SHOPPING FOR PRIVACY ONLINE: CONSUMER DECISION-MAKING STRATEGIES AND THE EMERGING MARKET FOR INFORMATION PRIVACY

*James P. Nehf**

I. INTRODUCTION

Privacy policies are seemingly everywhere. Banks, credit card issuers, insurers, hospitals, and other data collectors proclaim that they care about consumer privacy and then proceed to explain in copious rhetoric how their data collection, storage, and sharing are carried out. Curious Web surfers can click links to read the privacy policies of the sites they visit. Under U.S. law, businesses in several economic sectors—financial services,[1] health services,[2] cable television,[3] telecommunications,[4] children's online services,[5] and video rental[6]—are compelled to disclose their privacy practices. In other business sectors, disclosing information practices is largely voluntary, but disclosure is nearly as common.

Beyond legal mandates, several forces are driving the proliferation of privacy policies. Market pressures encourage many businesses to at least appear sensitive to customers' privacy concerns. Most businesses would like to avoid the perception or implication that they harvest and sell the personal data they obtain either openly or surreptitiously from

* Professor of Law and Cleon H. Foust Fellow, Indiana University School of Law-Indianapolis. The author presented an earlier version of this paper at the Tenth International Consumer Law Conference in Lima, Peru, in May 2005. Special thanks to Dr. Brenda Cude and the Department of Housing and Consumer Economics at the University of Georgia for comments on an early draft and suggestions for social science resource materials.

1. Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801–6809 (2000).
2. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, & 42 U.S.C.).
3. Cable Communications Policy Act (CCPA) of 1984, 47 U.S.C. § 551 (2000).
4. Telecommunications Act of 1996, 47 U.S.C. § 222 (2000).
5. Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. § 6501 (2000).
6. Video Privacy Protection Act (VPPA) of 1988, 18 U.S.C. §§ 2710–2711 (2000).

their customers. Indeed, business consulting firms now routinely encourage the adoption and promotion of privacy policies as a way to present a positive client image.[7] Appearing concerned about customer privacy has become a standard marketing strategy.

Beginning in the mid-1990s, firms that collected information from European consumers began to publish privacy policies to comply with the European Union (E.U.) data protection directive.[8] For most other businesses, persuasive efforts of the Federal Trade Commission (FTC) played an influential role. During the late 1990s, the FTC conducted studies of consumer privacy preferences and business privacy practices.[9] The studies concluded that firms were collecting and selling a vast amount of personal information without consumer knowledge or consent and using it in ways that consumers did not approve.[10] The problem was most acute on the Internet, where personal information is easily obtained, collated, and distributed through a variety of technological means, many of which are hidden from consumers.[11] The disconnect between consumer privacy preferences and business data-handling practices was so severe that by the end of the decade, the FTC was calling for national legislation to mandate fair information policies on the Internet.[12]

Political winds shifted, however, and with additional studies and a change in FTC leadership in 2001, the agency tabled its push for privacy legislation in favor of industry self-regulation.[13] As an incentive, the FTC

---

7. In October 2002, the American Institute for Certified Public Accountants (AICPA) formed a task force to promote the selling of privacy services by CPAs. *See* AICPA, Enterprise-Wide Privacy Solutions, http://www.aicpa.org/innovation/baas/ewp/homepage.htm (last visited Nov. 28, 2005). The task force developed strategies to position accountants as key players in the growing privacy protection industry. *Id.* The AICPA opined, "Good privacy practices can do far more than build customer confidence and protect the integrity of an organization's brand—they can also increase customer loyalty and add to the bottom line." *Id.*; *see also* Accenture, Business and Consumers See Privacy and Trust Differently (2003) [hereinafter Accenture Survey] (on file with JLTP) (survey of consumer privacy preferences by Accenture); *Businesses and Consumers See Privacy and Trust Differently*, ACCENTURE DIGITAL F., March 2004, http://digitalforum.accenture.com/DigitalForum/Italy/ViewByTopic/Privacy/Bsns_and_cons_see_differently.

8. *See* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) (concerning "the protection of individuals with regard to the processing of personal data and on the free movement of such data"); Council Directive 97/66, 1997 O.J. (L 24) 1 (EC) ("concerning the processing of personal data and the protection of privacy in the telecommunications sector"). In the United States, there are only a few state privacy laws that affect Internet commerce. *See, e.g.*, MINN. STAT. §§ 325M.01–.09 (2004) (privacy rules for Internet service providers).

9. In 2000, the FTC concluded that industry measures were far from adequate and that national privacy legislation was needed. *See* DIV. OF FIN. PRACTICES, FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 28–29 (2000) [hereinafter FTC, PRIVACY ONLINE], *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

10. *Id.* at 25.

11. *Id.* at i.

12. *Id.* at 36 ("The proposed legislation would set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites . . . .").

13. *See* Timothy J. Muris, Chairman, Fed. Trade Comm'n, Protecting Consumers' Privacy: 2002 and Beyond, Remarks at the Privacy 2001 Conference (Oct. 4, 2001) [hereinafter Muris, Protecting], *available at* http://www.ftc.gov/speeches/muris/privisp1002.htm; *see also Challenges Facing the Federal Trade Commission: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of*

kept alive its threat of regulatory action if Internet firms did not adopt fair information practices in due course.[14] The threat was serious for large e-retailers who had much to lose if government standards directed how they managed consumer information online. By the end of 2001, nearly all of the most frequently visited Web sites had implemented detailed information practices accompanied by published privacy policies, but data-collection techniques and sharing activities varied widely among firms, and the practices of many smaller firms were unknown.[15] Because the market for consumer purchasing, demographic, and Web-surfing information was in full swing with a seemingly unlimited future, firms with strong online presences overwhelmingly preferred self-regulation to mandatory privacy standards that might hinder further growth. It was therefore in the interest of the major online firms to encourage smaller firms to adopt privacy practices that satisfied the FTC.

To this end, several firms (IBM being the most notable) announced that they would no longer advertise or link to Web sites that did not publish privacy policies conforming to fair information practices.[16] The chain reaction was swift, as other firms announced similar plans, and many smaller Internet sites complied. This informal coordination among firms solved what might otherwise have been a classic free-rider problem.[17] Privacy policies cost money to develop, implement, and maintain, and they invite FTC and state enforcement actions if a firm does not follow them. An individual business, acting without market pressure, might be better off without a privacy policy so long as enough other businesses convinced the FTC that the problem did not justify broad-based government intervention. Market pressure assured that there would be no free riders in this lane of the information highway.

The FTC lauded the success of its market-driven solution.[18] Indeed, privacy policies can be seen everywhere today, and they give the impression that Web sites safeguard personal information that they collect. When the policies are read, however, there is often very little privacy protection being promised. Policies might disclose how data is collected and how it will be transferred, sold, or traded, but often the message is that information will be collected in whatever way the Web

---

the H. Comm. on Energy and Commerce, 107th Cong. 10–12 (2001) (statement of Timothy J. Muris, Chairman, Federal Trade Commission) [hereinafter Muris, Challenges], *available at* http://energycommerce.house.gov/107/action/107-68.pdf.

14. *See* Muris, Challenges, *supra* note 13.

15. *See* Muris, Protecting, *supra* note 13.

16. Jon G. Auerbach, *To Get IBM Ad, Sites Must Post Privacy Policies*, WALL ST. J., Mar. 31, 1999, at B1.

17. *See* Steven Hetcher, *The* De Facto *Federal Privacy Commission*, 19 J. MARSHALL J. COMPUTER & INFO. L. 109, 118 (2000).

18. Muris, Protecting, *supra* note 13 ("One of the agency's successes has been encouraging Internet sites to post privacy notices."). Indeed, in 1998, only two percent of all Web sites had some form of privacy notices. *Id.* By 2000, virtually all of the most popular commercial Web sites had privacy notices. *Id.*

site can obtain it, and the site reserves the right to share or sell it with impunity.[19] References to information security or safeguards tend to be vague and noncommittal.[20] Thus, despite the proliferation of privacy policies online, consumers' privacy interests may in fact be no better protected today than they were ten years ago. The FTC placed its faith in market incentives to curb unfair privacy practices, but there may be little incentive for online businesses to adopt and adhere to strong privacy policies. It is the appearance of privacy that seems to matter most.

To be fair, the FTC's goal has not been to mandate strong, consumer-friendly information practices, only market-efficient ones. The agency is pursuing a policy of transparency, urging businesses to post their practices and honor their commitments.[21] The agency expects market forces to produce privacy terms that reflect an efficient balance of consumer and business preferences. This approach makes sense in light of the FTC's mission as it historically has been viewed. Through the decades, the agency has focused most of its resources on ensuring accurate disclosure, preventing deceptive practices, and developing open and competitive markets that encourage and reward informed consumer choice.[22] It has seldom imposed contract terms or acted as a protector of basic consumer rights.

In this Article, I argue that encouraging the posting of privacy policies without regulating their content is likely to result in suboptimal privacy practices—that is, privacy practices that give consumers

---

19. For example, the privacy policy for the online Parisian department store begins with the words "JUST BETWEEN YOU AND US," but goes on to explain that personal information may be acquired in numerous ways and that Parisian

> may share this information about you with other members of our Saks Incorporated retail family of companies. . . . If you use your Parisian credit card, we will share information about you with other members of our retail family of companies.
>
> We and other members of our retail family of companies may occasionally share information about you (such as names and regular mail address) with responsible marketing organizations, outside of our retail family of companies, that offer products and services that we believe would be of interest to you.

Parisian, Privacy Policy, http://www.parisian.com/Default.aspx?PAGETYPE=PRIVACY_POLICY_POPUP (last visited Nov. 29, 2005).

20. The PGA Tour Web site is typical:

> The Site incorporates reasonable safeguards to protect the security, integrity, completeness, accuracy and privacy of the personal information that we may collect and we have put into place reasonable precautions to protect such information from loss, misuse and alteration. Your credit card number is encrypted via Secure Sockets Layer (SSL) and is stored behind a firewall. Only those employees who need access to your information in order to do their jobs are allowed access. Our security policies are reviewed periodically and revised as required.

PGATOUR.com, Privacy Policy: Security, http://www.pgatour.com/info/privacy#security (last visited Nov. 29, 2005).

21. The publication of privacy policies thus has important institutional effects regardless of the content of the privacy practices that are disclosed. The FTC and state attorneys general can prosecute deceptive practices if a site does not honor its published privacy policy. Several cease-and-desist orders have resulted from such enforcement actions. *See* FTC, Unfairness & Deception: Enforcement, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Nov. 29, 2005).

22. *See generally* FTC, PRIVACY ONLINE *supra* note 9, at 3–6 (describing the FTC's approach to online privacy).

substantially less information privacy than an efficient market would produce.[23] To support the argument, I examine research on consumer decision strategies and behavioral economics. I first describe rational choice theory in the context of a market for personal information online. I then explore whether the assumptions underlying the theory are supported by social science research concerning consumer behavior and decision-making patterns. The evidence is conflicting but, I believe, reconcilable, and troubling for those who put their faith in market solutions to privacy problems.

On the one hand, studies in behavioral economics suggest that online information privacy is important to consumers and that consumers desire more control over access to their personal information and subsequent use of the information after it is obtained.[24] These findings support a market-driven approach. If consumers are aware of their privacy concerns and deem privacy important, they are more likely to take steps to protect their own interests—for example, avoiding firms that might compromise their privacy interests and frequenting the ones that are more likely to protect them. Without prohibitively high transaction costs or impediments to understanding the varying privacy practices of competing firms, informed consumer choices should produce more efficient privacy practices online.

On the other hand, research on bounded rationality and consumer decision making suggests that in most circumstances consumers, acting rationally, do not factor privacy policies into their decision processes, even when they consider privacy important, because privacy concerns are seldom salient.[25] When rational consumers value privacy but do not factor privacy concerns into the decision-making process, the market may produce suboptimal privacy terms that benefit data collectors. Moreover, the research suggests that the problem is not solvable by reducing transaction costs and making information about privacy practices more visible or easily understood.

To the extent that this condition exists, it would seem to elicit three responses, which I explore in Part III of this Article. The first response is patience. We are still in the relatively early stages of an emerging market for information privacy. Over time, market influences such as advertising, personal experience, privacy signals (such as privacy trust marks), and technological developments may make privacy terms more

23. The argument is pertinent to unregulated market sectors as well as economic sectors in which privacy laws already exist because those laws rely primarily on disclosure of privacy policies and consumer choice rather than mandating the content of privacy practices. *See supra* text accompanying notes 1–6. For the laws to work effectively, consumers must police their own privacy interests by learning the content of a firm's privacy practices and then acting in their own best interests to limit information disclosure or opt out of information sharing. *See generally* James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 45–58 (2003) (discussing the protection of privacy in the private sector).

24. *See* discussion *infra* Part II.C.

25. *See* discussion *infra* Part II.D.1–.3.

salient.[26] Online firms may respond to a resulting shift in consumer decision strategies, and more efficient privacy policies may emerge in time.

A second response is government imposition of mandatory privacy terms drafted to ensure that privacy practices online coincide better with rational consumer preferences, as the FTC urged in the late 1990s. Regulatory or legislative privacy mandates have been imposed in various degrees and with varying success in several economic sectors in the United States and even more broadly in Europe. Experience with those laws and practical problems in drafting an efficient set of online privacy mandates, however, suggest that this alternative may be less desirable than the current but inadequate market-driven approach.[27]

A third response, and one I argue is best for the foreseeable future, is to encourage the evolution of more efficient privacy practices over time through more aggressive public and private enforcement actions. I urge the FTC and state consumer protection agencies to resurrect and flex their unfairness and deceptive practices authority, which thus far has been fairly weak in policing the market for injurious privacy practices.[28] Bringing enforcement actions only for the most blatantly deceptive privacy breaches or database security failures is not likely to strengthen the substance of privacy practices and align them better with consumer preferences. Expanding the reach of deception and unfairness adjudication has several advantages over legislative or rulemaking action, the most important of which is allowing norms to emerge and evolve incrementally over time. Although the FTC's unfairness and deception standards do not align well with many online privacy concerns, the standards can and should be revised and applied more aggressively if our market-regulating agency is serious about developing a more efficient privacy regime.

II. BOUNDED RATIONALITY AND THE MARKET FOR INFORMATION PRIVACY ONLINE

A. Legitimizing Private Law in Market Transactions Generally

Law seeks to control societal tendencies towards anarchy by directing, and at times punishing, the behavior of those who live within the legal regime and act beyond generally accepted societal norms. When a government exerts power to direct the behavior of its subjects, there are always questions of legitimacy—what justifies the imposition of law to restrict the freedom of individuals? In our constitutional system,

26. *See* discussion *infra* Part III.A.
27. *See* discussion *infra* Part III.B.
28. *See* discussion *infra* Part III.C.

the consent of the governed acting through their elected representatives legitimizes public law. Consent between individuals or groups legitimizes private law. Contract law, in particular, has long been viewed as a legitimate creation of private law because it results from voluntary undertakings that direct the behavior of two or more willing parties.[29] Similarly, the relationship between Web sites and their users is contractual in nature. Web sites offer content, products, and services in exchange for money and, in many cases, personal information.

Although the consent model of contract law is still taught in most law schools, it is widely viewed as an inadequate description and normative justification for modern contractual relationships.[30] Standard form contracts are consent-based on only the most basic terms. In most transactions, at least one party (and sometimes both) has little awareness of contract terms, and it is difficult to defend term legitimacy on consent grounds alone. This elicits three categories of response. One is to champion measures that may create an environment in which informed, subjective consent is more likely to occur.[31] Laws calling for conspicuous disclosure of terms, notice of contract rights, plain language, and mandatory rescission or cooling-off periods try to ensure that consumers make better informed and more voluntary decisions.

A second type of response is to acknowledge the absence of actual consent, accept it as an unavoidable condition of transacting business in the modern world, and argue that non-consensual private law is

29. *See* JOHN RAWLS, A THEORY OF JUSTICE 343 (rev. ed. 1999); Randy E. Barnett, *Rational Bargaining Theory and Contract: Default Rules, Hypothetical Consent, the Duty to Disclose, and Fraud*, 15 HARV. J.L. & PUB. POL'Y 783, 801 (1992) ("A fundamental tenet of the liberal conception of justice is that resources rightfully belonging to another may not be taken without the manifested consent of the rights-holder.").

30. *See* William W. Bratton, Jr., *The "Nexus of Contracts" Corporation: A Critical Appraisal*, 74 CORNELL L. REV. 407, 458–59 (1989) ("Contract law literature contains commentary effectively challenging classical contract's conjunction of contract, consent, and freedom."); Duncan Kennedy, *The Stages of the Decline of the Public/Private Distinction*, 130 U. PA. L. REV. 1349, 1352 (1982) ("[T]he 'free' 'private' market is really an artifact of public violence."); Betty Mensch, *Freedom of Contract as Ideology*, 33 STAN. L. REV. 753, 764 (1981) ("Coercion, including legal coercion, lies at the heart of *every* bargain. Coercion is inherent in each party's legally protected threat to withhold what is owned. The right to withhold creates the right to force submission to one's own terms."). *See generally* Lawrence Kalevitch, *Gaps in Contracts: A Critique of Consent Theory*, 54 MONT. L. REV. 169, 188–95 (1993) (discussing the problems of consent and traditional contracts).

31. The point here is not whether a subjective or objective standard of consent should be used to assess the legitimacy of privacy policies. *See generally* Randy E. Barnett, *A Consent Theory of Contract*, 86 COLUM. L. REV. 269 (1986) (discussing subjective and objective theories for contract enforcement). Subjective consent to privacy policies is largely a fiction, and justifications for non-intervention therefore must come from elsewhere—rational choice being the justification adopted by the FTC (and many others) thus far. Objective consent is an oxymoron or at best a shorthand term for concluding that while there is no intentional consent, the undertaking should be enforced for other reasons. *See, e.g.*, RANDY E. BARNETT, PERSPECTIVES ON CONTRACT LAW 313 (1995). In other words, if a person did not actually consent to something, he can still be bound by the outcome because there is a normative justification for holding him to the terms. My point is, without subjective consent, the justification for government non-intervention in the making of private law is called into question. Rational choice is a popular theory that tries to fill the void (as a normative underpinning for private law in an objective consent scenario), but, for the reasons discussed below, it does not serve as a viable justification for privacy policies.

legitimized in other ways. Presently, the most widely accepted alternative is rational choice theory, often referred to in this context as the contract-as-product justification.[32] A non-consensual contract term is one of many non-negotiable, hidden aspects of a product or service being offered. Consumers purchase many products and services without knowing many of their physical, experiential, and legal attributes—good, bad, or otherwise. In the sale of a computer, for example, a typical buyer may be aware of some but not all software and hardware properties. Similarly, the buyer may be fully aware of a few contract terms (for example, a one-year warranty) but only vaguely aware of others. At the time of delivery, the computer comes as a bundled, packaged product, and the buyer must decide whether to buy the entire bundle, terms and all.[33]

Observing that contract terms are simply part of a package deal may describe contracting in today's world, but it does not necessarily legitimize the terms. Without a normative justification to legitimize private law created in the absence of informed, voluntary agreement, there is no reason why we should not ignore the adhesion contract terms and use default rules found in legislation, at common law, or in some other source. Absent a trade custom, a court likely would not enforce a secret term that one contracting party did not even disclose to the other. A disclosed but unread term—or privacy policy—also could be held unenforceable, unless there is a good reason to consider it binding.

One reason we might enforce a disclosed but unread term is essentially fault-based. If people choose, without coercion, to enter into a transaction without reading the terms, they take a risk and the law will not hear their complaint if harm later results. We might say that they waived their legitimacy claim by foregoing the opportunity to withhold consent if they thought the term was unfair. Fault-based justifications have normative appeal, but only when there is a societal consensus that a person is genuinely at fault. Through personal experience we know that in most form-contracting situations our failure to read is excusable and even expected. If someone insisted on reading, questioning, and even

32. *See generally* Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. 1125 (2000) (discussing the contract-as-product model of contract with respect to online transactions).

33. Drafters of some adhesion contracts, particularly end-user license agreements for software, may attempt at least to give the appearance of negotiable terms (and thereby deflect potential unconscionability claims) by including a telephone number that the licensee can call if terms are not satisfactory or if additional rights are desired. *See, e.g.*, P22, End User Agreement, http://www.p22.com/support/license.html (last visited Nov. 29, 2005) (explaining the method for obtaining licensing rights beyond those granted in the standard agreement); Veer, End User License Agreement, http://www.veer.com/help/license.aspx?eula=VLI (last visited Nov. 29, 2005) ("Please be aware that we are serious about preserving the integrity of this License Agreement, and will take action to enforce it when necessary. At the same time, though, we will be pleased to make special arrangements to permit you to use an image or images in many ways that are excluded by this Agreement. Generally, this is a quick and easy process. Please call us at 1-888-708-8777 . . . .").

dickering over standard terms, others likely would find the behavior odd and pointless.

Those who argue for enforcing standard contract terms, therefore, seldom use fault-based justifications. Instead, they argue that if market participants behave rationally, market forces will ensure that contract-drafting parties include efficient terms, whether bargained for or not.[34] Market actors make choices in their own best interests, and the resulting equilibrium is then efficient. If efficiency is accepted as a morally legitimate end, then the regime is morally defensible.[35] As Judge Easterbrook wrote in *ProCD, Inc. v. Zeidenberg*,[36] "Competition among vendors, not judicial revision of a package's contents, is how consumers are protected in a market economy."[37]

A third response to the perceived legitimacy of non-bargained-for terms is to claim that they have no legitimacy and to call for mandatory terms imposed by government authority. Legitimacy is then reestablished by the democratic process. Indeed, broadly speaking, the evolution of law in many areas can be viewed as a movement away from unrealistic consent-based assumptions and inadequate disclosure-based market refinements and toward mandatory rules, whether creations of common law or statutory imperatives. Examples can be found in virtually all fields, including, to name just a few, employment (including exceptions to employment-at-will, numerous anti-discrimination laws, and mandatory accommodations for workers with disabilities); insurance (for instance, state-imposed insurance terms); competition (such as restrictions on anti-competitive mergers and product tie-ins); and

---

34. *See* Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203, 1206, 1210–11 (2003). *See generally* Richard Craswell, *Passing on the Costs of Legal Rules: Efficiency and Distribution in Buyer-Seller Relationships*, 43 STAN. L. REV. 361 (1991).

35. *See* Eve M. Caudill & Patrick E. Murphy, *Consumer Online Privacy: Legal and Ethical Issues*, 19 J. PUB. POL'Y & MARKETING 7, 14–15 (2000); Frank V. Cespedes & H. Jeff Smith, *Database Marketing: New Rules for Policy and Practice*, SLOAN MGMT. REV., Summer 1993, at 7–8. For purposes of this Article, I do not challenge the idea that economic efficiency is a valid norm for judging the effectiveness of online privacy policies. Privacy could be viewed as a fundamental right that should not be commodified or traded away at any price. Ontological justifications for privacy protection have a long history, and I do not review them here. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 31–32 (1968); Stanley I. Benn, *Privacy, Freedom, and Respect for Persons, in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 223 (Ferdinand David Schoeman ed., 1984); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2088, 2092–98 (2001) (connecting privacy to three distinct concepts: dignity, autonomy, and the creation of knowledge); Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra*, at 300; Jeffrey Rosen, *The Purposes of Privacy: A Response*, 89 GEO. L.J. 2117, 2121 (2001). Market regulation of privacy practices is the predominant approach in the United States for now, at least in the private sector. Rightly or wrongly, information is seen as a tradable commodity. Those opposing government mandates usually argue economics in their favor, so it is important to explore the ramifications of efficiency claims for online privacy practices. Moreover, while economic arguments might not provide definitive normative justifications, they can at least be useful in informing decisions about the appropriate allocation of rights.

36. 86 F.3d 1447 (7th Cir. 1996) (challenging standard licensing terms within a software package).

37. *Id.* at 1453.

landlord-tenant relations (including court- or legislature-imposed habitability requirements, anti-discrimination laws, and eviction procedures). Statute books are replete with laws that impose terms in relationships that previously had been left to market forces and to the immediately affected parties to decide for themselves. Whether government-mandated terms are fairer or more efficient than terms produced by market exchange is continually questioned, but the practice of state interference with private relationships, as a means of legitimizing the law created therein, is commonplace.

Consumer law has certainly evolved along such a path. As new products and business practices develop, relationships between firms and consumers often are seen initially as consent-based because consumers usually enter into transactions of their own free will, and the rules governing those transactions are, to a large extent, created by the parties' express or tacit agreement. Common law doctrines of deceit and misrepresentation support the consent model because a person's consent is defective, and therefore less legitimate, if based upon erroneous information supplied by the other party. Much statutory consumer law fits the consent model as well. Disclosure laws (for example, truth-in-lending, credit reporting, and warranty disclosure laws) are premised on the idea that consent is more voluntary and markets work better when consumers are better informed. Even when consent remains imperfect, disclosed terms can ensure that market forces will protect collective consumer interests by driving out undesirable practices. Yet market failures abound even with full disclosure, and legislative limits on contractual freedom in consumer transactions are commonplace.[38]

Privacy policy in the United States is still in its relatively early stages and is discussed largely with the rhetoric of consent. The collection and trading of personal information is viewed as part of a voluntary undertaking and exchange between consumers who give businesses their personal information and businesses that use or sell the information.[39] The model is under increasing scrutiny, however. Many consumers feel wronged if a firm collects information without their express knowledge and agreement, if the firm sells or rents that information to a third party without permission, or if a consumer's desire to revoke consent is not

38. Debates about regulating the sub-prime lending market are a recent example. In some states, disclosure of sub-prime lending fees and corresponding annual percentage rates is regarded as sufficient to protect societal interests. In others, caps on fees or outright prohibition of certain lending practices, such as "payday" loans, have been legislated. *See generally* James P. Nehf, *Secured Consumer Credit and the Fringe Banking Industry*, *in* SECURED TRANSACTIONS UNDER THE UNIFORM COMMERCIAL CODE ch. 20A (J.B. McDonnell ed., 2005) (discussing state and federal laws governing traditional pawns, automobile title pawns, "payday" loans, tax refund anticipation loans, and rent-to-own transactions).

39. *See, e.g.*, Mary J. Culnan, *Protecting Privacy Online: Is Self-Regulation Working?*, 19 J. PUB. POL'Y & MARKETING 20, 21 (2000) (discussing the exchange of personal information for economic or social benefit and urging measures to enhance consumer choice).

heeded (for instance, if a consumer is not given the opportunity to remove personal information from the database or restrict its use).[40]

This is where privacy policies become relevant. To address the perception of surprise and betrayal, collectors of personal information disclose privacy policies by mail or, for online services, through Web site links. Consumers then have the opportunity to read and understand the terms before disclosing personal information.[41] Privacy policies essentially propose to transform an implicit exchange into an explicit, consensual one: the consumer gets the benefit of the product or service that the business offers (such as financial services, insurance, Web site content, health care, or video rentals), and the business gets (in addition to, perhaps, the consumer's money) some personal information, agreeing to treat the data in accordance with the stated terms in the policy.[42]

Research and everyday personal experience tell us that consumers seldom read privacy policies. In a study of adult Internet users who were asked to evaluate the credibility of Web sites, less than one percent of respondents even noticed privacy policies.[43] Still, privacy laws and the FTC's current approach to privacy online work within the consent and rational choice models by requiring or encouraging disclosure of privacy practices as the primary control mechanism.[44] If privacy policies are not widely read, the consent justification for allowing businesses to set their

---

40. Joseph Phelps, Glenn Nowak & Elizabeth Ferrell, *Privacy Concerns and Consumer Willingness to Provide Personal Information*, 19 J. PUB. POL'Y & MARKETING 27, 28 (2000).

41. With cookies, Web bugs, GIF tags, and other technologies, however, some information likely has been transmitted already before the consumer has had an opportunity to read the Web site's privacy terms. *See* Viktor Mayer-Schonberger, *The Internet and Privacy Legislation: Cookies for a Treat?*, 1 W. VA. J.L. & TECH. 1.1 (1997), http://www.wvu.edu/~law/wvjolt/Arch/Mayer/Mayer.htm. *See generally* Robert O'Harrow, Jr., *Fearing a Plague of "Web Bugs,"* WASH. POST, Nov. 13, 1999, at E1.

42. In other transactions, the exchange is less obvious. A consumer may provide personal information to an Internet search engine (knowingly or not) in exchange for access to the search engine's content. The search engine collects the information and treats it in accordance with its information privacy policy. The exchange may not be expressly bargained for, but there is an exchange of value nonetheless.

43. B.J. FOGG, ET AL., CONSUMER REPORTS WEBWATCH, HOW DO PEOPLE EVALUATE A WEB SITE'S CREDIBILITY?: RESULTS FROM A LARGE STUDY 86 (2002), http://www.consumerwebwatch.org/pdfs/stanfordPTL.pdf.

44. The FTC's list of Fair Information Practices encourages but does not require disclosure, nor does it mandate any particular privacy terms. FTC, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.htm (last visited Nov. 29, 2005). Recommended privacy practices include: notice or awareness (publishing privacy statements regarding storage, dissemination, manipulation, and security); choice or consent (providing either opt-out or opt-in alternatives); access or accuracy (allowing access to confirm accuracy); integrity or security (controlling against theft and tampering); and enforcement or redress (implementing some mechanism to ensure compliance). *Id*. Among the five recommendations, the FTC considers notice of privacy practices to be the most fundamental, but the law does not compel such notice or mandate the terms of the privacy policy. Kim Bartel Sheehan & Mariea Grubbs Hoy, *Dimensions of Privacy Concern Among Online Consumers*, 19 J. PUB. POL'Y & MARKETING 62, 69 (2000). This dovetails with the FTC's oversight responsibility under § 5 of the FTC Act, which prohibits unfair or deceptive practices. *See* 15 U.S.C. § 45(a)(1)–(2) (2000). If a business does not follow its stated privacy policy, it commits a deceptive act in violation of the FTC Act. The FTC has yet to hold, however, that failure to disclose one's privacy practices is unfair.

own privacy terms is doubtful. This leaves rational choice as the justifying theory.

The regime is not necessarily justified, however, under rational choice theory. When purchasing a product or using a service, consumers get many things that they explicitly bargain for plus many additional attributes that go unnoticed. These may include some beneficial and some detrimental product or service attributes as well as some beneficial or detrimental legal attributes. Market forces may be able to produce efficient terms on all of these attributes, including privacy terms, and therefore legitimize them even in the absence of true consent. Research in consumer behavioral sciences suggests, however, that market forces do not produce optimal privacy practices because privacy policies are seldom salient in the decision-making process.[45] The following discussion shows why.

B. The Market for Information Privacy Online

The rational choice model assumes that when faced with a decision, consumers will take into account the relevant attributes among competing alternatives and choose the one that yields the best net result. In its purest form, this is sometimes described as a weighted-adding strategy, whereby people cognitively assign an importance weight or value (positive or negative) to each attribute of the product or service about which they have a preference, total the weights, and choose the alternative with the highest total value.[46] For example, in the context of

45. This conclusion is one of the foundations of the E.U. approach to privacy protection, where several duties are imposed on data collectors by law. Caudill & Murphy, *supra* note 35, at 15. A duty of "fidelity" requires businesses to act in a forthright and honest manner and includes a duty to disclose privacy policies truthfully, conspicuously, and coherently and to redress injuries without delay. *Id.* A duty of "beneficence" imposes an obligation to do right by one's customers. *Id.* This requires more of an opt-in rather than an opt-out rights approach and permits the tracking of only those customers who knowingly participate in data collection. *Id.* A duty of "nonmalfeasance" is the duty not to injure others. *Id.* This requires the maintenance of security and accuracy with respect to the information stored and a commitment to keep the information from getting into the hands of those who could harm consumers. *Id.*

46. In the classic weighted-adding strategy, the decision maker considers one alternative at a time and examines each of its attributes, arriving at a certain value for each attribute. *See* James R. Bettman et al., *Constructive Consumer Choice Processes*, 25 J. CONSUMER RES. 187, 190 (1998). The decision maker then multiplies each attribute value by its weighted importance and chooses the alternative with the highest total value. *Id.* Because weighted-adding is extensive (evaluating all attributes of competing alternatives), compensatory (a good value on one attribute can compensate for a poor value on another), and requires explicit trade-offs, it is generally regarded as the most accurate process for determining individual preferences. *Id.*; Deborah Frisch & Robert T. Clemen, *Beyond Expected Utility: Rethinking Behavioral Decision Research*, 116 PSYCHOL. BULL. 46, 49 (1994). It places great demands on the decision maker's memory and computation abilities. Bettman et al., *supra*, at 190. Despite these obvious deficiencies, it is the method underlying much market research. *Id.* A simplified version of weighted-adding is the equal weight strategy, in which the decision maker considers all attributes of all alternatives, but processing is simplified by assigning the same weight to each attribute. *See* Robyn M. Dawes, *The Robust Beauty of Improper Linear Models in Decision Making*, 34 AM. PSYCHOLOGIST 571 (1979). Even in its simplified form, the strategy is cognitively intensive.

privacy and a consumer deciding between two news Web sites to frequent, one site might offer in-depth news content for free but collect and share registration and cookie data with third parties (a "weak" privacy provider). Another might offer more limited news content for free and enhanced coverage if the consumer pays $3.99 per month but keep any personal data secure and share it with no one (a "strong" privacy provider). If other attributes of the Web sites are equal, an informed consumer who wants extensive news coverage and also cares about privacy must decide whether her privacy is worth $3.99 per month.

When informed consumers use a weighted-adding strategy, market pressures should force businesses to produce efficient outcomes, and an efficient price point for personal information is reached.[47] If a very small number of customers think keeping their information private is worth $3.99, then the strong privacy provider will not gain many customers by offering privacy for that price. If it costs the strong privacy provider only two dollars per subscriber to provide good privacy protection (in added cost of security and lost marketing opportunities), the publisher may lower its price in an attempt to attract more customers and maximize its profits. If very few consumers are even willing to pay more than two dollars for strong privacy protection, then very few Web sites will provide it. From a societal perspective, this is still efficient because few consumers are willing to pay what it costs to honor their preferences.

For the model to produce efficient outcomes, consumers must shop their privacy preferences. Consumers must not only be aware of the content of privacy policies, but they also must incorporate that information into their decision whether to share personal information. In other words, privacy must be important enough to enter the decision-making calculus—to be a salient attribute in the consumer's decision process.[48] If privacy preferences are salient and consumers shop for privacy terms that meet their preferences, the market will produce efficient privacy policies, just as it does for other salient terms (price probably being the most common in purchasing transactions). If privacy is not salient, businesses offering weaker privacy terms than those that consumers prefer will capture a consumer surplus, i.e., get the benefit of personal information without paying or trading for it at the rate consumers would demand. The case for government intervention is then stronger.

47. The price need not be monetary for a privacy market to work. A site might offer greater download speeds, more striking graphics, special offers, more in-depth content, and other enticements to "purchase" users' personal information.

48. There is another assumption at work here. To shop effectively for privacy, consumers must be able to value their privacy interests. *See* Nehf, *supra* note 23, at 62–63. This is hugely problematic for a number of reasons. *Id.*

In many situations, consumers have privacy preferences, and, if forced to evaluate privacy terms, consumers would in fact give up some personal information in exchange for added value. We see this when consumers sign up for premium online services that offer video clips and other enhanced content in exchange for registration information or customer survey participation. Conversely, consumers sometimes pay more or give up discounts to have better privacy protection, as many refuse to use grocery store "convenience" cards because they do not want their purchasing habits tracked and traded.[49] When privacy terms are salient, the market can provide incentives for Web sites to provide strong privacy protection because doing so would attract new customers who value privacy above the cost of the Web site providing it, which would increase the site's profitability. When privacy terms are not salient, however, sites have less incentive to offer stronger privacy protections. They will not lose a significant number of customers by providing weak terms (or no privacy terms at all) because very few consumers will take notice. This creates a classic "lemons" problem in which most market participants offer weak, inefficient terms and pay no penalty for doing so.[50] Laws legitimately can be imposed to correct the imbalance.

C. Behavioral Studies Reveal Strong Consumer Privacy Preferences

The interactive nature of the Internet creates a unique environment for information gathering by Web site operators and thus increases consumer anxiety about privacy invasions.[51] Generally speaking, personal information can include both public and private data. Public data includes information that we either display regularly (such as a driver's tag number) or put on file in a public place (such as home mortgage information at the county recorder's office). Private data is information that we generally keep out of the public eye. As the Internet increases the ease with which data is collected, manipulated, and transferred, public information about us is growing as the private data

49. Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) urges the boycotting of stores that only give discounts to shoppers who use convenience cards. *See* Consumers Against Supermarket Privacy Invasion and Numbering, http://www.nocards.org (last visited Nov. 29, 2005).

50. Privacy terms may well be salient to some consumers, but to many others the terms are not salient. Inefficiencies still are present, however, even if some people shop for privacy. If a substantial number of consumers are in each group, we would expect some sites to offer strong privacy protections to attract the consumers for whom privacy is a salient attribute. Others would offer weak terms and be content to profit from customers for whom privacy is not so salient. Customers who shop for privacy terms will receive efficient terms by gravitating to the strong privacy sites. Those who do not shop for privacy will receive inefficient terms if, when forced to consider the issue, they would pay more than it costs a Web site to provide stronger privacy terms. If privacy is important but not salient for this group, sites with weak privacy protections reap a consumer surplus from them.

51. Sheehan & Hoy, *supra* note 44, at 62. *See* Pradeep K. Korgaonkar & Lori D. Wolin, *A Multivariate Analysis of Web Usage*, 39 J. ADVERTISING RES. 53, 57 (1999).

shrinks.[52] Social scientists have recognized this phenomenon and have studied how it affects consumer behavior online.

Research in behavioral economics suggests that consumers are concerned about information privacy. Unlike many standard terms in adhesion relationships, such as severability clauses, "time of the essence" language, or even arbitration clauses, consumers appear to have strong preferences when the subject of privacy is brought to their attention. In experimental settings, consumers are capable of acting rationally within the limits of the information to which they are exposed.[53] Numerous surveys and controlled experiments have found that consumers value privacy and generally want more privacy than they perceive they now have.[54] Researchers have asked consumers to make decisions that reveal their privacy preferences in a way that places the question firmly into the decision-making process.[55] When this happens, consumers profess to have strong privacy preferences.[56]

Several findings appear to be well supported. First, consumers generally are aware of privacy issues, and they are concerned about guarding their personal information.[57] Although not all consumers seem to care about online privacy, Internet users tend to cluster in three categories: "privacy guardians," who attach a relatively high value to information privacy; "information sellers," who have little regard for privacy and are willing to sell it for monetary rewards; and "convenience seekers," who prefer Web site convenience to information privacy safeguards.[58] When asked in surveys or controlled experiments, many

52. Caudill & Murphy, *supra* note 35, at 10. Even church Web sites post a great amount of personal information, including details about illnesses, church member addresses, personal vacation schedules, and names and locations of members serving as missionaries. *See* Mariea Grubbs Hoy & Joseph Phelps, *Consumer Privacy and Security Protection on Church Web Sites: Reasons for Concern*, 22 J. PUB. POL'Y & MARKETING 58, 66 (2003). In one study, less than 3% of these sites posted a privacy policy, and less than 25% posted a statement about privacy practices. *Id.* at 68.

53. David A. Sheluga et al., *Preference, Search, and Choice: An Integrative Approach*, 6 J. CONSUMER RES. 166, 175 (1979).

54. Phelps, Nowak & Ferrell, *supra* note 40, at 29. A caveat is in order here. Research on privacy in e-commerce is still in the nascent stage and always will lag behind the fast moving market for Internet services. *See id.* at 40. As soon as research findings are published about online commercial or consumer practices, they are soon outdated. *See id.* at 39–40. Consumer attitudes and marketing behavior are constantly changing, and there is a continual need for updating research on consumer beliefs, behaviors, and preferences. *Id.*

55. One fundamental concept of behavioral economics is the behavioral contingency, which posits a stimulus, a response, and the ensuing outcome of the response, which derives from Skinnerian behaviorism. Gordon R. Foxall, *The Behavior Analysis of Consumer Choice: An Introduction to the Special Issue*, 24 J. ECON. PSYCHOL. 581, 582–83 (2003). In the context of consumer privacy on the Internet, a behavioral theorist might posit that the stimulus of economic (or other) rewards for information will elicit a consumer response of more information released, and the outcome will be a satisfied consumer who feels better off after the exchange. Such a consumer therefore would be inclined to repeat the transaction.

56. Sheehan & Hoy, *supra* note 44, at 63.

57. *Id.*

58. IL-HORN HANN ET AL., AEI-BROOKINGS JOINT CTR. FOR REGULATORY STUDIES, THE VALUE OF ONLINE INFORMATION PRIVACY: AN EMPIRICAL INVESTIGATION 15 (2003), *available at* http://www.aei-brookings.org/admin/authorpdfs/page.php?id=297.

consumers fall into the first group and show great concern about database privacy.[59] In one study, online threats to privacy were a concern to more than three-quarters of Internet users.[60] All but a small minority of consumers were either very concerned or somewhat concerned about the ways companies use personal information.[61] Most did not think that marketing companies are sufficiently concerned about protecting privacy.[62] A majority believed that companies already know too much about them.[63] Two-thirds thought there should be limits on how much information businesses can collect about consumers.[64] The vast majority desire more control over how companies use information after they obtain it.[65] If consumers suspect that a business will use information beyond the original transaction, they become increasingly concerned.[66] Indeed, possible usage beyond the original purpose is the most important factor influencing consumer disclosure of information and is often viewed as an invasion of privacy and an illegitimate misappropriation of the information for commercial purposes.[67]

Second, although many consumers value their information, they also are willing to trade information for other benefits.[68] Consumers generally believe that they own their personal information and should have control over its collection and usage.[69] Conversely, marketers tend to believe that they own any information that they can obtain lawfully.[70] People are more willing to disclose information if they obtain something of value in exchange.[71] Consumers who are aware of the value of their information will ask for rewards in exchange for disclosure, suggesting that consumers can place a value on personal information and that data can be elicited through monetary and other trade-offs.[72]

Third, people who are aware of data-collection practices also tend to be aware that personal information likely will be used for profit and that

---

59. *Id.*

60. Caudill & Murphy, *supra* note 35, at 7 (discussing a U.S. Department of Commerce study that found 81% of Internet users concerned about online threats to privacy). A survey by the Accenture firm in 2003 found that 97% of consumers were "concerned" about information privacy. *See* Accenture Survey, *supra* note 7, at 2.

61. Phelps, Nowak & Ferrell, *supra* note 40, at 33.

62. *Id.*

63. *Id.*

64. *Id.*

65. *Id.*

66. Sheehan & Hoy, *supra* note 44, at 63.

67. *Id.*; *see also* Cespedes & Smith, *supra* note 35, at 10.

68. Sheehan & Hoy, *supra* note 44, at 63.

69. *Id.* at 64.

70. *Id.*

71. Robert McKim, *Information: The Newest Currency*, TARGET MARKETING, Jul. 1999, at 36, 39; Sheehan & Hoy, *supra* note 44, at 68.

72. Little is known, however, about how the trade-offs will affect long-term interests. Nadia Olivero & Peter Lunt, *Privacy Versus Willingness to Disclose in E-commerce Exchanges: The Effect of Risk Awareness on the Relative Role of Trust and Control*, 25 J. ECON. PSYCHOL. 243, 245 (2004); Sheehan & Hoy, *supra* note 44, at 64.

it has exchange value.[73] They show a pragmatic attitude and account for the risk in two ways.[74] First, they may be willing to disclose but only if they are properly rewarded.[75] Rewards can be open and specific.[76] One study showed that, when informed about the extent of collection and use of personal information, consumers valued protection against errors, improper access, and secondary use at approximately $30–$45 per transaction.[77] Second, because they assume the information will be sold to third parties, informed consumers disclose only those bits of information that are not perceived to be particularly risky or too valuable to risk trading without high rewards in exchange.[78]

Fourth, educated, experienced, and knowledgeable consumers tend to be more concerned and take more precautions to protect their personal information. High levels of technical knowledge positively correlate with privacy concerns.[79] Better educated and more affluent computer users are more likely to refuse to share personal information online.[80] Consumers who had attended some college or vocational school but did not have a college degree showed the highest levels of privacy concern.[81] Frequent online users are most concerned that information

---

73. Olivero & Lunt, *supra* note 72, at 257.

74. *Id.*

75. Caudill & Murphy, *supra* note 35, at 8.

76. One marketing company offered $40 in discount coupons for demographic data and information about the consumer's preferred supermarket. *Id.*

77. Based on a conservative figure of fifty-eight million purchases over the Internet annually, the benefits of privacy protection online could be valued at $1.77 to $2.59 billion per year. HANN ET AL., *supra* note 58, at 18. Studies also have shown, however, that promised rewards for information can be counterproductive as a way to elicit information from consumers. Olivero & Lunt, *supra* note 72, at 258. Awareness of the risks of sharing personal information increases the desire of individuals to control the information being collected and restrict how it is being used. *Id.* Thus, by offering discounts or other rewards, a business can raise consumer awareness of privacy issues, and as the business highlights the activity (and its value), resulting suspicions can reduce the degree of trust the consumer has in the data collector. *Id.* In behavioral economic terms, the stimulus (promised rewards) elicits an unfavorable response (greater awareness of risk). Therefore, it may be counterproductive for the data collector to offer rewards openly in exchange for information disclosure. Sheehan & Hoy, *supra* note 44, at 64. Compensating the consumer can turn a clandestine data-mining activity into an overt, and hostilely perceived, solicitation. *Id.*

78. Olivero & Lunt, *supra* note 72, at 250. Individual-specific data used for marketing purposes generally falls into one of five categories: demographic data; lifestyle interests (including media habits); shopping behavior; financial data (including credit data); and personal identifiers (social security number, names, addresses). *See* Phelps, Nowak & Ferrell, *supra* note 40, at 28. Consumers are most willing to share demographic data and lifestyle information and least willing to share financial data and personal identifiers. *Id.* at 33. Surveyed consumers were unwilling or not very willing to share annual household income, kinds of credit cards possessed, Social Security numbers, and most recent credit card purchases. *Id.* These consumers generally were willing to reveal favorite hobbies, age, marital status, occupation, and education level. *Id.*; Sheehan & Hoy, *supra* note 44, at 64.

79. Olivero & Lunt, *supra* note 72, at 250.

80. *See, e.g.*, George R. Milne & Andrew J. Rohm, *Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives*, 19 J. PUB. POL'Y & MARKETING 238, 241 (2000).

81. Phelps, Nowak & Ferrell, *supra* note 40, at 36.

will be shared with third parties.[82] Consequently, savvy online consumers provide false information about themselves approximately one-fourth of the time.[83] Informed individuals demand more control over their information for two reasons: as a protection against misuse and as an extension of a perceived right of ownership in the information.[84] Being aware of the value of the information, consumers assert increased control both to protect their vulnerability and to prevent exploitation of their interests by others without just rewards.[85]

Fifth, perceived risk can be reduced, and more information shared, when consumers have developed a feeling of trust with the data collector.[86] When consumers are faced with uncertainty and risk, the reputation of the data collector becomes increasingly important.[87] People are more willing to disclose data when they have an established relationship with a data collector or when the collector is well known and has an image to maintain.[88] A data collector's desire to maintain its reputation is a perceived deterrent to data misuse.[89] If consumers have an established relationship with the data collector, they usually have fewer privacy concerns.[90] There is some evidence that consumers would be willing to disclose more information if they knew a trusted party (whether a business or governmental entity) was monitoring use and control of the information after disclosure.[91]

In sum, several factors appear to influence the level of consumer concern about sharing information with businesses: (1) the type of information requested, such as demographic, lifestyle interests, media habits, personal identifiers, or financial data[92]; (2) the amount of control the consumer has over the use of the information[93]; (3) the potential consequences and benefits of the exchange (for instance, increased volume of junk mail or risk of identity theft versus shopping savings or convenience)[94]; and (4) characteristics of the individual consumer,

82. George R. Milne, *Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue*, 19 J. PUB. POL'Y & MARKETING 1, 4 (2000).

83. *Id.*

84. Olivero & Lunt, *supra* note 72, at 257.

85. *Id.*

86. Milne & Rohm, *supra* note 80, at 239.

87. Olivero & Lunt, *supra* note 72, at 259.

88. *Id.*; *see* David Knights et al., *Chasing Shadows: Control, Virtuality and the Production of Trust*, 22 ORG. STUD. 311, 321 (2001).

89. Olivero & Lunt, *supra* note 72, at 259.

90. Sheehan & Hoy, *supra* 44, at 68.

91. Olivero & Lunt, *supra* note 72, at 251, 255.

92. Phelps, Nowak & Ferrell, *supra* note 40, at 30.

93. *Id*. Perceived lack of control of information on the Internet has two dimensions: (1) an environmental dimension—information can be obtained through unauthorized access and data-mining activities (e.g., theft, fraud, cookies, or hacking); (2) the uncertainty of use by the data collector after mining the data—it may use the information for purposes not expected by the individual or it may sell the information to third parties. Olivero & Lunt, *supra* note 72, at 244.

94. Phelps, Nowak & Ferrell, *supra* note 40, at 30.

including demographic characteristics, prior experiences, technical knowledge, and shopping habits.[95] Controlled surveys and experimental studies show that people will (or will not) give up their personal information based upon the results of a "privacy calculus" that assesses whether their information will be used fairly and whether negative consequences might result in the future.[96]

To assist consumers in the calculus, several researchers have concluded that consumers must be able to control the amount and type of information collected and they must have knowledge about the manner in which the information will be used. Behavioral economists often conclude that consumer awareness of privacy options is key to the functioning of a self-regulatory system.[97] Many urge the adoption of fair information practices to assist the consumer in performing the calculus, so long as the practices are adequately disclosed and followed. In this way, fair information practices actually can be good for businesses that want to elicit more information from their customers.[98]

More important, these findings suggest that consumers have incentives and are motivated to shop for privacy terms and that firms have incentives to respond to consumer preferences. Consumers seem to care enough about privacy to seek information about privacy practices, so they may take those practices into account when deciding whether and with whom to share personal information. Indeed, there is some evidence that a market for information privacy is developing. Studies have shown that by adopting fair information practices a business can elicit more disclosure from consumers because the gesture builds trust.[99] Research also has shown that Web site disclosures regarding privacy practices and information security are positively related to the likelihood of online purchases.[100] All of this suggests that a market for information

95. *Id.*; *cf.* Sheehan & Hoy, *supra* note 44, at 64 (outlining three factors that influence the level of privacy concern: (1) how sensitive the person considers the particular information being disclosed; (2) how familiar the person is with the entity collecting the information; and (3) what the person is receiving in exchange for the information).

96. HANN ET AL., *supra* note 58, at 7.

97. Mary J. Culnan, *Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing*, 9 J. DIRECT MARKETING 10, 18–19 (1995) (recommending that opt-out procedures explicitly be conveyed to consumers); Milne & Rohm, *supra* note 80, at 244, 248 (concluding that the least preferred opt-out method is a requirement that consumers call or write the business to remove or restrict use of the information and arguing for greater disclosure to promote awareness because only 34% of regular computer users were aware of data-collection practices and also aware that opt-out opportunities existed, and 70% of respondents wanted to be reminded of opt-out opportunities beyond the first transaction with the business).

98. Culnan, *supra* note 39, at 21. *See generally* Accenture Survey, *supra* note 7 (surveying consumer privacy preferences).

99. Mary J. Culnan & Pamela K. Armstrong, *Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation*, 10 ORG. SCI. 104, 112 (1999); Olivero & Lunt, *supra* note 72, at 244.

100. Anthony D. Miyazaki & Ana Fernandez, *Internet Privacy and Security: An Examination of Online Retailer Disclosures*, 19 J. PUB. POL'Y & MARKETING 54, 58 (2000) (finding only 17% of Web sites surveyed disclosed that they would not share personal information with third parties).

privacy may be emerging and that government intervention is not necessary to ensure efficient privacy practices online.

D. Decision-Making Theory and Research on Saliency

In controlled surveys, consumers value privacy and strive for accuracy in their decision making. Yet consumers seldom read privacy policies and seldom even cite them as a factor in deciding which business to use or Web sites to frequent. A study of 1500 adult Internet users concluded that less than one percent thought a Web site's privacy policy was relevant in determining the site's credibility.[101] In another study, which was designed specifically to demonstrate to corporate executives that consumers have a high concern for privacy, less than half of consumers said privacy was among the top three factors influencing consumer trust with a company.[102] If privacy is so important, why do consumers not bother to learn about the privacy practices of the firms with which they do business and share information?

The simplest answer may be that consumers seldom act rationally.[103] It is debatable whether rational behavior is the principal objective for highly structured organizational decision making; it is highly questionable whether individuals consistently pursue goals with rational thought processes. What applies to firms and other organizations may not apply in the same way or at all to an individual consumer.[104] In all likelihood, no person is capable of responding to outside stimuli in a strictly rational way.

If a privacy policy is to influence a consumer's rational choice, several cognitive steps must occur in sequence. A source (Web site) must transmit a stimulus (message) in order to reach a receiver (the consumer) for the purpose of achieving certain effects (such as Web site use or product purchase). The receiver then must render a series of responses or effects in response to the stimulus, perhaps ultimately resulting in some action being taken in consequence.[105] Specifically, for a stimulus (such as disclosure of privacy terms) to elicit a response, the

---

101. FOGG ET AL., *supra* note 43, at 6, 86.

102. Accenture Survey, *supra* note 7, at 9.

103. Researchers have studied consumer decision processes and began questioning the rational choice model since at least the mid-1960s. *See* JOHN A. HOWARD & JAGDISH N. SHETH, THE THEORY OF BUYER BEHAVIOR 379 (1969); FRANCESCO M. NICOSIA, CONSUMER DECISION PROCESSES: MARKETING AND ADVERTISING IMPLICATIONS 39 (1966).

104. Jacob Jacoby, *Is it Rational to Assume Consumer Rationality? Some Consumer Psychological Perspectives on Rational Choice Theory*, 6 ROGER WILLIAMS U. L. REV. 81, at 102–03 (2000).

105. The model depicted here is a simplification. Many variations exist, with some depicting at least fifteen separate stages in the receiver's reaction to the incoming communication. *See generally* William J. McGuire, *Attitude Change: The Information-Processing Paradigm*, *in* EXPERIMENTAL SOC. PSYCHOL. 108, 119–20 (Charles Graham McClintock ed., 1972) (discussing behavioral steps in persuasion); William J. McGuire, *Some Internal Psychological Factors Influencing Consumer Choice*, 2 J. CONSUMER RES. 302 (1976) (providing a good overview).

target must first be exposed to the stimulus. The exposure must draw the attention and perception of the target, who must then process and comprehend the information.[106] Having comprehended it, the target must evaluate its relative importance in the decision-making process, use it in the calculus to make a choice, and finally engage in the chosen behavior. Only the very last effect takes the form of overt behavior, such as the choice to use one Web site over another or to reveal some personal information. Because the effects produced by a stimulus generally occur in sequential form, failure at one stage either eliminates or severely limits what happens at subsequent stages, which weakens or eliminates the effect of the stimulus on the receiver.

Viewing the decision-making process in several stages has important implications for rational choice theory. It is not enough that behavioral models show rational decision making in controlled experiments; the models also must describe behavior in realistic environments in which failures at each stage in the decision process can and often do occur.[107] People generally do not make decisions with a perfectly rational weighted-adding calculus. Nor, however, do they act randomly. Consumers make decisions under conditions of limited or bounded rationality because they have limited capacity for understanding and using information at each stage in the process.[108] Considerable research shows that most consumer behavior is predicated upon "low effort" or "low involvement" decision making using a limited number of stimuli in less than rational ways.[109] This does not necessarily mean that consumers are acting irrationally, but they may be pursuing other goals besides strict accuracy of the decision. It is therefore important to examine other goals that consumers pursue as they make decisions and how those goals may affect consumer decision making online.

106. Much of the information that reaches consciousness has multiple meanings, with some of these meanings registering, through symbolism or metaphorical allusion, at less than conscious levels. Jacoby, *supra* note 104, at 104.

107. Christine Jolls et al., *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471, 1500 (1998).

108. Theories of bounded rationality emerged in the 1950s. *See* Herbert A. Simon, *A Behavioral Model of Rational Choice*, 69 Q.J. ECON. 99, 99 (1955). Limitations include memory capacity and computational abilities. Bettman et al., *supra* note 46, at 187. Consumer behavior literature also provides numerous bases from which to argue that the consumer does not necessarily make her choice from a stable set of preferences. "For example, if preference sets remained stable, one might predict high levels of brand loyalty, approaching 100%. Yet, in a very large number of product categories, the rates of brand loyalty are below (sometimes appreciably below) 50% . . . ." Jacoby, *supra* note 104, at 106. In addition, consumers often exhibit strong exploratory or variety-seeking behavior. *Id.* "Though they may have a pre-existing set of option preferences, consumers also derive enjoyment in departing from this preference set." *Id.* *See* MICHAEL J. APTER, THE DANGEROUS EDGE: THE PSYCHOLOGY OF EXCITEMENT 63 (1992) (discussing the concept of "detachment frame").

109. *See generally* WAYNE D. HOYER & DEBORAH J. MACINNIS, CONSUMER BEHAVIOR 139–61 (1997) (discussing the cognitive bases of consumer attitudes).

1. Categories of Bounded Rational Decision Strategies

There are several broad categories of bounded rational decision making.[110] In the lexicographic strategy, the decision maker selects the alternative that has the best value on the most important attribute only (e.g., price).[111] The decision maker ignores other attributes.[112] This is the easiest strategy to apply because the decision maker compares only one attribute among alternatives, but it yields the least efficient result for the same reason.[113] An alternative may win because it was best on the most important attribute, but other alternatives may have been much better on other attributes and would have prevailed if those attributes had been brought into the calculus.[114]

In the conjunctive or satisficing strategy, the decision maker selects the first alternative that meets a minimum level of acceptability on all attributes, regardless of the amount by which the levels are exceeded.[115] Having made a satisfactory choice on this basis, the decision maker does not even evaluate other alternatives.[116] For example, having decided on a maximum price and a minimum level of acceptability on other factors, the decision maker chooses the first alternative that satisfies all threshold levels.[117] If no alternative meets the minimum level for all attributes, the levels are relaxed and the process repeated.[118] This strategy can be expedient but inefficient because while decision makers end up with a minimally satisfying choice, other choices might have been preferred if the decision maker had taken the time to evaluate them.[119]

The elimination-by-aspects strategy combines elements of the lexicographic and satisficing strategies.[120] The decision maker decides which attribute is most important and eliminates all alternatives that do not meet a minimum level of acceptability on that attribute.[121] If more than one alternative satisfies that inquiry, the decision maker then sets a

110. Related concepts of bounded willpower and bounded self-interest also may be important here. *See* Jolls et al., *supra* note 107, at 1479–81. Bounded willpower becomes most relevant when decisions have consequences over time, for example, when benefits are immediate but costs are deferred. *Id.* People often make choices that they know conflict with their long-term interests. *Id.* For example, most smokers say they would be better off quitting, yet they continue to smoke because their will is overcome by chemical addiction or other influences. *Id*. Bounded self-interest refers to the fact that people often act as if they care about others, even strangers, when it is not in their self-interest to do so and when there will be no societal repercussions if they behave unfairly. *Id*. at 1479. For example, people usually leave tips in out-of-town restaurants that they likely will never visit again. *Id.* at 1493.

111. Bettman et al., *supra* note 46, at 190.

112. *Id.*

113. *Id.*

114. *Id.* at 190–91.

115. *Id.* at 190.

116. *Id.*

117. *Id.*

118. *Id.*

119. *See id.*

120. *Id.*

121. *Id.*

minimum value on the next most important attribute.[122] Several alternatives may satisfy the maximum price point, for example, so the decision maker moves to the next most important attribute (e.g., reliability) and eliminates alternatives that do not meet the acceptable level for that attribute, and so on until all but one alternative has been eliminated.[123] This strategy can result in inefficient choices because while the ultimate choice is the only one that meets a minimum level of acceptability on all attributes, other choices might have received a higher total value.[124] For example, if an alternative failed the minimum test on one attribute (color) but exceeded the levels on other attributes by a great amount, it might have netted a higher total value than the chosen alternative.

In the majority-of-confirming-dimensions or "playoff" strategy, alternatives are considered in pairs, with each attribute of the two alternatives facing off against each other (e.g., price of *A* versus price of *B*, reliability of *A* versus reliability of *B*, and so on).[125] Between the two alternatives, the one that wins more attribute contests then moves on to battle the next alternative, and this continues until only one survivor remains.[126] This strategy can be inefficient because in any particular playoff, one alternative could win the majority of attribute battles by small margins and lose the minority by big margins. Thus, the losing alternative actually might be the better choice if the decision maker had used a more complex strategy.

People often combine elements of different strategies and shift back and forth among them as they construct a decision process.[127] For the purpose of examining choices made online, the important point is that regardless of the strategy employed, consumers ignore information that they should consider if market incentives are to produce efficient outcomes. In all decision strategies, the critical question is which attributes are likely to be salient, and therefore evaluated, and which ones are not.[128] If privacy is seldom a salient attribute for consumers and there are rational reasons leading to this result, then market behavior is not likely to produce more efficient privacy practices.

---

122. *Id.* at 191. *See generally* Amos Tversky, *Elimination by Aspects: A Theory of Choice*, 79 PSYCHOL. REV. 281 (1972) (discussing the covert elimination process involved in decision making).

123. Bettman et al., *supra* note 46, at 191.

124. *Id.* at 190–91.

125. *Id.*

126. *Id. See generally* J. Edward Russo & Barbara Anne Dosher, *Strategies for Multiattribute Binary Choice*, 9 J. EXPERIMENTAL PYSCHOL.: LEARNING, MEMORY, AND COGNITION 676 (1983) (exploring empirically the information-processing strategies used in multi-attribute binary choice).

127. Bettman et al., *supra* note 46, at 191.

128. *See id.* at 190–91.

2. Rational Decision-Making Goals Besides Maximum Accuracy

People have limited cognitive abilities and resources, and they use them judiciously.[129] They choose decision strategies that are a compromise between their desire for complete accuracy and their desire to achieve other goals.[130] Besides maximizing accuracy of the decision, another important goal is the minimization of cognitive effort.[131] When making decisions, people tend to expend only as much effort as is necessary to reach a satisfactory, rather than optimal, decision.[132] As circumstances require more cognitive effort to process available information, decision makers often choose decision methods that are easier to implement but less accurate.[133] Moreover, when consumers must exert more cognitive effort to evaluate a particular alternative, they often are less inclined to prefer it to alternatives that require less effort to evaluate, unless the alternative that required more effort was clearly superior.[134] In other words, exerting more cognitive effort results in a "negative affect" associated with that alternative and makes that alternative less appealing simply because it was harder to evaluate.[135]

Another important goal in consumer decision making is minimizing the negative emotional response that individuals experience when forced to make difficult trade-offs. People are emotional beings, and choices sometimes involve wrenching decisions, requiring that the decision maker give up something of value that she does not wish to lose.[136] People want to minimize the discomfort that arises from facing emotion-laden choices, and they tend to select decision strategies that further this goal.[137] This can reduce the accuracy of the decision because the individual will avoid certain parts of the calculus that require discomforting comparisons. When this occurs, individuals focus their attention elsewhere and choose strategies that allow them to avoid making the uncomfortable comparison.[138]

---

129. Ellen C. Garbarino & Julie A. Edell, *Cognitive Effort, Affect, and Choice*, 24 J. CONSUMER RES. 147, 148 (1997); *see* John W. Payne, *Contingent Decision Behavior*, 92 PSYCHOL. BULL. 382, 382 (1982).

130. Garbarino & Edell, *supra* note 129, at 149.

131. Bettman et al., *supra* note 46, at 192.

132. Garbarino & Edell, *supra* note 129, at 148.

133. *Id*. at 149; Eric J. Johnson et al., *Information Displays and Preference Reversals*, 42 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 1, 19 (1988); Denis A. Lussier & Richard W. Olshavsky, *Task Complexity and Contingent Processing in Brand Choice*, 6 J. CONSUMER RES. 154, 154 (1979).

134. Garbarino & Edell, *supra* note 129, at 152–53, 156.

135. *Id.*

136. *See* Bettman et al., *supra* note 46, at 193; Richard S. Lazarus, *Progress on a Cognitive-Motivational-Relational Theory of Emotion*, 46 AM. PSYCHOLOGIST 819, 819 (1991).

137. Mary Frances Luce, *Choosing to Avoid: Coping with Negatively Emotion-Laden Consumer Decisions*, 24 J. CONSUMER RES. 409, 409 (1998).

138. *Id.*; *see* Philip E. Tetlock, *The Impact of Accountability on Judgment and Choice: Toward a Social Contingency Model*, *in* 25 ADVANCES IN EXPERIMENTAL SOCIAL PSYCHOLOGY 331, 335 (Mark P. Zanna ed., 1992); Amos Tversky & Eldar Shafir, *Choice Under Conflict: The Dynamics of Deferred Decision*, 3 PSYCHOL. SCI. 358, 358 (1992).

Depending on the context, one or more of these goals—accuracy, cognitive ease, and emotional comfort—may be more prominent in the decision process. For example, when faced with an irreversible decision that will have profound effects on her life, the decision maker may care less about cognitive ease and emotional comfort and work harder to make the most accurate choice. The decision maker's ability to get feedback about her choice also influences the relative weight given to each goal. In general, feedback about cognitive effort and emotional comfort will be more immediate and less ambiguous than feedback about the accuracy of the choice.[139] When that occurs, the decision maker is more likely to give less weight to the accuracy goal and more weight to the two other goals.

3. Factors Influencing Consumer Choice

As consumers pursue the three decision-making goals, the likelihood that a consumer will process a stimulus, and thereby make it salient, is influenced by several factors that are relevant to online behavior.

Number of attributes. Research suggests that the number of attributes decision makers are capable of investigating and integrating into the decision process is as few as five, though the number will vary depending on the individual and the context.[140] For example, an automobile purchasing decision may involve a detailed comparison of several attributes of many competing models, or the consumer may simply choose to purchase the same model he bought the last time.[141]

Time available to make the decision. When time for making a decision is scarce, people switch to decision strategies that accelerate their information processing, such as lexicographic or elimination-by-aspects strategies. When time pressure is severe, quickly scanning several pieces of information is more effective than examining fewer in depth.[142] Moreover, when time pressure is present, consumers tend to weigh negative information more heavily than positive.[143]

---

139. Bettman et al., *supra* note 46, at 193; *see also* Hillel J. Einhorn, *Learning from Experience and Suboptimal Rules in Decision Making*, *in* COGNITIVE PROCESSES IN CHOICE AND DECISION BEHAVIOR 1, 8 (Thomas S. Wallsten ed., 1980).

140. Lussier & Olshavsky, *supra* note 133, at 162; Richard W. Olshavsky, *Task Complexity and Contingent Processing in Decision Making: A Replication and Extension*, 24 ORGANIZATIONAL BEHAV. & HUM. PERFORMANCE 300, 314 (1979).

141. Bettman et al., *supra* note 46, at 189.

142. John W. Payne et al., *When Time Is Money: Decision Behavior Under Opportunity-Cost Time Pressure*, 66 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 131, 145 (1996); Rik Pieters et al., *The Effect of Time Pressure and Task Motivation on Visual Attention to Brands*, *in* 24 ADVANCES IN CONSUMER RES. 281, 281 (Merrie Brucks & Deborah J. MacInnis eds., 1997); *see also* Bettman et al., *supra* note 46, at 200.

143. Peter Wright, *The Harassed Decision Maker: Time Pressures, Distractions, and the Use of Evidence*, 59 J. APPLIED PSYCHOL. 555, 555–56 (1974).

Perceptibility of the attribute. If people do not notice an attribute or stimulus, it cannot have an impact on their decision process.[144] People pay attention to attributes either voluntarily or involuntarily. Some attributes may be unavoidable and get noticed automatically. Stimuli that are surprising, novel, threatening, or otherwise perceptually striking can capture attention involuntarily.[145] Otherwise, a person must have some motivation that prompts her to seek the information voluntarily.

Importance of the attribute in attaining the consumer's objectives. For information that is not intrinsically noticeable, people voluntarily direct attention to (and actively seek information about) attributes that are particularly important to them, attributes that will help them reach their intended objective with the decision.[146]

Inferences. Even if the attribute is important, people may infer the missing value in one of two ways rather than investigate further. They may infer a value from the values they know from other alternatives, i.e., assume that the attribute is similar across brands (for example, all car warranties are similar). Or they may infer a value in line with the values they assigned to other attributes of the given option, i.e., assume that the value is comparable to other attributes for that option (for instance, because the engineering is first-rate, the warranty probably is as well).[147] With respect to "noncontractible" characteristics such as service quality, consumers often choose to use a firm's brand as a proxy for credibility rather than investigate the characteristic more completely.[148]

Framing effects. The form and manner in which information is provided will affect its saliency.[149] Consumers process information in a way that is congruent with the format of presentation; they process the information in the form presented without rearranging it.[150] This is

144. *See generally* B.J. Fogg, *Prominence-Interpretation Theory: Explaining How People Assess Credibility Online*, PROCEEDINGS OF ACM CHI 2003 CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 722 (2003), *available at* http://credibility.stanford.edu/pdf/PITheory.pdf (describing prominence-interpretation theory and the process of noticing and interpreting prominent elements).

145. Bettman et al., *supra* note 46, at 193.

146. *See id.*

147. Gary T. Ford & Ruth Ann Smith, *Inferential Beliefs in Consumer Evaluations: An Assessment of Alternative Processing Strategies*, 14 J. CONSUMER RES. 363, 370–71 (1987); Richard D. Johnson & Irwin P. Levin, *More than Meets the Eye: The Effect of Missing Information on Purchase Evaluations*, 12 J. CONSUMER RES. 169, 170 (1985).

148. Michael D. Smith & Erik Brynjolfsson, *Consumer Decision-Making at an Internet Shopbot: Brand Still Matters*, 49 J. INDUS. ECON. 541, 556 (2001), *available at* http://www.econ.jhu.edu/people/harrington/375/sb01.pdf; *see* Birger Wernerfelt, *Umbrella Branding as a Signal of New Product Quality: An Example of Signalling by Posting a Bond*, 19 RAND J. ECON. 458, 458–59 (1988).

149. *See, e.g.*, W. Kip Viscusi, *Individual Rationality, Hazard Warnings, and the Foundations of Tort Law*, 48 RUTGERS L. REV. 625, 630–36 (1996) [hereinafter Viscusi, *Individual Rationality*]; W. Kip Viscusi et al., *An Investigation of the Rationality of Consumer Valuations of Multiple Health Risks*, 18 RAND J. ECON. 465, 477–78 (1987) [hereinafter Viscusi, *An Investigation*].

150. *See* James R. Bettman & Michel A. Zins, *Information Format and Choice Task Effects in Decision Making*, 6 J. CONSUMER RES. 141, 142 (1979).

sometimes referred to as the "concreteness" principle.[151] The effect is most pronounced when consumers perceive the costs of accepting the given format (both the costs of delving deeper into the subject and the lost accuracy in accepting it as given) as low.[152] Only if costs of format acceptance are perceived to be high or the information is presented in a disorganized or confusing way will consumers discount the format as presented and seek additional information.[153] Advertisers are well aware of this, and when describing risks, they may describe them in the least frightening or most favorable way as possible. The announcer in a television advertisement for a prescription drug might describe adverse side effects in the same uplifting voice as he used to describe the drug's benefits, hoping to discount their negative effect. Research shows that labeling beef as 75% lean results in more favorable impressions than labeling it 25% fat.[154] People often choose between descriptions of options rather than the options themselves, accepting the description as accurate.[155]

Negative reaction to commodification. People feel conflicted when trying to compare attributes that are dissimilar, especially when the comparison asks people to put a price on something they intuitively believe should not be commodified or traded away.[156] The problem is most acute when people are asked to trade values they view as "sacred" or "protected" (namely, life, liberty, and justice).[157] Consequently, the

151. Paul Slovic, *From Shakespeare to Simon: Speculation—and Some Evidence—About Man's Ability to Process Information*, OR. RES. INST. RES. BULL. (Or. Res. Inst., Eugene, Or.), Apr. 1972, at 9, http://www.decisionresearch.org/pdf/dr36.pdf.

152. Eloise Coupey, *Restructuring: Constructive Processing of Information Displays in Consumer Choice*, 21 J. CONSUMER RES. 83, 96–99 (1994).

153. *Id.*

154. Irwin P. Levin & Gary J. Gaeth, *How Consumers Are Affected by the Framing of Attribute Information Before and After Consuming a Product*, 15 J. CONSUMER RES. 374, 377 (1988).

155. A related finding is that people tend to weigh potential losses more heavily than potential gains. Thus, framing consequences in terms of losses rather than gains may be more effective in changing behavior. For example, promoting screening tests for breast cancer is more effective if women are told of the harms that can result from not screening rather the benefits of screening. Jolls et al., *supra* note 107, at 1536–37. In addition, people tend to think of risks in terms of proportions rather than differences. People think it is more important to reduce a 15% risk to 5% than to reduce a 70% risk to 50%. *See* Jonathan Baron, *Confusion of Relative and Absolute Risk in Valuation*, 14 J. RISK & UNCERTAINTY 301, 301–03 (1997); Karen E. Jenni & George Loewenstein, *Explaining the "Identifiable Victim Effect,"* 14 J. RISK & UNCERTAINTY 235, 254 (1997).

156. Bettman et al., *supra* note 46, at 189; *see* James R. Bettman & Mita Sujan, *Effects of Framing on Evaluation of Comparable and Noncomparable Alternatives by Expert and Novice Consumers*, 14 J. CONSUMER RES. 141, 141 (1987).

157. *See* Jonathan Baron & Mark Spranca, *Protected Values*, 70 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 1, 2 (1997); Philip E. Tetlock et al., *Revising the Value Pluralism Model: Incorporating Social Content and Context Postulates*, *in* 8 THE PSYCHOLOGY OF VALUES: THE ONTARIO SYMPOSIUM ON PERSONALITY AND SOCIAL PSYCHOLOGY 25 (Clive Seligman et al. eds., 1996).

more easily comparable attributes carry more weight in the decision process, and difficulties in comparing attributes are discounted.[158]

Likelihood of risk. People are not good at making probability estimates for low-probability risks. People either overestimate the probability and take excessive precautions, or they ignore the risk altogether. For low-probability risks, people tend to view them in black-or-white terms—safe or unsafe—and overestimate the likelihood of small probabilities occurring. For example, when asked about the risks of lung cancer to smokers, both smokers and nonsmokers generally overestimate the risk.[159] Low-stated probabilities, therefore, have more effect on consumer behavior than they should.[160] On the other hand, consumers are not willing to pay anything to reduce a risk that they perceive to be a very low or effectively non-existent probability.[161] People are more likely to consider risks (whether high or low probability) and assess them accurately if they have experience with that type of risk.[162]

Action vs. inaction. People are more concerned about the harms that result from actions than those resulting from omissions.[163] For example, people may resist vaccinations because of the side effects, even when the risk of not vaccinating is greater.[164] This phenomenon seems to result from a belief that actions cause the harm, and causality is important. Actions with direct harmful effects are considered worse than actions with indirect effects.[165] The law often incorporates a similar bias. Companies are more likely to be sued for actions they take (such as the side effects of a drug or the making of a false claim) but seldom for failure to produce a product or the omission of information that might be helpful in a decision-making process.

"Gut" feelings and affect cues. One common heuristic is the intangible or "gut" feeling one associates with a particular alternative. Consumers often base decisions upon feelings derived from their experiences with an alternative (affect cues) rather than a strict weighted-adding strategy. For example, consumers may purchase automobiles partly because of the feelings they have when test driving a

158. Bettman et al., *supra* note 46, at 188; Stephen M. Nowlis & Itamar Simonson, *Attribute-Task Compatibility as a Determinant of Consumer Preference Reversals*, 34 J. MARKETING RES. 205, 205–06 (1997).

159. W. Kip Viscusi et al., *Smoking Risks in Spain: Part III—Determinants of Smoking Behavior*, 21 J. RISK & UNCERTAINTY 213, 214 (2000).

160. *See* Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis of Decision Under Risk*, 47 ECONOMETRICA 263, 284–89 (1979).

161. Gary H. McClelland et al., *Insurance for Low Probability Hazards: A Bimodal Response to Unlikely Events*, 7 J. RISK & UNCERTAINTY 95 (1993).

162. Bettman et al., *supra* note 46, at 188.

163. *See generally* Mark Spranca et al., *Omission and Commission in Judgment and Choice*, 27 J. EXPERIMENTAL SOC. PSYCHOL. 76 (1991) (discussing the bias to favor harmful omissions rather than harmful commissions).

164. Jacqueline R. Meszaros et al., *Cognitive Processes and the Decisions of Some Parents to Forego Pertussis Vaccination for Their Children*, 49 J. CLINICAL EPIDEMIOLOGY 697, 702 (1996).

165. Edward B. Royzman & Jonathan Baron, *The Preference for Indirect Harm*, 15 SOC. JUST. RES. 165, 167 (2002).

vehicle. Advertising campaigns often explicitly seek to associate products with particular feelings. Literature shows that affect cues exert a stronger influence on choice when consumers have diminished ability to judge alternatives rationally (conditions of "low elaboration").[166] Thus, when consumers are not particularly motivated to make a correct decision under weighted-adding analysis, or when consumers find it difficult to process all the information necessary to make such a decision, affect cues become more pronounced.[167]

The availability heuristic. It is widely known that people overrespond to risks that are well known because of news coverage or immediacy. Such risks are "available" in people's minds, and they can therefore bring the information into the decision process more readily.[168] The availability heuristic becomes relevant when people base judgments on the probability of certain events happening. The familiarity of decision makers with instances of an event occurring often affect judgments about that event's probability. In environmental regulation, for example, this encourages the "pollutant of the month" syndrome, where regulation is driven by recent events, news stories, and public relations campaigns.[169] "Availability entrepreneurs" exploit the heuristic by focusing public attention on events to ensure that the event will be more available and more salient in the decision-making process.[170] The availability heuristic can work the other way as well. People may underestimate the likelihood of certain events because those events do not come to their attention often. When public policy is driven by the availability heuristic, regulation is often characterized by a patchwork of laws that tend to under- or over-regulate the targeted problem.[171]

4. Implications for Privacy Shopping Online

The decision strategies and goals and behavior patterns summarized above have important implications for the information privacy market in online commerce. If consumers are using decision strategies rationally to pursue other goals besides maximum accuracy of the decision, then gains in accuracy can be offset by losses in the pursuit of those other goals. One loss results from an increase in cognitive effort to evaluate privacy policies. When consumers exert more effort to evaluate a particular

166. *See* Michel Tuan Pham, *Representativeness, Relevance, and the Use of Feelings in Decision Making*, 25 J. CONSUMER RES. 144, 144–46 (1998).

167. *See id.* at 158; Piotr Winkielman et al., *Subliminal Affective Priming Resists Attributional Interventions*, 11 COGNITION & EMOTION 433, 434–35 (1997). *See generally* ALICE H. EAGLY & SHELLY CHAIKEN, THE PSYCHOLOGY OF ATTITUDES (1993) (discussing social psychology research in the area of attitudes).

168. Timur Kuran & Cass R. Sunstein, *Availability Cascades and Risk Regulation*, 51 STAN. L. REV. 683, 686 (1999).

169. Jolls et al., *supra* note 107, at 1518.

170. *Id.* at 1519.

171. *Id.* at 1518–19.

alternative, they tend to have a more negative view of that alternative simply because it takes more effort to evaluate it. They are less inclined to prefer it to alternatives that require less effort, unless it ends up clearly superior. Thus, while it may be in a firm's interest to post a privacy policy on its Web site to give the impression that it cares about safeguarding user information, it may not be in the firm's interest to encourage or direct consumers to view privacy terms before entering into a transaction or even click an "I agree" button—even if the firm has a stronger privacy policy than its competitors. Requiring such a step could make the firm's Web site less attractive overall because it requires more cognitive effort to evaluate the choice. Unless the firm's Web site can demonstrate a substantially superior privacy practice, its efforts may be counterproductive.

The goal of minimizing emotional conflict is relevant as well. People want to minimize the discomfort that arises from facing emotion-laden choices or choices that make them uncomfortable. Comparing prices or warranties may not create much conflict because the attributes are roughly comparable and only monetary values are at stake. People may feel conflicted, however, when trying to compare attributes that are dissimilar, especially when the comparison asks people to put a price on something they intuitively believe should not be commodified or traded away. When this occurs, consumers may shift to decision strategies that focus attention elsewhere. They may struggle through the conflict only when the outcome is of fundamental importance—for example, when deciding whether to pay more for an automobile that has higher safety ratings. This is a difficult trade-off, but a person might work through the decision process because automobile safety is highly important.

With information privacy, there is a basic incomparability of competing values.[172] If consumers actively shop for privacy, they must make difficult and uncomfortable trade-offs. Consumers will seldom know what a Web site will do with their personal information and how it will affect them. One site may say that it does not keep or sell information of any kind, but a consumer will have difficulty comparing that claim with another site that seems better in other ways but does not make such a promise. Because of the basic incomparability of competing values, these are difficult trade-offs to evaluate emotionally and cognitively. The site may become less appealing simply because it is increasing emotional discomfort by bringing privacy issues into the decision process.

Moreover, if the relative weight given to the three competing goals is influenced by a person's ability to get feedback about those goals, any increase in the accuracy goal may be hard to discern. The more

172. *See generally* James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1 (2005) (discussing the incomparability of the competing norms of free information advocates and privacy advocates).

immediate and concrete the feedback about a particular goal, the more emphasis one is likely to give it in making choices. This is important in the market for privacy protection because the accuracy of any decision about revealing personal information usually will not be apparent until long after the transaction has ended, if ever. Only rarely will a consumer be able to trace the spam, identity theft, consumer profiling, advertising campaign, junk mailings, and other trespasses to a particular Web site's weak privacy policy. Feedback on the accuracy of the decision may never occur. In contrast, feedback on cognitive effort and emotional conflict are likely to be more immediate because Web users experience them at the same time they are making decisions about sharing information or choosing which sites to frequent. As a result, those two goals will weigh more heavily in the decision strategy chosen, and the user is therefore less likely to search for and evaluate privacy practices.

Time constraints can also be important in online behavior. When time for making a decision is scarce, people abandon more complete strategies and gravitate to strategies that are easier and accelerate their information processing, such as the lexicographic strategy in which a person chooses the first option satisfying the most important goal. On the one hand, Web users usually have as much time as they like to review Web site information. Unless a user's computer time is limited (as it might be in an Internet café), a user can revisit the site many times and move through links at leisure. Moreover, depending on the reason for visiting a Web site, there may be no outside pressure to make a decision in a hurry. On the other hand, people use the Internet because it is a fast and convenient way to obtain information, communicate with others, and purchase goods and services. Thus, while there may be plenty of time to learn about the privacy practices of each Web site visited, to do so would substantially impair the principle benefit of going online. Unless privacy is a particularly important goal for a consumer interacting with a Web site, the consumer's desire to move quickly on the Internet will likely frustrate the desire to process the privacy practices of competing sites. Regardless of time constraints, if there are limits on the number of attributes consumers can effectively investigate when making choices—perhaps as few as five—for privacy to be salient in online decision making, it must be important enough to work into that top tier.[173]

Framing effects can also contribute to the decreased saliency of a site's privacy practices. Because consumers tend to process information in the form in which it is displayed to them without transforming it, a Web site may give the impression that it has a strong privacy policy when in fact it does not, knowing that most consumers will take them at their word without delving into the details. Unless consumers believe that the costs of accepting the given format are high (that is, they have suspicions about a strong privacy claim, and they believe they will pay a high cost if

173. *See supra* notes 140–41 and accompanying text.

they do not verify the claim), they will not be motivated to obtain additional information.

Inferences can also lead to erroneous assumptions about privacy practices. Consumers may assume that the privacy policies of similar retailers are roughly alike, or that brand-name retailers must have strong privacy policies because they are generally reliable and credible in other aspects of their business. Web sites must work hard to overcome such inferences if they want to distinguish themselves as "strong" privacy providers. If they do make efforts to draw attention to their privacy practices, however, they may increase the cognitive effort of users and force emotion-laden comparisons, which can make the sites less appealing to consumers in the decision-making process.

The availability heuristic also may influence consumers not to shop for privacy online. People may underestimate the effects of information disclosure and its potential costs if the adverse consequences of weak privacy practices come to their attention only infrequently. While there is increasingly more publicity about security leaks and unauthorized access to consumer databases, such as the highly publicized disclosure at ChoicePoint,[174] consumers seldom hear about the actual harms resulting from weak privacy practices. Hearing about security leaks raises a societal concern about privacy, but because consumers seldom know what information about them is collected and sold, tracing injury to particular data brokers is extremely difficult. Even in the ChoicePoint incident, affected consumers likely will not know if the security breach resulted in harm to them. If they suffer from identity theft at some future date, the source of the problem likely will never be known. Moreover, few consumers will learn how ChoicePoint built its database and who supplies its information. Without knowing the sources, consumers cannot avoid sharing information with them in the future. Thus, while publicity can increase the societal concern about information privacy, it does not necessarily raise the saliency of privacy in any particular decision-making process.

III. ALTERNATIVES TO THE MARKET APPROACH

When presented with the issue in controlled situations, consumers show strong privacy preferences. Yet for understandable reasons, privacy is seldom a salient attribute in online decision making. We can use these findings to draw a number of conclusions.

Privacy preferences only appear strong in controlled surveys when the question is put directly to consumers, but survey evidence can be misleading. Preferences may in fact be rather weak—or at least not

174. *See ChoicePoint: More ID Theft Warnings*, CNN/MONEY, Feb. 17, 2005, http://money.cnn.com/2005/02/17/technology/personaltech/choicepoint (describing unauthorized access by potential identity thieves into ChoicePoint's consumer databases).

strong enough to warrant a legal response. Survey questions about privacy concerns can distort or manipulate answers. Surveys showing a high level of concern for online privacy often group together different problems (such as, credit card theft, identity fraud, spam, and security), without identifying the particular risk that troubles consumers most. Moreover, surveys seldom develop a full picture of the trade-offs between increased privacy protection and its costs. Without asking consumers to decide how much they are willing to give up in exchange for increased privacy, surveys can distort the level of concern that consumers actually have.[175] It is easy to express concern about information privacy when nothing is at stake. The FTC's market approach might be working more efficiently than privacy surveys would lead us to believe. Consumer behavior in the market shows that we do not value privacy highly at all.

Moreover, even if the market for information privacy is not working efficiently, it is possible that the collective harm to consumers is negligible, and, therefore, any surplus enjoyed by online businesses is too small to merit concern. One of the main difficulties with analyzing privacy issues is demonstrating the harm that results from an invasion of consumer privacy.[176] Industry-sponsored studies show that consumers do not mind being tracked online if it results in more customized Web surfing and if they have an opportunity to opt out of certain data sharing practices.[177] The purportedly high level of consumer angst about privacy seems to have had little effect on online shopping behavior.[178] The perceived injuries may be too small to affect behavior in any noticeable way.

If, however, consumers do value information privacy highly, and their behavior in the market is explainable on rational decision-making grounds, then the consumer injury is not de minimis and some type of response might be justified. Three responses are explored below. First, we could remain patient while waiting for a more mature privacy market to develop. Second, we could impose mandatory privacy rules by legislative or regulatory action that better align with consumer privacy

175. JIM HARPER & SOLVEIG SINGLETON, COMPETITIVE ENTER. INST., WITH A GRAIN OF SALT: WHAT CONSUMER PRIVACY SURVEYS DON'T TELL US 3 (2001), *available at* http://www.cei.org/PDFs/with_a_grain_of_salt.pdf.

176. Phelps, Nowak & Ferrell, *supra* note 40, at 27–28. When personal information is used for unwanted marketing (such as mail, spam, or phone solicitations), consumers bear costs that can be placed into two broad categories: contact costs (including nuisance, disposal, and wasted time) and reliance costs (incurred when the consumer follows up on the solicitation for further consideration). Ross D. Petty, *Marketing Without Consent: Consumer Choice and Costs, Privacy, and Public Policy*, 19 J. PUB. POL'Y & MARKETING 42, 43 (2000). Because the marketer does not internalize these costs, the allocation of marketing resources is inefficient and results in over-marketing. *Id.* Over-marketing results in advertising clutter, which drives marketers to create new ways to get consumers' attention. *Id.* It also creates incentives for deceptive marketing practices that disguise the marketing message, which increases the costs imposed on consumers. *Id.*

177. Milne, *supra* note 82, at 4.

178. Phelps, Nowak & Ferrell, *supra* note 40, at 27.

preferences. Third, we could move incrementally toward stronger privacy practices by stepping up enforcement actions to punish market behavior that deviates from generally held consumer expectations about fair information practices.

A. Wait for the Privacy Market to Mature

Problems with privacy saliency may be causing market inefficiencies at the moment, but that could change in time. Concerns about information privacy in the digital age are still relatively new, and in time consumers may bring privacy concerns into the decision-making calculus more frequently. The saliency of privacy practices could be raised by a combination of several forces. Four are explored below: advertising, personal experience, market signals, and technological solutions.

1. Raising Saliency Through Advertising and Marketing

Advertising and marketing efforts could raise the saliency of privacy practices online. Business consulting firms already advise their clients to publicize good privacy practices as a part of their overall marketing plan.[179] Credit reporting agencies now sell privacy protection plans,[180] which not only raise the saliency of privacy issues but generate new revenues from consumers who are willing to place a monetary value on protecting their personal information through the purchase of privacy insurance.

As a general matter, advertising can draw attention to product and service attributes when they otherwise would not be incorporated into the decision process.[181] If a Web site has a competitive advantage with a strong privacy policy, it has an incentive to promote that policy to attract more users. A site may have invested in technical infrastructure to secure data, or its business plan might not involve data collecting or sharing. Some sites may have no ability to collect and store data, leaving them a strong privacy provider by default.

Advertising privacy practices can help consumers in two of the three decision-making goals mentioned above. To the extent that the advertising gives accurate information about important privacy practices, the decision-making calculus is more complete. Advertising can also

---

179. *See* Andrew E. Fano et. al., *The Economic Value of Trust*, OUTLOOK J., October 2003, at 34, 40, *available at* http://www.accenture.com/NR/rdonlyres/22FD46BC-5091-46B9-8033-DA8A6E0FB557/0/technology.pdf.

180. *See* Equifax, Equifax Credit Watch™ Overview, https://www.econsumer.equifax.com/consumer/sitepage.ehtml?forward=cs_esn (last visited Nov. 30, 2005).

181. *See generally* ISSUES IN ADVERTISING: THE ECONOMICS OF PERSUASION (David G. Tuerck ed., 1978) (discussing the effects of advertising on consumer purchasing behavior); Phillip Nelson, *Advertising as Information*, 82 J. POL. ECON. 729 (1974) (discussing how advertising provides information to the consumer); Phillip Nelson, *Information and Consumer Behavior*, 78 J. POL. ECON. 311 (1970) (discussing the effect of limited consumer information on the consumer goods market).

reduce the cognitive effort required to put the privacy attribute into the calculus. It can make privacy practices more noticeable and bring them to the involuntary attention of the user, thereby reducing the effort required to process the message.

There are reasons to be skeptical, however, about the potential for advertising to influence privacy shopping behavior. First, marketing efforts have costs, so firms must balance the benefits of promoting their competitive advantage on privacy against the costs of persuading users that they should respond to that message. They must ask how many users or how much information will be gained by the added marketing and what will be the cost of acquisition.

Second, opportunity costs must be weighed. Resources might be better spent promoting other attributes of the product or service where the gain is likely to be greater. Because consumers have limited abilities to process information, increasing the saliency of the privacy attribute may reduce the saliency of others in which the site also has a competitive advantage. Consumers will bring only a limited amount of attributes into the decision-making calculus.[182] The trade-off might not be worth the effort.

Third, advertising does little to further the third decision-making goal—minimization of emotional strain or conflict. In fact, it could impede that goal by highlighting a trade-off that consumers have difficulty making. Depending on how the message is conveyed, advertising privacy practices may cause some consumers to increase their concern about privacy. If a site is making a strong effort to promote its privacy practices over those of a competitor, consumers may feel uncomfortable with the proposed trade. By raising the saliency of privacy advantages, a business is asking its users to assess the value of their personal information. With some attributes, such as a product's price or a free phone with a mobile phone service, the value comparison is clear and the message is direct and unambiguous. When considering the value of increased privacy, however, consumers must ask themselves, "What is it worth?" This raises difficult valuation problems. Asking consumers to put privacy into the decision-making calculus may cause them to increase cognitive effort and emotional concern, which makes the decision process more taxing and may make the business appear less desirable than other alternatives.[183]

Fourth, for advertising to raise saliency, it cannot be misleading. Due to framing effects and other heuristics discussed above, advertising good privacy practices may not give consumers a more accurate understanding of how a firm actually uses and safeguards the personal information it collects. Without more aggressive law enforcement efforts to police misleading claims, as discussed above, the temptation to

182. *See supra* text accompanying notes 140–41.
183. *See* discussion *supra* Part II.D.2.

oversell one's concern for customer privacy is likely to continue for some time.[184]

2. Raising Saliency Through Personal Experience

Web sites that use inefficient privacy terms may reap a consumer surplus for a while, but through repeat transactions visitors may become dissatisfied with their experience and move to sites that have stronger privacy practices. If the long-term costs of having inefficient privacy terms exceed the short-term gains, then it is in a Web site's interest to move toward practices that better align with consumer preferences. This will occur, however, only if two conditions are present. First, terms that are not salient to Internet users initially become salient through their personal experiences and then to others whom they inform by word of mouth, through Web logs, via news reports, or otherwise. Second, Web sites desire the repeat business of users who care about privacy and will adjust their practices to attract them. There is reason to doubt whether these conditions exist now or will emerge in the future.

With respect to the first condition, if a Web site has weaker privacy policies than a user would prefer, it is not likely that any harm caused by the weak policy will come to the user's attention. Tracing privacy injuries to their source is extremely difficult in most cases.[185] Most harms caused by information disclosure go unnoticed, in which case consumers learn nothing from the experience.[186] Harms caused by consumer profiling are one example. People understand that profiling is common, but they seldom know precisely when it is occurring and whether they are benefiting from the practice or not.[187]

The most noticeable harms caused by the release of personal information—excessive spam, junk mail, or identity theft—may cause a consumer to raise concern about privacy generally, and if this occurs to a significant number of consumers, it might cause Web sites to provide stronger privacy protections. It is unlikely, however, that a consumer's privacy injuries can be traced back to any particular information disclosure. With data about us in so many databases, tracing a problem to a particular source is nearly impossible.[188] Without the ability to trace,

184. *See, e.g.*, *supra* note 19 and accompanying text.

185. *See, e.g.*, Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 65 (2003) (noting that nearly every transaction a consumer makes is tracked and that there are "[m]ore than 1000 data-mining companies").

186. Janet Dean Gertz, Comment, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 947–48 (2002).

187. *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1284–85 (2000); McClurg, *supra* note 185, at 65; Gertz, *supra* note 186, at 947–48.

188. For some attributes of a product or service, tracing an injury to its cause is straightforward. Consider a weak or short product warranty: consumers will know who the seller is and will learn in due course that the seller does not stand behind its products. When it is time for another purchasing decision, these consumers may decide to go somewhere else. With harms caused by disclosure of

there is little risk of accountability when a firm collects and shares data in a way that does not coincide with consumer preferences. With no accountability, there is little likelihood that a site will either lose users as a result of personal experience or change its privacy practices to avoid customer defections caused by their experience.

The second assumption—that Web sites want to attract privacy-concerned individuals—may be valid for some firms. But if privacy shoppers tend to be more tech-savvy and privacy-aware,[189] Web sites that expect to extract value from the personal information of their users might not wish to attract more of them. If a site is interested in collecting and using reliable data, it might not want to attract privacy-conscious individuals. Studies show that privacy-savvy shoppers are more inclined to use programs that preserve anonymity, keep dummy e-mail accounts, or provide false information to the database.[190] To the extent that this is true, there is an additional cost to attracting and keeping privacy-conscious users. The site may get more of them, but the information obtained from such users may be less valuable.

3. Raising Saliency Through Market Signals

Intermediaries can raise the saliency of privacy in a way that increases the accuracy of consumer decision making without increasing cognitive effort and emotional discomfort. Market-generated signals, such as the privacy seals of TRUSTe or BBBOnline, may attract the attention of Web users if the seals are conspicuously displayed on Web sites. Such signals can reduce cognitive effort and take advantage of framing effects and the concreteness principle—consumers will accept the information conveyed by the seal as displayed, without delving further into the details.[191] Standardizing information disclosure can convey information economically. For example, before Congress enacted the Truth-in-Lending Act in the late 1960s, lenders disclosed interest rates in a variety of different ways, requiring consumers to exert substantial effort (and perform complex computations) to make

---

personal information, consumers generally may be aware that information leaks are causing them problems, but they have no reason to think that information was released by any source in particular. Literature on regret supports this conclusion. Research suggests that if a consumer actively agrees (i.e., consciously chooses) to interact with a site that presents threats to privacy and the consumer subsequently learns of a breach, the consumer will have greater regret than if his or her interaction with the site was inadvertent, unknowing, or passive. As the regret derived from the experience becomes more intense, it is more likely to affect future decision making. The key to learning the lesson well, however, is becoming aware of the breach and linking it to a decision consciously made at an earlier time. Without such a link, regret is less likely to result and future behavior is less likely to change. See Terry Connolly and Marcel Zeelenberg, *Regret in Decision Making*, 11 CURRENT DIRECTIONS IN PSYCHOL. SCI. 212 (2002); Thomas Gilovich and Victoria Husted Medvec, *The Experience of Regret: What, When, and Why*, 102 PSYCHOL. REV. 379, 380–81 (1995).

189. *See supra* text accompanying note 81.

190. *See supra* text accompanying note 83.

191. *See* Viscusi, *Individual Rationality*, *supra* note 149, at 630–36; Viscusi, *An Investigation, supra* note 149, at 477–78.

comparisons.[192] With mandatory, conspicuous disclosure of APR according to the actuarial method, consumers could compare rates by looking at simple numbers in bold font, presented in a uniform manner on all credit agreements.[193] This reduced the cognitive effort necessary to acquire as well as process the information. Standard, conspicuous disclosure of privacy information might be conveyed in a similar way.

Thus far, however, privacy seals have done little to further the accuracy goal, and they can be more misleading than helpful. Seals signify that the site has a privacy policy consistent with the seal sponsor's list of fair information practices, but those standards are neither uniform nor particularly strong. The most popular seal programs do little more than signify that the site has a privacy policy consistent with the seal standards and, to the extent the sponsor can audit subscribers, that the site generally follows its policy.[194] The seal says little about the content of the policy itself. A site with a privacy seal may collect copious amounts of personal information and sell it to third parties. A site without a privacy seal may collect and disclose nothing. Consumers who believe that a Web seal confirms a higher standard of privacy protection can be easily misled. Indeed, if a seal creates a misleading impression, it may induce more disclosure of information and patronage by consumers.[195] Thus, privacy seals may reduce cognitive effort, but they can lead to less accurate decision making if they do not convey information consistent with consumer assumptions about a particular privacy seal's meaning.

For seals to serve as accurate and meaningful signals of privacy practices, there must be incentives for a seal sponsor to set strong standards. To date, incentives have moved seal programs in the other direction.[196] To maximize the number of paying subscribers, it is better to have standards that look impressive to the casual observer but do not impede the ability of subscribers to collect and share personal information as they wish. What is needed is a market signal for the seals

192. Memorandum from OEO Legal Services Training Program (Apr. 1972), *reprinted in* JOHN A. SPANOGLE ET AL., CONSUMER LAW 108, 108–09 (2d ed. 1991).

193. John A. Marold, *Third Circuit's Decision in* Roberts v. Fleet Bank*: Thinking Outside of the "Schumer Box" or "Consumerism Gone Berserk"?*, 8 N.C. BANKING INST. 399, 403 (2004).

194. Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 767 ("[T]he existence of competing privacy seal programs permits forum shopping by Web sites that hope for weaker enforcement from one seal service rather than the other."); Tal Z. Zarsky, *Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society*, 56 ME. L. REV. 13, 23 (2004); Jeremy Quittner, *Should You Pay for a Privacy Seal of Approval?*, BUSINESSWEEK ONLINE, Apr. 27, 1999, http://www.businessweek.com/smallbiz/news/date/9904/f990427.htm. For an in-depth analysis of the effectiveness of third-party privacy seals, see Ann Cavoukian & Malcolm Crompton, Web Seals: A Review of Online Privacy Programs, Presentation at the 22nd International Conference on Privacy and Personal Data Protection (September 2000), *available at* http://www.privacy.gov.au/publications/seals.html.

195. Anthony D. Miyazaki & Sandeep Krishnamurthy, *Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perception*, 36 J. CONSUMER AFF. 28, 30, 40–41 (2002).

196. Milne, *supra* note 82, at 3; Chet Dembeck, *Report Labels Internet Privacy Policies "A Joke,"* E-COMMERCE TIMES, Sept. 16, 1999, http://www.ecommercetimes.com/story/1243.html.

themselves, or standards imposed by law that would give greater meaning to privacy seals. A regulation might provide, for example, that a "five star" privacy site means the site complies with certain privacy standards, with fewer stars signaling less privacy protection. Absent such a change, seals will continue to give mixed signals at best.

4. Technological Solutions

Claims about harms caused by information collection and sharing are often met with arguments that the problem is temporary and emerging technologies will address legitimate concerns. More widespread use of cryptography can protect some types of privacy invasion, particularly in the telecommunications and Internet data transfer industries.[197] Knowledgeable consumers can install and employ a wide range of products that defend against surreptitious data mining. Products such as Anonymizer[198] allow users to retain anonymity while surfing the Internet.[199] More important for our purposes, computer software can be programmed to act like an "electronic lawyer," negotiating privacy policies with Internet sites.[200] P3P technology, which provides a standard language for Web sites to encode privacy policies, allows Web browsers to display privacy warnings to users, block cookies, and restrict access to Web sites that do not conform to the pre-set privacy preferences on the user's computer.[201] User-friendly technologies such as these could help enhance the saliency of privacy policies online.

While technology holds promise in this area, there are reasons to be skeptical. Privacy enhancing technologies have yet to be widely used. Economic incentives more often produce technologies that enhance data collection and sharing rather than restrict it.[202] Because personal

---

197. BRUCE SCHNEIER & DAVID BANISAR, THE ELECTRONIC PRIVACY PAPERS 4 (1997).

198. For a more detailed product description, see Anonymizer, Anonymous Surfing, http://www.anonymizer.com (follow "Anonymous Surfing" hyperlink) (last visited Dec. 1, 2005).

199. *See* Eric Shih, *Putting Internet Privacy Laws Aside, What Technology Might Guard Your Privacy?*, 5 ELEC. BANKING L. & COM. REP. 12, 12–13 (2001).

200. A company called Lumeria took this idea one step further by offering to block transmission of subscribers' data to Web sites they visit, and then selling the subscribers' data in anonymous form to marketers and paying royalties to its subscribers. *The Coming Backlash in Privacy*, ECONOMIST, Dec. 9, 2000, at 4, 5.

201. Lorrie Cranor, et al., The Platform for Privacy Preferences 1.0 (P3P1.0) Specification: W3C Recommendation (Apr. 16, 2002), http://www.w3.org/TR/P3P. One such product is Privacy Bird, which was developed by AT&T. It purports to perform

> searches for privacy policies at every website you visit. You can tell the software about your privacy concerns, and it will tell you whether each site's policies match your personal privacy preferences. The software displays a green bird icon at Web sites that match, and a red bird icon at sites that do not.

Privacy Bird, http://www.privacybird.com (last visited Dec. 1, 2005). *See generally* Kimberly Rose Goldberg, *Platform for Privacy Preferences ("P3P"): Finding Consumer Assent to Electronic Privacy Policies*, 14 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 255 (2003) (discussing efforts to protect the privacy of personal data in online transactions).

202. *See* John MacDonnell, *Exporting Trust: Does E-Commerce Need a Canadian Privacy Seal of Approval?*, 39 ALTA L. REV. 346, 348–49 (2001); John Hanchette, *New Microsoft Software Raises Privacy Protection Concerns*, INDIANAPOLIS STAR, Aug. 26, 2001, at D1 (describing Microsoft's plans

information has become so valuable, technologies have developed that increase data collection and decrease our ability to monitor the data-collection process. This makes privacy protection more difficult for computer users who might be interested in curbing surreptitious data-collection practices.

If P3P or similar technologies are to gain widespread popularity, a large-scale educational effort would be needed and software would need to be developed that is difficult for data seekers to evade (without paying a price in the market) and relatively easy for consumers to use.[203] With respect to the first of these predicates, P3P in its current form gives Web sites the option whether to incorporate the protocol on their Web sites. If a Web site has relatively weak privacy practices, it has little incentive to incorporate the protocol. If few sites support P3P, consumers will have little incentive to use the technology, and its benefits will be marginal. In addition, although P3P provides a technical mechanism for assisting users who wish to be informed about privacy policies before they release personal information, it does not provide a mechanism for making sure sites act according to their stated policies. For this and other reasons, the European Union has not adopted P3P as a technical mechanism for enforcing its privacy laws.[204]

---

to combine personal identification information with a powerful information distribution network). *See generally Oversight Hearing on Privacy and Electronic Commerce Before the Subcomm. on Courts and Intell. Prop. of the H. Comm. on the Judiciary*, 106th Cong. (2000) (statement of Joel R. Reidenberg, Professor of Law and Director of the Graduate Program, Fordham University School of Law), *available at* http://judiciary.house.gov/legacy/reid0518.htm. A version of the Microsoft Internet Explorer came equipped with default settings that enabled hidden surveillance of users, and a version of Netscape Communicator reported back to Netscape every time a user read e-mail. Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 723 (2001).

203. *See Exposure in Cyberspace*, WALL ST. J., Mar. 21, 2001, at B1 (survey showing that almost 30% of computer users did not know about cookies and almost 40% had no idea how to deactivate them); *see also* SUSANNAH FOX, PEW INTERNET & AM. LIFE PROJECT, TRUST AND PRIVACY ONLINE: WHY AMERICANS WANT TO REWRITE THE RULES 5, 6 (2000), http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf (discussing various methods currently being employed by data seekers that challenge Internet users' ability to protect personal information). *Time* ran a feature story on information privacy in July 2001 that recommended ten steps to protect privacy. The list includes changing browser preferences to delete a user's e-mail address and replacing it with a "false name and dummy e-mail account"; opting out of information sharing policies when given the choice; resetting browsers to reject cookies or install software such as "Cookie Crusher"; checking to make sure a Web site uses encrypted transfer software before giving sensitive information online; hiding your identity with an anonymizer program; and clearing your memory cache each time you surf the Internet. *See* Adam Cohen et al., *Internet Insecurity*, TIME, July 2, 2001, at 46, 50.

204. *See* Eur. Comm'n, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)*, XV D/S032/98 WP 11 (June 16, 1998), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1998/wp11_en.pdf.

With respect to the second predicate, if a large proportion of Web sites adopted P3P, practical problems may weaken its usefulness. Even the most user-friendly P3P programs require users to set their initial privacy preferences if they want to vary the default settings. Studies show that consumers generally find changing default settings to be burdensome and confusing.[205] Consumer experience setting cookie preferences is a recent example.[206] Consumers who configure their browsers to notify them when they detect cookies often find that Web surfing is nearly impossible. A similar problem can inhibit widespread use of P3P. Concerned users will configure their computers to reflect high privacy preferences. When they attempt to access the majority of commercial Web sites, pop-up windows or other warnings will indicate that their privacy preferences are stronger than the privacy practices of the sites they wish to visit. Unless the user is willing to reject the site without further inquiry, the user will need to investigate further to see how serious the conflict is, and then compare the potential risks of going forward to the expected benefits gained by interacting with the Web site. Many consumers will find this calculus cognitively difficult and may respond by reverting to low P3P privacy protection configurations, as they do with cookie preferences now.

B. Mandatory Privacy Terms for the Internet

When consumer markets do not work efficiently, laws that punish practices deemed by government authorities to be unfair can constrain providers of goods and services. Indeed, laws are often enacted to punish unfair practices even when markets are efficient. Lenders may loan money at exorbitant interest rates to well-informed but desperate borrowers, and price-gouging suppliers may take advantage of scarce supplies after a natural disaster. Laws are imposed to curtail such behavior because lawmakers believe fairness norms can be violated even when the market is open and reasonably transparent. Behavioral analysis suggests that community judgments about fairness may explain why bans on voluntary transactions are enacted; such legislation is often difficult to explain by economic efficiency theories.[207] If data collectors

205. *See* ELEC. PRIVACY INFO. CTR., PRETTY POOR PRIVACY: AN ASSESSMENT OF P3P AND INTERNET PRIVACY (2000), http://www.epic.org/reports/prettypoorprivacy.html.

206. *See id.*

207. People care about being treated fairly and will reciprocate with fair treatment if they think others are behaving fairly towards them. Jolls et al., *supra* note 107, at 1479. Conversely, when the conduct of one actor has deviated substantially from a norm of fairness, the other actor may incur costs to "punish" the behavior even when no personal gain results from the punishment. *Id.* at 1494. Boycotts are one example. The "ultimatum game" is another: people refuse to trade for a commodity at a perceived unfair price even when they know that by not trading they will get nothing at all. *Id.* at 1489–90. The implications for privacy policy are evident. If a consumer believes that a Web site guards personal information consistent with a perceived norm of fairness, the consumer may reward the site with more information. If the perception is otherwise and the consumer suspects unfair

engage in information practices beyond the fairness norms governing online activity, mandatory privacy laws may be warranted.

The behavioral research discussed in this Article suggests that online privacy practices may exceed generally held fairness norms, supporting a call for mandatory privacy terms. Nevertheless, there are several practical and theoretic impediments to imposing privacy standards on Web site operators. A few are briefly described below.

1. First Amendment Concerns

Because Internet privacy laws would interfere with the exchange and free flow of information, First Amendment concerns arise. Broad-based privacy rules can run afoul of the *Central Hudson*[208] guidelines for regulating commercial speech.[209] The test looks at whether the government has a substantial interest in restricting the flow of information and whether there is a "reasonable fit" between the government's goal and the means chosen to achieve it.[210] While there is a strong public interest in protecting personal information online, Internet privacy regulation would need to be tailored narrowly enough to avoid a challenge that it prohibits more data collection and distribution than is reasonably necessary to address legitimate privacy concerns. Broad-based legislation that does not distinguish between different types of Web sites and different Web uses may not satisfy the reasonable fit standard.[211]

2. Political Drawbacks

Public choice theory and recent experience with privacy laws in other economic sectors suggest significant obstacles as well. Legislating privacy through the political process may result in a framework that entrenches the interests of the major Internet companies that can muster influence in Washington. Resulting laws could create barriers to entry that favor older, established companies that have invested heavily in the

---

information practices, less information (or false information) will be revealed. *See also* Olivero & Lunt, *supra* note 72; Culnan & Armstrong, *supra* note 99, at 112–13.

208. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557 (1980).

209. Caudill & Murphy, *supra* note 35, at 11.

210. *Cent. Hudson*, 447 U.S. at 564; *see also* Fla. Bar v. Went For It, Inc., 515 U.S. 618, 624 (1995).

211. Courts have recognized First Amendment limitations on regulating Internet privacy. See U.S. W., Inc. v. FCC, 182 F.3d 1224, 1239 (10th Cir. 1999); United Reporting Publ'g Corp. v. Cal. Highway Patrol, 146 F.3d 1133, 1140 (9th Cir. 1998), *rev'd sub nom.* L.A. Police Dep't v. United Reporting Publ'g Corp., 528 U.S. 32, 40 (1999). *See generally* Larry E. Ribstein & Bruce H. Kobayashi, *State Regulation of Electronic Commerce*, 51 EMORY L.J. 1 (2002) (discussing whether the regulation of electronic commerce should be at the state or federal level); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1080–87 (2000) (discussing the problems confronting arguments that Internet privacy laws are constitutional because they restrain only commercial speech).

current privacy regime.[212] With innovation stifled by mandatory laws, inefficiencies in the system could crystallize.

The Gramm-Leach-Bliley Act (GLBA)[213] is a good example of well-intentioned legislation gone awry. The primary purpose of the GLBA was to allow affiliations among companies in the financial services industry.[214] Some members of Congress recognized that these affiliations could create privacy risks, and privacy groups lobbied to include some privacy protection for individuals.[215] In the end, however, the GLBA's privacy protections were weak and sharing consumer information among affiliates and non-affiliated entities is commonplace.[216] The act does not even require covered entities to identify with any specificity what information is shared and the identity of those who may obtain it by sale, transfer, or otherwise.[217]

3. Institutional Inadequacies

Efficiency determinations are difficult to make legislatively. Even if current privacy practices are inefficient, new rules would interfere with the flow of some consumer information, which imposes costs. Some sites might go out of business as a result. Some consumers welcome collection and sale of information in exchange for benefits that they would no longer receive. The government would need to strike the appropriate balance in a way that is an improvement over the current market-driven allocation of rights and responsibilities.[218] Although the deliberative process allows for many factors to be considered, ex ante mandatory terms are difficult to tailor precisely to specific contextual situations. Legislative action is most appropriate when the specific contextual relationships between businesses and consumers are not particularly important—simple rules that apply to a large number of situations in which context does not matter much or rules that apply only to a narrow sphere of commercial activity.[219] Privacy practices and online interactions between consumers and firms are varied and complex. Recent

212. *See* James B. Speta, *FCC Authority to Regulate the Internet: Creating It and Limiting It*, 35 LOY. U. CHI. L.J. 15, 30 (2003).

213. 15 U.S.C. §§ 6801–6809 (2000).

214. *See* Jolina C. Cuaresma, *The Gramm-Leach-Bliley Act,* 17 J. BERKELEY TECH. L.J. 497, 515–16 (2002); Chris Jay Hoofnagle, Guest Commentary, *Notice Is Not Enough!*, 5 CONS. FIN. SERV. L. REP., Feb. 13, 2002, at 19, 19 ("[A] group of six-year-olds could do a better job in crafting Gramm-Leach-Bliley Act privacy notices than the $400 per hour lawyers hired by the banking industry." (citing Massachusetts Representative Edward Markey)); Julia C. Schiller, Comment, *Informational Privacy v. The Commercial Speech Doctrine: Can the Gramm-Leach-Bliley Act Provide Adequate Privacy Protection?*, 11 COMMLAW. CONSPECTUS 349, 355 (2003).

215. Schiller, *supra* note 214, at 355; *see also* Hoofnagle, *supra* note 214, at 19.

216. Cuaresma, *supra* note 214, at 510–17; Schiller, *supra* note 214, at 358–63.

217. Cuaresma, *supra* note 214, at 510–11; Hoofnagle, *supra* note 214, at 19; Schiller, *supra* note 214, at 358–59.

218. *See* Cuaresma, *supra* note 214, at 515–17.

219. *See* Korobkin, *supra* note 34, at 1293–94 (2003) (arguing against legislative prohibitions of unfair contract terms).

experience in the financial and health sectors suggests that striking the right balance is not easy even when a specific economic area is targeted.[220] Mandatory terms covering the vast array of market interactions online could make consumers and businesses worse off.

C. Case-by-Case Evolution of Privacy Norms

Imposing standard privacy terms for all Web sites, regardless of the amount and types of information they collect and the purposes for which the information is used, may not result in net consumer benefit, yet market approaches have significant inefficiencies as well. A third approach is case-by-case enforcement of unfair or deceptive privacy practices, which may lead to more efficient privacy terms over time. The difficulty is deciding which privacy practices are so unfair or deceptive that they should be prohibited. The behavioral science research discussed in this paper can be helpful to enforcement agencies as they decide which information practices cross the line. The impact of this research on the FTC's unfairness and deceptive practices authority is discussed below.

1. Unfair Data-Collection Practices

Setting an appropriate standard for identifying "unfair" transactions has proved problematic in the United States. In the 1970s, the FTC began to use its unfairness authority aggressively to redress practices that it deemed contrary to general principles of morality and public policy. The result was a series of administrative adjudications and rulemakings that relied on general notions of morality and the inherent unfairness of one-sided business practices but lacked empirical support and were

220. After the passage of the GLBA, firms attempting to comply with this financial privacy legislation drafted privacy policies that require a reading skill (at least two years of college) considerably higher than the population's typical level. *See* Annie I. Antón et al., *The Lack of Clarity in Financial Privacy Policies and the Need for Standardization*, N.C. ST. U. COMPUTER SCI. TECHNICAL REP., NO. TR-2003-14, Aug. 1, 2003, at 1–2, 10, http://www.theprivacyplace.org/papers/glb_secPriv_tr.pdf. In the health field, personal information may be more susceptible to privacy breaches now than prior to enactment of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C. §§ 1320d to d-8 (2000). Before HIPAA, privacy policies were fairly short, simple, and more uniform. Annie I. Antón et al., *An Analysis of Web Site Privacy Policy Evolution in the Presence of HIPAA*, N.C. ST. U. COMPUTER SCI. TECHNICAL REP., No. TR-2004-21, Jul. 24, 2004, at 7, http://www.theprivacyplace.org/papers/hipaa_7_24_submit.pdf. HIPAA prompted the drafting of firm-specific privacy policies by legions of lawyers, which tend to be lengthier (approximately twice as long) and more difficult to understand (an increase by almost a grade level in required reading skill). *Id.* at 3–7. Web sites of most health organizations now require at least two links—a privacy policy link and a legal disclaimer link—before a privacy policy can be read in its entirety. *Id.* at 6. Many have additional links with more privacy-related information. *Id.* at 6–7. Even when a consumer does navigate through the site, the meaning of the policy may be difficult to discern. For example, because HIPAA allows organizations to determine what a "reasonable effort" to protect data means, consumers have no way of knowing when data is being safeguarded. One online pharmacy stated that it "may disclose any content, records, or electronic communications of any kind . . . if such disclosure is necessary or appropriate to operate the site." *Id.* at 5 (quoting Drugstore.com's Terms of Use).

based largely on individual commissioners' personal values.[221] In the view of many in the business community, and more importantly in Congress, the FTC was asserting unbridled discretion to punish commercial practices that it deemed unwarranted when reasonable minds might conclude otherwise.[222] Under pressure from Congress, the FTC began to reevaluate its unfairness authority, beginning with a 1980 letter to Congress explaining a new unfairness approach[223] and continuing with more restrained application in several regulatory proceedings during the following decade.[224] The FTC replaced its old approach with a less subjective, more empirically verifiable cost-benefit test for unfairness that Congress codified in a 1994 amendment to the FTC Act.[225] The principal focus under the current standard is the maintenance of consumer choice and sovereignty, an economic approach that seeks to identify conduct harmful to consumers in its net effects.[226]

The standard proved difficult to satisfy initially, however, and the pendulum swung far in the opposite direction. In the 1990s, the FTC used its unfairness authority sparingly and seldom when the conduct in question could be challenged under its deception theory.[227] The threshold inquiry for unfairness is whether the conduct in question has

---

221. The Supreme Court acquiesced in the FTC's approach. *See* FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 244 (1972) (reversing the FTC but observing that the FTC, "like a court of equity, considers public values beyond simply those enshrined in the letter or encompassed in the spirit of the antitrust laws."). *See generally* Richard Craswell, *The Identification of Unfair Acts and Practices by the Federal Trade Commission*, 1981 WIS. L. REV. 107; David A. Rice, *Consumer Unfairness at the FTC: Misadventures in Law and Economics*, 52 GEO. WASH. L. REV. 1 (1983).

222. *See Sperry & Hutchinson Co.*, 405 U.S. at 244.

223. *See generally* Letter from the FTC to Hon. Wendell H. Ford & Hon. John C. Danforth, S. Comm. on Commerce, Sci., & Transp. (Dec. 17, 1980), *reprinted in In re* Int'l Harvester Co., 104 F.T.C. 949 app. at 1070–76 (1984).

224. *Compare In re* Orkin Exterminating Co., 108 F.T.C. 263 (1986), *and In re* Int'l Harvester Co., 104 F.T.C. 949, 1070–76, *with* Labeling and Advertising of Home Insulation, 44 Fed. Reg. 50,218, 50,218 (Aug. 27, 1979) (representing the old approach).

225. 15 U.S.C. § 45(n) (2000). The amendment provides:

> The Commission shall have no authority under this section or section 18 [15 USCS § 57a] 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.

Id.

226. *Int'l Harvester*, 104 F.T.C. at 1061 n.47. For example, in adopting the Credit Practices Rule, the FTC considered and rejected a rule that would prohibit consumer credit contracts from containing a provision that required debtors to pay the creditor's attorneys' fees in debt collection actions. Credit Practices Rule, 49 Fed. Reg. 7740, 7784 (Mar. 1, 1984). The agency reasoned that creditors already have an incentive to minimize attorneys' fees because they usually are not reimbursed fully by defaulting debtors and must absorb the losses. *Id.* at 7785. Any benefit that an attorneys' fees ban would provide to debtors would be offset by losses to creditors for no net economic gain. *Id.* Furthermore, a ban might increase total legal costs by emboldening debtors to raise additional defenses and drag out litigation in hopes of a favorable settlement. *Id.* The cost of credit could increase as a result. *Id.*

227. J. Howard Beales III, *The Federal Trade Commission's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, 22 J. PUB. POL'Y & MARKETING 192, 192 (2003).

caused a "substantial consumer injury."[228] The injury can be economic harm or a threat to public health or safety, but the test is supposed to be objective and verifiable.[229] It can consist of small harm to a large number of consumers or significant harm to only a few.[230] The FTC has stated, however, that mere emotional discomfort or psychological distress ordinarily is insufficient to show substantial injury.[231]

The second inquiry is whether countervailing benefits to consumers or to competition resulting from the conduct in question outweighs the harm to consumers.[232] High prices, for example, are not necessarily unfair because they provide important market signals to consumers and other market participants that can help reallocate resources in ways that ultimately benefit consumers as a class.[233] In this balancing test, the costs of imposing a remedy also must be considered, as must any benefits that consumers enjoy as a result of the challenged practice, such as added consumer convenience.[234] Credit card fraud, for example, could be reduced if merchants were required to check photo or biometric identification before each use, but the impact of such a rule on consumer convenience, particularly in mail order, telephone, and Internet sales, likely would outweigh the benefits.[235]

The third and final inquiry focuses on consumer avoidance.[236] The FTC will declare a practice unfair only if the injury is not one that consumers can reasonably avoid.[237] The FTC views its role as promoting consumer choice, not second-guessing those choices.[238] It will not change market outcomes when the injury can be avoided by consumers taking reasonable actions themselves.[239]

Each of the three inquiries can be problematic in an FTC challenge to Internet privacy practices. There is some precedent, however, suggesting that the problems are not insurmountable.

a. Substantial Consumer Injury

Does the collection and sale of personal information online without consumer consent constitute a substantial injury? According to the FTC's 1980 policy statement, substantial injury requires more than mere

228. *Id.* at 195.
229. *Id.*
230. *Id.*
231. *Int'l Harvester*, 104 F.T.C. at 1073 ("Emotional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair.").
232. Beales III, *supra* note 227, at 195.
233. *Id.*
234. *Id.*
235. *Id.* at 198.
236. *Id*. at 195.
237. *Id*.
238. *Id*. at 196.
239. *Id.*

trivial or speculative harm.[240] In most cases, the injury must be economic or monetary or an increased health or safety risk. Emotional impact generally is regarded as insufficient.[241] The collection and sale of information online increases the risk that the information will be used in unauthorized ways, identity theft being the most economically injurious. The difficulty, however, comes in establishing that the risk is more real than speculative in the context of a specific Web site's practices. Most privacy or security breaches, even when detected, do not result in immediate economic harm to anyone. There may be potential harm from future use of the information, but until the use occurs and is traced to the specific privacy breach, any harm is largely psychological, emotional, and speculative.

In prior actions, however, the FTC has indicated that unfair privacy invasions can result in injury that is more than trivial or speculative even without an immediate economic injury. In *Touch Tone*,[242] a majority of FTC commissioners believed that a broker who obtained consumer financial information from banks created a likelihood of substantial injury, even though there was no evidence that the information was used to harm anyone.[243] The possibility of harm, including the possibility of identity theft, was deemed sufficient to sustain an enforcement action.[244] The case is not the strongest precedent for reviewing online data practices because the broker deceived the bank to obtain the information,[245] but the FTC said the conduct could be challenged under either its deception or unfairness authority, indicating that the deceptive nature of the conduct was not its only vice.[246]

The FTC also has recognized that relatively minor annoyances can constitute substantial injury when aggregated among a large number of consumers. In *Pereira*,[247] the agency challenged "pagejacking" and "mousetrapping" practices that lured Web surfers to pornographic sites,

240. S. REP. NO. 103-130, at 13 (1994), *reprinted in* 1994 U.S.C.C.A.N. 1776, 1788.

241. *Id.*

242. FTC v. Rapp (*Touch Tone*), No. 99-WM-783, 2000 U.S. Dist. LEXIS 20627 (D. Colo. June 27, 2000), *available at* http://www.ftc.gov/os/2000/06/touchtoneorder.htm. The defendants did business as Touch Tone Information, Inc., and FTC statements refer to the case in that manner. *Id.* at *1; *see* FTC, Dissenting Statement of Commissioner Orson Swindle In the Matter of *Touch Tone Information*, File No. 982-3619 [hereinafter Swindle Dissent], *available at* http://www.ftc.gov/os/2000/06/touchtoneswindle.htm (last visited Dec. 1, 2005); *see also* Complaint for Injunction and Other Equitable Relief, FTC v. Rapp, No. 99-WM-783, 1999 FTC LEXIS 112, at *2–3 (Fed. Trade Comm'n April 22, 1999) [hereinafter Touch Tone Complaint].

243. *See* Swindle Dissent, *supra* note 242; *see also* Touch Tone Complaint, *supra* note 242, at *3–4.

244. Swindle Dissent, *supra* note 242 at n.4.; *see also* Touch Tone Complaint, *supra* note 242, at *8 (statement of Chairman Pitofsky and Comm'rs Anthony and Thompson).

245. Swindle Dissent, *supra* note 242.

246. Touch Tone Complaint, *supra* note 242, at *5–6; *see id.* Swindle Dissent, *supra* note 242.

247. FTC v. Pereira, No. 99-1367-A (E.D. Va. Sept. 21, 1999) (order granting preliminary injunction), *available at* http://www.ftc.gov/os/caselist/9923264/990922prelim9923264.htm; *see also* Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Pereira, No. 99-1367-A (E.D. Va. Sept. 21, 1999) [hereinafter Pereira Complaint], *available at* http://www.ftc.gov/os/caselist/9923264/990922comp9923264.htm.

including one site that appeared to be a good copy of the Harvard Law Review home page.[248] Consumers suffered no monetary harm.[249] Potential harms included waste of time, frustration, risk of possible embarrassment, potential employer discipline to consumers who were directed to pornographic sites while at work, and risk of exposure to children of pornographic material.[250] These harms are more emotional and psychological than economic, yet the practices clearly were unfair and the FTC was right to prosecute them as such.[251]

ReverseAuction.com involved the use of personal information for unauthorized purposes, where the information was given voluntarily for other purposes.[252] ReverseAuction.com joined eBay as a customer but then obtained other eBay members' e-mail addresses and sent them solicitations to join its competing auction site.[253] A divided FTC thought that consumer injury was substantial because consumers had given eBay their e-mail addresses thinking that the information would not be used in this way.[254] Although the information was obtained through deceptive means, the injury is not materially different when any Web site sells e-mail or home addresses to a third party that intends to use the information to send spam, junk mail, or other commercial solicitations without the users' express permission.[255] As in *Touch Tone*, ReverseAuction.com's acquisition of the information may have been more objectionable because it involved false pretenses, but the injury to consumers essentially was the same.[256] Consumers voluntarily gave information thinking it would be used for one purpose, and it was then used for a different and objectionable purpose without their consent.[257]

b. Countervailing Benefits to Consumers or to Competition

The second inquiry in the unfairness test is whether benefits to consumers or to competition outweigh the consumer injury.[258] In the

248. Press Release, FTC, FTC Halts Internet Hijacking Scam (Sept. 22, 1999), *available at* http://www.ftc.gov/opa/1999/09/atariz.htm.

249. *See id.* The FTC did not allege that consumers had suffered monetary harm. *See* Pereira Complaint, *supra* note 247.

250. *See* Pereira Complaint, *supra* note 247.

251. The working rule at the FTC was to avoid pleading unfairness if at all possible. *See* Beales III, *supra* note 227, at n.12.

252. *See* FTC v. ReverseAuction.com, Inc., No. 00 0032, 2000 U.S. Dist. LEXIS 20761 (D.D.C. Jan. 10, 2000); Complaint for Permanent Injunction and Other Equitable Relief, FTC v. ReverseAuction.com, Inc., No. 00 0032 (D.D.C. Jan. 12, 2000) [hereinafter ReverseAuction.com Complaint], *available at* http://www.ftc.gov/os/2000/01/reversecmp.htm.

253. ReverseAuction.com Complaint, *supra* note 252.

254. *See* Statement of Commissioners Orson Swindle and Thomas B. Leary Concurring in Part and Dissenting in Part in *ReverseAuction.com, Inc.*, File No. 0023046, *available at* http://www.ftc.gov/os/2000/01/reverses1.htm (last visited Dec. 1, 2005).

255. *See* ReverseAuction.com Complaint, *supra* note 252.

256. *Id.*; Touch Tone Complaint, *supra* note 242, at *3–6.

257. *See* ReverseAuction.com Complaint, *supra* note 252.

258. Beales III, *supra* note 227, at 195.

context of online collection and sale of information, the question is whether consumers benefit from surreptitious data collection in ways that outweigh any consumer injury.[259] This inquiry is likely to be the most troubling when challenging online information practices because there are several benefits that a Web site might argue outweigh any injury. A site may be able to offer better quality of services, quicker downloads, better graphics, or lower prices because it is profiting from the collection and sale of information. If privacy policies became salient, more consumers would not share personal information, profits would be reduced, and either services would suffer or users would pay more for them. In addition, if privacy practices became salient, firms likely would need to adopt systems to honor more opt-in and opt-out requests and employ additional security measures to see that consumers' privacy preferences were honored, all at additional cost.

Another arguable benefit to undisclosed or non-salient privacy practices is consumer convenience. To make privacy practices salient, the Web site would need to take steps to bring the policy to the attention of users. Drawing attention to even a short summary of a firm's information sharing practices likely would be seen as a nuisance by many Web site users. If a site required users to visit and assent to its privacy policy, even with a quick mouse click, the inconvenience would be noticed.

The basic analytical problem with this part of the unfairness test is that it requires the FTC to compare incomparable values. It is difficult to quantify a consumer injury resulting from unwanted information collection and use.[260] Some harms can be individual and identifiable—identity theft costs might be quantified, for example, by examining the money lost by consumers and credit grantors due to theft. Other harms, such as increased spam, e-mail, junk mail, and pop-up ads, are difficult to reduce to monetary or other economic terms. Societal harms resulting from consumer profiling and manipulation of consumer preferences are even harder to quantify.[261] In a cost-benefit calculation to determine whether the harms outweigh the benefits, it may be easier for businesses to demonstrate the costs of a required change in information practices and the monetary benefits that result from widespread data collection and sale.[262] Given the basic incomparability of consequences, both good and bad, deciding whether harms of data practices outweigh countervailing benefits is bound to be subjective and difficult to support empirically in many cases.

---

259. *See* Nehf, *supra* note 172, at 31–32.

260. *See id.* (stating that calculating a value for personal information is almost impossible).

261. *See id.* at 8.

262. *See* Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 157, 169–71 (2002) (estimating the costs of various privacy-enhancing proposals but conceding that valuing the benefits of privacy protection is extremely difficult).

To overcome these difficulties, the FTC would need to expand its view of cognizable consumer injury to include societal harms and harms that are somewhat speculative and not easily quantifiable. For example, the sale of information to a third party that allows the purchaser to personally identify consumers without their express consent should be viewed as a more cognizable harm than the disclosure of non-identifiable data, even if there is no evidence that the disclosure resulted in identity theft or other economic injury. A significant risk of harm should be sufficient, as the FTC found in *Touch Tone*.[263] On the other side of the balancing test, the agency should closely scrutinize claims by online firms that they are bestowing benefits on consumers by using their personal information in ways that many consumers would find offensive, or at least insist on proof that the benefits are real.

c. Reasonable Avoidance

The consumer avoidance part of the unfairness test is less problematic when privacy terms are not salient. People have a reasonable opportunity to avoid a privacy injury only if the firm's practices are incorporated into the decision process. If there are rational reasons why a posted privacy policy is not salient to the vast majority of consumers, then consumers cannot reasonably avoid unfair information practices simply by reading the policy and taking steps to withhold personal information. In the past, the FTC has brought actions against firms that take advantage of poorly informed decision making. In *International Harvester*, a firm manufactured tractors that were subject to fuel geysering, or the rapid expulsion of hot fuel from gas tanks when a user loosened the gas cap.[264] Discussing whether farmers reasonably could have expected and avoided injury, the FTC concluded that farmers may have known that loosening the fuel cap on a hot engine was a poor practice, but they could not be expected to comprehend the full consequences that might result.[265]

The FTC has found this part of the unfairness test satisfied even when consumers had been given the information in writing that put them on notice that their rights were being violated. In *Orkin*, a pest exterminating company offered "lifetime" contracts at fixed rates in written contracts. Over the years, the contracts became unprofitable, and Orkin raised its rates.[266] Some consumers read their original contracts, noticed the promise of fixed rates, and complained.[267] Orkin

263. *See* FTC v. Rapp (*Touch Tone*), No. 99-WM-783, 2000 U.S. Dist. LEXIS 20627 (D. Colo. June 27, 2000), *available at* http://www.ftc.gov/os/2000/06/touchtoneorder.htm; Swindle Dissent, *supra* note 242.

264. *In re* Int'l Harvester Co., 104 F.T.C. 949, 950 (1984).

265. *Id.* at 1066.

266. *In re* Orkin Exterminating Co., 108 F.T.C. 263, 264 (1986), *aff'd*, 849 F.2d 1354 (11th Cir. 1988).

267. Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1358 (11th Cir. 1988).

reduced the rates of complaining customers, but continued to charge higher rates to customers who did not re-read their contracts and complain.[268] The FTC said this was unfair, concluding that it was not reasonable to require consumers to find the contract, notice the fixed-rate commitment, and complain about the increases.[269] A similar position could be taken with privacy policies. In most instances, expecting consumers to read privacy policies, understand their import, and take protective action will be unreasonable.

2. Deceptive Data-Collection Practices

To determine if conduct is deceptive, the FTC asks whether there was a material statement or omission that is likely to mislead consumers acting reasonably under the circumstances.[270] Deception is easy to prove when a firm does not follow its published privacy practices, and on several occasions the agency has brought actions against firms that stated privacy practices but did not adhere to them.[271] More difficult are cases in which no privacy policy is stated or when a policy is followed but it is weaker than consumers ordinarily would expect.

Historically, the FTC has offered little protection for pure omissions of relevant information. Omissions can be deceptive only under circumstances in which silence constitutes an implied but false representation.[272] For example, by offering goods for sale, a merchant makes an implied representation that the goods are reasonably fit for their intended uses and free of safety hazards.[273] Applying this precedent to privacy practices, the FTC could conclude that if a Web site does not post a privacy policy, its privacy practices are deceptive if disclosure of the site's information practices would be necessary to correct a basic assumption upon which users are reasonably relying.[274] The FTC could bring such an action against a firm whose information collection and sharing practices far exceed generally held consumer expectations. Studies show, however, that Internet users are increasingly aware of the potential for data collection online.[275] Thus, the basic assumption of a growing number of consumers today is that data is being collected and sold all the time. As this assumption becomes more widespread among

---

268. *Id.* at 1359.

269. *Id.*

270. *See In re* Cliffdale Assocs., 103 F.T.C. 110, 153 (1984); Patricia P. Bailey & Michael Pertschuk, *The Law of Deception: The Past as Prologue*, 33 AM. U. L. REV. 849, 850 (1984).

271. *See, e.g.*, Complaint, *In re* Gateway Learning Corp., No. C-4120 (Sept. 10, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf. *See also, e.g.*, FTC, Unfairness & Deception: Enforcement, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Dec. 14, 2005).

272. *In re* Int'l Harvester Co., 104 F.T.C. 949, 1058 (1984).

273. *In re* Figgie Int'l, Inc., 107 F.T.C. 313, 379 n.17 (1986).

274. *See* Thomas J. Holdych, *Standards for Establishing Deceptive Conduct Under State Deceptive Trade Practices Statutes That Impose Punitive Remedies*, 73 OR. L. REV. 235, 294 (1994).

275. *See supra* text accompanying notes 57–67.

Internet users, it will be more difficult to establish a deception case if a firm chooses not to publish its information practices.

If a Web site mentions a privacy policy, however, an allegation of deception should be sustained even if the site does not technically breach its stated terms. If a Web site makes statements that would lead a reasonable consumer to believe that the site's privacy practices are strong—a practice that is not uncommon—it is deceptive if those practices are in fact weak. Stating "we care about your privacy" in the lead sentence of a privacy policy could be deceptive if the policy allows for the wholesale collection and distribution of information to third parties. The conduct could be deceptive even if subsequent paragraphs or links explained the practices accurately. As behavioral research shows, consumers acting rationally are not likely to read and understand the details of the privacy policy.[276] They will rely on heuristics and other decision-making strategies to form conclusions about a site's privacy practices, taking the site at its word that its practices are strong.[277]

More than thirty years ago, the FTC brought an action against Metromedia, which had sent consumers a form letter and questionnaire inviting them to answer several questions, submit the form, and become eligible for prizes.[278] In fact, Metromedia had requested the information to generate direct mail solicitation lists.[279] The FTC complaint charged Metromedia with deceptive conduct by implying that the questionnaires were sent for purposes different from their intended use, even though the questionnaires did not explicitly state the purpose for which Metromedia would use the information.[280] The complaint acknowledged a significant consumer interest in keeping personal information private, noting, "A substantial portion of the purchasing public has a preference that their names not appear on mailing lists."[281] The action resulted in a consent order, and the FTC never had to prove its case, but the proceeding indicates that the agency believed the challenged conduct was deceptive.[282] The practices of many Web sites are not functionally different. If a site gives the impression that it cares about consumer privacy and collects information that consumers reasonably believe they are providing only for a limited purpose, it is deceptive to use the information for other purposes, even if the site discloses its information sharing practices in a published policy.

276. Coupey, *supra* note 152, at 83.
277. *See supra* text accompanying notes 149–55.
278. *In re* Metromedia, Inc., 78 F.T.C. 331, 333 (1971).
279. *Id.* at 337.
280. *Id.*
281. *Id.*
282. *Id.* at 338–40.

3. Effective Use of Limited FTC Resources

Of course, the FTC has limited resources and cannot afford to prosecute every Web site that engages in deceptive or unfair privacy practices. This does not mean that the FTC cannot bring more privacy cases, however, especially if the agency selects cases that set important precedents without expending substantial resources. Highly publicized FTC actions likely would have a deterrent effect, and online firms would be well advised to follow FTC policy statements and precedents rather than risk the publicity and expense of a regulatory confrontation. One commentator has observed, "Companies do heed the words of the FTC and do respond to problems the FTC identifies through its enforcement actions."[283]

Although the FTC has retreated from its earlier call for federal privacy legislation,[284] its chairman has indicated that the resources dedicated to enforcing existing rules should be increased by as much as fifty percent.[285] When the FTC has initiated privacy enforcement actions, they generally have settled quickly, limiting the investments needed to obtain results.[286] The FTC also could engage consumer advocacy groups to review the privacy practices of Internet firms, working with industry trade associations in a cooperative venture to encourage voluntary reform.[287] Partnering with the private sector would allow the FTC to devote its resources to prosecuting the most serious offenders, aided by industry watchdog groups that could help identify such offenders.[288]

IV. CONCLUSION

Creating a law of online information privacy that results in an efficient balance of interests may be an impossible task. Web site operators come in all shapes and sizes, and they use personal information in a wide variety of ways, some good and others harmful. Consumers are not a monolithic force, and they show varying levels of concern about perceived misuses of their personal information. They also want the benefits that information sharing can bring. Given the vast array of commercial interests and consumer privacy preferences involved in

283. Devin Gensch, *Putting Enforcement First*, THE RECORDER, Nov. 7, 2001, at 5 (commenting that being subject to a FTC § 5 action is "like facing a nuclear bomb in a food fight"); *see also* Julia Gladstone, *The U.S. Privacy Balance and the European Privacy Directive: Reflections on the United States Privacy Policy*, 7 WILLAMETTE J. INT'L L. & DISP. RESO. 10, 28 (2000) ("Upon the recommendation of the FTC many web sites now publish their privacy policies . . . .").

284. *See supra* text accompanying note 13.

285. Muris, Protecting, *supra* note 13.

286. *See* Robert R. Schriver, *You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission*, 70 FORDHAM L. REV. 2777, 2813 (2002).

287. *See* Tom Valuck, *Keeping Dietary Supplement Regulations Slim and Fit: Finding a Healthy Balance Between Paternalism and Consumer Choice*, 2 GEO. J.L. & PUB. POL'Y 285, 313 (2004).

288. *Id.* (recommending public-private partnerships to assist the FTC in policing the dietary supplement industry).

online activity, it is no wonder that the FTC and other market regulators, for the most part, have chosen to let market forces decide the outcome.

Studies in consumer decision making, however, reveal important and perhaps intractable difficulties in consumers' ability to shop for privacy. Until privacy becomes a salient attribute influencing consumer choice, Web site operators will continue to take and share more personal information than consumers would choose to provide in a more transparent exchange. Market regulators can allow the inefficiencies to persist, hoping that consumers will be better able to police their interests in time, but a passive approach has a price, and it is not insubstantial. While regulators wait for market mechanisms to evolve to the point at which a more efficient balance is achieved, the privacy interests of countless consumers will be compromised in ways that could have been prevented with more aggressive action. In addition, inaction allows data-collection practices to crystallize and powerful interests to become entrenched, making it more difficult to initiate change in the future.

During this period of evolving consumer attitudes and business responses to concerns about information privacy, the FTC can set the boundaries for acceptable methods of data collection and sharing. A sensible path between regulatory passivity and legislative mandates is more aggressive prosecution of unfair and deceptive privacy practices on a case-by-case basis. Much as common law principles have evolved over time, common themes about fair information practices are likely to emerge through individual enforcement actions. Compared to a broad-based legislative approach, the ebb and flow of an incremental, evolutionary process is less likely to set inefficient norms in stone, and adjustments can be made over time as businesses obtain and manipulate personal information in increasingly sophisticated ways. In accepting this challenge, the FTC must consider the cognitive limitations on consumers' abilities to protect their interests online and hold firms accountable when they unfairly take advantage of these limitations to the detriment of privacy interests. With a better understanding of the methods by which consumers make decisions online, the agency can bring actions to ensure that market-based approaches to privacy concerns have a legitimate chance of success.