest that they would not. Instead, consumers, upon entering the store and seeing the notice, would prefer to enjoy the instant gratification of lower prices and decreased checkout times rather than take the additional time to opt-out of tracking and enjoy the future benefits of seclusion. These studies support Commissioner Wright's argument that any consumers who really wanted to opt out would have done so online when they read Nomi's privacy policy.

Nevertheless, regulation might be appropriate when hyperbolic discounting leads decision makers to make choices that do not maximize their expected utility. In the case of location-based retail analytics, regulators could consider actions that will correct irrational decision making. Because consumers are not ignorant of price, one way regulators could correct consumer shortsightedness that leads to bad choices is to "tax" businesses that collect consumer location information. Businesses will pass the costs on to consumers, and consumers will include these costs in their decision-making process. In order to determine the appropriate amount to tax these businesses, however, regulators must understand the costs and benefits that arise from the underlying practice—something that the FTC routinely fails to do and is not required to do under its deception framework. Therefore, while regulatory action might be called for, an FTC deception claim is not well suited to properly correct consumer behavior.

For example, assume that location-based retail analytics provides a $15 net gain to consumers and that seclusion provides them with a $20 net gain. However, a number of consumers attach a $10 "premium" to the instant gratification achieved by decreased prices and checkout times and, therefore, erroneously believe that consenting to data collection will maximize their utility. In order to correct this behavior, the FTC could take action to effectively reduce the gain of data collection to $5. In this case, the consumer would make the proper decision to practice seclusion despite the $10 premium caused by hyperbolic discounting. In order to do so, however, the FTC would have to conduct its own cost-benefits

analysis to determine the gains and losses of data collection and seclusion as well as the value of the premium that consumers attach to immediate satisfaction.

2. Cognitive Biases

In addition to assuming that parties account for and compare all relevant attributes of alternatives, traditional law and economics assumes that parties will make correct factual judgments in determining the expected utility of alternatives to the extent information necessary to make such determinations is available.[238] For instance, suppose that a person is asked to choose between a guaranteed $1,000 and a coin toss that will pay $2,000 if heads and $0 if tails. Under a rational model, it is assumed that he can and will compare the guaranteed outcome to the risky outcome and that he knows that the chance of the coin toss coming up heads is 50%. If he believes the chance of heads coming up is 99%, the prediction as to his choice will be different than if he knew that the true probability was 50%, and there would be far less certainty that his choice of the flip rather than the guaranteed payoff would maximize his expected utility.

Behavior literature has identified at least two judgment biases that support the notion that many consumers will fail to understand the true costs of location-based retail analytics. First, consumers may suffer from optimism bias, meaning that they will sometimes underestimate the likelihood of a risk happening to them and overestimate their ability to prevent a risk from occurring.[239] For example, suppose that consumers have a 1% chance of being negatively impacted by in-store tracking. If a particular consumer believes that he has more control over unforeseen injuries than he really does and thus incorrectly believes the chance of loss is only .01%, he might prefer in-store tracking. This would allow a retailer to keep prices $20 lower than they would otherwise be, even if the consumer's objective expected utility would be higher if the retailer discontinued the practice and raised prices.

---

238. Korobkin, *supra* note 177, at 460.

239. *Id.* at 461 (citing Christine Jolls, *Behavioral Economics Analysis of Redistributive Legal Rules*, 51 VAND. L. REV. 1653, 1659 n.22 (1998); Dan Stone, *Overconfidence in Initial Self-Efficacy Judgments: Effects on Decision Processes and Performance*, 59 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 452, 452 (1994); J. Crocker, *Biased Questions in Judgment of Covariation Studies*, 8 PERSONALITY & SOC. PSYCHOL. BULL. 214 (1982); E.J. Langer, *The Illusion of Control*, 32 J. PERSONALITY & SOC. PSYCHOL. 311 (1975)).

Therefore, optimism bias may cause consumers to underestimate the risk-adjusted expected value of patronizing businesses that utilize in-store tracking, and the behavior of those consumers could encourage businesses to continue the practice even though the expected costs known to rational consumers beforehand exceed the social benefits. This practice would be inefficient and would make consumers worse off because the expected cost to them will exceed the accompanying price reduction that data collection will provide. Similar to the hyperbolic discounting problem, regulation could correct this behavior by taxing businesses that collect consumer location information. Businesses will pass the tax on to consumers, and consumers will account for these added costs when making decisions to reach the utility-maximizing conclusion. However, an FTC deception claim is also not the proper regulatory action in the case of optimism bias because such action would not require the agency to determine the appropriate amount to tax these businesses—this can only occur when the FTC understands the costs and benefits that arise from the underlying practice.

A different bias can arise when a decision maker feels endowed with a particular right—the so-called "status quo bias"[240] or "endowment effect."[241] This is a particular type of loss aversion that runs counter to the Coase Theorem's key principle that markets will efficiently allocate resources regardless of their initial assignment when there are no transaction costs.[242] Contrary to the Coase Theorem, behavioral studies show that people typically dislike losing a unit of certain value more than acquiring an identical unit and thus often place a value premium on products they own over equivalent ones that they do not possess.[243] In other words, the value that a person places on an object may increase sharply once he owns (or believes he owns) it.

The endowment effect can certainly manifest in the case of consumer information privacy.[244] Without a doubt, an opt-in regime effectively shifts information ownership to consumers. But an opt-out regime has a similar effect when the opt-out right is exercised. Indeed, because consumers can opt out of tracking without monetary consideration of any kind, consumers often feel that they

---

240. DEVLIN, *supra* note 154, at 404.

241. Richard Thaler, *Toward a Positive Theory of Consumer Choice*, 1 J. ECON. BEHAV. & ORG. 39, 44 (1980).

242. *See* DEVLIN, *supra* note 154, at 404.

243. *Id.*

244. *See* Acquisti et al., *supra* note 40.

own "their" information. In fact, while consumers do not own their own personal information in a legal sense,[245] behavioral research has found that many individuals feel endowed with their personal information, which causes substantially different valuations of the privacy of personal data.[246]

To illustrate the impact of the endowment effect, first assume that a consumer attaches a $10 value to information for which the law does not attach property rights. This value represents the expected loss the consumer will suffer if the information leaves his exclusive possession or, said differently, the amount he would be willing to pay to avoid the privacy intrusion. If a retailer collects this information it will enjoy a $10 gain and the consumer will enjoy a $20 gain. In this case, the retailer will collect the information, and both the retailer and the consumer will be better off—the efficient outcome occurs.

By contrast, as supported by behavioral studies, a consumer will attach a greater value to his information when he feels that his right to exclusive possession is protected by law, which can lead to an inefficient outcome. For example, now assume that the consumer lives in a jurisdiction that has enacted a mandatory opt-in prerequisite to third-party information collection. As a result, the consumer now attaches a $30 value to his privacy, representing the amount that he would be willing to accept to relinquish his exclusive right to the information. Here, the consumer will not consent to data collection because he effectively "owns" his personal information and demands more to "lose" it. Despite the fact that the consumer will actually enjoy a greater, real gain by consenting to information collection, he will refuse to do so because of the $20 premium he attributes to the information, resulting in an economically inefficient outcome.

Unlike the case of optimism bias, regulation of retail analytics providers or retailers themselves will not correct irrational consumer behavior arising from the endowment effect. However, regulators like the FTC should be mindful of this problem when analyzing

---

245. *See* H. Brian Holland, *Privacy Paradox 2.0*, 19 WIDENER L.J. 893, 896 (2010) ("Individuals hold no property rights in their personal information. Rather, individuals control their rights in that data only to the extent that they are able to conceal or manage its disclosure, just as the information seeker may use reasonable means to collect personal data outside of the consent market." (footnotes omitted)).

246. Acquisti et al., *supra* note 40, at 252 (finding that consumers are five times more likely to reject cash offers for their data if they believe their privacy is protected by default than if they did not have such a belief).

consumer privacy harms. Specifically, the FTC must understand that it cannot rely solely on consumer surveys when making consumer privacy decisions because many consumers will attach a premium to rights or property to which they feel entitled. If the FTC fails to do so, it may overestimate consumer losses and take actions not called for by the economic realities of the situation.

3. Limited Opportunism

The concept of opportunism has an important role in economic analysis. In short, opportunism means "self-interest seeking with guile,"[247] involving some kind of deliberate deceit facilitated by information asymmetry. For instance, opportunism could occur when a retail analytics provider includes a deliberate misstatement in its privacy policy or purposefully fails to fulfill the promises it has made in the policy. As explained above, however, businesses are adequately incentivized to minimize opportunism because of the loss of reputation and consumer trust that consistently occurs when the market learns of the deception.[248]

Contrary to the traditional concept of opportunism, behavioral literature suggests that economic negotiations, such as the negotiations that occur regarding the terms under which consumers will permit information collection, function as a "laboratory for the construction of relationships" rather than a mere dialogue over the terms of a transaction.[249] This literature has found that while some parties seek to develop a trusting relationship to secure efficiency gains, others are predisposed to seek trusting relationships.[250] A predisposition to seek trusting relationships, however, gives rise to limited opportunism, or the belief that others are honest, make good-faith attempts to behave as promised, and do not take advantage of others even when given the opportunity to do so.[251] Indeed, this characteristic may be particularly prevalent in the case of location-based retail analytics in light of a recent study finding that most consumers believe the existence of a privacy policy means that their

---

247. Oliver E. Williamson, *Opportunism and Its Critics*, 14 MANAGERIAL & DECISION ECON. 97, 97 (1993).

248. *See supra* note 179 and accompanying text.

249. G. Richard Shell, *Opportunism and Trust in the Negotiation of Commercial Contracts: Toward A New Cause of Action*, 44 VAND. L. REV. 221, 252–53 (1991).

250. *Id.* at 253.

251. RODERICK M KRAMER & TOM R. TYLER, TRUST IN ORGANIZATIONS: FRONTIERS OF THEORY AND RESEARCH 303 (1996).

personal information is protected.[252] These naïve bargainers who expect trustful cooperation will often be victimized, leading to inefficient economic outcomes.[253]

For example, assume that a consumer who attaches a $30 value to his information privacy reviews the privacy policy of a retail analytics provider containing the untrue statement that consumers may opt out of tracking at store locations. While the consumer can opt out online, he does not do so because the service provider has not provided a client list—such that he prefers to opt out only when he learns that it is necessary to do so (upon seeing a data collection notice in a store he actually visits). Although the consumer enjoys a $20 gain by patronizing stores that engage in data collection, he ultimately suffers a $10 net loss in utility because of his erroneous belief that the service provider would follow through on its promise.

While limited opportunism is likely to decline with respect to information privacy as growing numbers of consumers learn of the widespread reliance on Big Data by both government and business, regulation might provide an interim solution. As previously explained,[254] an action by the FTC sanctioning the service provider's deceptive conduct will induce it to not make misstatements in its privacy policy and force it to live up to its promises. In some instances, a deception claim will foster an efficient outcome. However, sanctioning broken promises will not always lead to efficiency unless the FTC engages in a cost-benefits test like the one that it must undertake when sanctioning unfair methods of competition. That said, if a cost-benefits assessment is required, then FTC enforcement of privacy policies would offset limited opportunism by consumers while promoting economically efficient behavior.

4. Zero Price Effect

Consumer decision making can also deviate from the rational model because of the so-called "zero price effect." Specifically, observations of the zero price effect suggest that traditional cost-benefit models cannot account for the psychological effect of a free

---

252. Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RES. CTR. (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/ (finding that 52% of Internet users believe that privacy policies ensure the confidentiality of their personal information.).

253. Shell, *supra* note 249, at 273.

254. *See supra* Section V.A.

product. This arises because when individuals make decisions about a free product, they do not just subtract costs from benefits but instead ascribe additional, intrinsic value to the product and thus value it more highly than the real benefit received.[255] While this theory is not implicated by location-based retail analytics since consumers receive lower-priced rather than free goods, this Article would be incomplete without considering it because many online services and mobile applications market themselves as "free."

The rising number of new products and services that market themselves as "free" can have a significant effect on consumer decision making because consumers may fail to consider the tradeoffs implicit in acquiring that product or service. For example, assume that a consumer is deciding between two voice-to-text smartphone applications ("apps"). The first app normally costs $15, but the developer offers it for $5 if users consent to some information collection. The developer also promises not to share that information with any third parties (it wants to collect information to improve user experiences and grow market share). The second app would normally cost $10, but the developer offers it for free if users consent to broad data collection and to sharing with third parties. Because of the zero price effect, a large number of consumers will prefer the "free" app because of the emotional response triggered by the app that appears to have no downside.

For a real-world example, consider Facebook: More than 1.5 billion individuals have a "free" Facebook account. Until recently, however, most of these individuals did not realize the extent to which Facebook collects, analyzes, and markets personal information about them.[256] When these practices became publicly known, user outrage prompted Facebook to implement a number of new privacy-protecting measures.[257] This shows that consumers

---

255. Kristina Shampan'er, Nina Mazar & Dan Ariely, *Zero As a Special Price: The True Value of Free Products*, 26 MARKETING SCI. 742, 743 (2007); Kristina Shampan'er & Dan Ariely, *How Small Is Zero Price? The True Value of Free Products*, 3-4 (Fed. Res. Bank of Bos., Working Paper No. 06-16, Oct. 2006), https://www.bostonfed.org/economic/wp/wp2006/wp0616.pdf.

256. *See, e.g.*, Taylor Casti, *Facebook Knows Everything About You, and If You Don't Believe Us Here's Proof*, HUFFINGTON POST (Apr. 26, 2014), http://www.huffingtonpost.com/2014/04/22/watch-dogs-facebook-privacy-settings_n_5191237.html; JR Raphael, *Facebook Privacy: Secrets Unveiled*, PCWORLD (May 16, 2010, 3:12 PM), http://www.pcworld.com/article/196410/Facebook_Privacy_Secrets_Unveiled.html.

257. Hamish Barwick, *Facebook Responds to Privacy Concerns*, COMPUTERWORLD (Apr. 10, 2014, 2:03 PM),

must know and understand the true costs associated with "free" services in order to properly assess the associated risks and make an informed decision.

As has been the case with the other consumer behaviors discussed in this Section that can result in irrational decision making, regulation might be appropriate to correct the zero price effect. Specifically, a "tax" on those that collect and use consumer data will be passed on to consumers, which will offset consumer miscalculations in the decision-making process and induce them to make rational, utility-maximizing choices. However, to correctly determine the amount of the offsetting tax, regulators must understand the costs and benefits that arise from the underlying practice. Thus, while regulatory action might be appropriate, an FTC deception claim will not always properly correct irrational consumer behavior.

5. Summary of the Behavioral Model

The behavior model has shown that the rational model can fail to accurately predict market outcomes that lead to inefficiency when consumers fail to make rational, utility-maximizing decisions. This might occur because of incomplete information, failure to consider all relevant information, hyperbolic discounting, optimism bias, the endowment effect, limited opportunism, or the zero price effect. However, this Section has also shown that regulation can correct almost all of these problems by inducing or requiring decision makers to make rational choices when detected in the market. Specifically, by imposing a "tax" on parties that collect and use consumer information, regulation works to offset the impact of consumers undervaluing the harms that flow from information collection relative to the corresponding benefits because the tax will be passed on to them. However, efficient outcomes are likely to result only when regulators like the FTC understand the costs and benefits that arise from the underlying practice and are then able to determine the price adjustment necessary to correct the irrational behavior.

Due to the limited facts supporting the FTC's deception claim against Nomi, it is impossible to determine whether any irrational behavioral traits were at play. However, the FTC's failure to conduct a cost-benefits analysis or identify any concrete consumer injuries coupled with the unlikelihood that any consumers would have

---

http://www.computerworld.com.au/article/542577/facebook_responds_privacy_concerns_/.

exercised the in-store opt-out option had it been available suggests that its action against Nomi did not produce an efficient outcome from a social welfare standpoint. As a result, the normative conclusion from the rational model has not changed. A cost-benefits prerequisite to all Section 5 enforcement actions is more likely to ensure an economically efficient outcome when compared to the FTC's strict liability regime for deceptive acts or practices. In fact, the behavioral model supports the proposition that a cost-benefit analysis is necessary when the FTC seeks to manipulate market outcomes to "correct" irrational behavior. Only then can the agency correct these behaviors in a way that generates the outcome that would result in a competitive market with rational actors.

VI. CONCLUSION

Information is a critical—if not the most important—component of today's technology-driven economy. Readily available consumer information provides numerous benefits to both businesses and consumers and has fostered vast economic expansion over the last twenty-five years. This does not mean that consumer privacy is unimportant and should not be protected; it means that privacy concerns must be balanced with the social benefits of information availability. Partly due to a lack of direct congressional action, the FTC has become responsible for balancing these interests through its Section 5 authority to protect consumers from deceptive acts or practices and unfair methods of competition.

Ironically, the primary method through which the FTC makes consumer information privacy decisions does not require it to undertake any balancing whatsoever. As this Article's analysis of the FTC's action against Nomi has shown, this shortcoming can negatively affect social welfare when the agency sanctions a business for trivial privacy policy misstatements where consumer harm is not shown and the net social gains of data collection are greater than net social losses. However, these outcomes can be avoided by imposing a cost-benefits prerequisite to all Section 5 enforcement actions. This Article has also shown that the market can adequately respond to most consumer privacy violations and that the FTC is currently better positioned to function as a "privacy watchdog" rather than as the nation's predominant privacy regulator because of its propensity to take overzealous action that ultimately injures consumer welfare.