William Mitchell Law Review

Volume 37 | Issue 4 Article 9

2011

The FTC's Proposed Framework for Privacy Protection Online: A Move Toward Substantive Controls or Just More Notice and Choice?

James P. Nehf

THE FTC'S PROPOSED FRAMEWORK FOR PRIVACY PROTECTION ONLINE: A MOVE TOWARD SUBSTANTIVE CONTROLS OR JUST MORE NOTICE AND CHOICE?

James P. Nehf†

The Federal Trade Commission (FTC) made headlines in December 2010 when its staff released a "Proposed Framework" for privacy protection on the Internet.[1] Most of the attention was drawn by a controversial "do not track" proposal that could significantly restrict the surreptitious collection and use of personal information obtained from individuals browsing online.[2] Relatively little attention was paid to other parts of the report, which for the most part continue the FTC's emphasis on self-regulation and its preference for notice and choice regimes over mandatory privacy norms.

† Professor of Law and Cleon H. Foust Fellow, Indiana University School of Law-Indianapolis.

1. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (2010) [hereinafter PROPOSED FRAMEWORK], *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

2. *Id.* at 63–69.

This article argues that the FTC, and Congress if necessary, should recognize that a notice and choice approach to privacy protection is not likely to protect consumer interests in most modern day settings. Indeed, policy makers may be doing more harm than good by continuing to focus on notice and choice, thereby giving a misleading impression that privacy is being protected when it is not. Moreover, by adhering to a notice and choice regime, they avoid discussing the more difficult yet most fundamental questions in the privacy debate. Under what circumstances is data collection likely to harm individuals, and when is it benign? If a practice is reasonably likely to cause harm, what is the most effective way to prevent the harm from occurring? Even if data collection causes no direct harm, should it still be limited if it undermines other values, such as personal autonomy, or should we just accept that our lives are increasingly an open book?

When reviewing the Proposed Framework, one should keep in mind the agency's history in this area. For more than two decades, the FTC has struggled to formulate an effective and coherent approach to regulating privacy as information technologies advance at a rapid pace. Beginning in the late 1990s, the agency conducted studies on consumer privacy preferences and business privacy practices online.[3] The studies confirmed that a vast amount of personal information was being collected without consumer knowledge or consent, and use of that data often did not conform to the expectations and preferences of most individuals.[4] The disconnection between individual preferences and business practices prompted the FTC to call for national legislation to mandate fair information policies on the Internet by the end of the twentieth century.[5]

Following stiff resistance from the online business community and a change in FTC leadership in 2001, the agency quieted its calls for privacy mandates and, instead, moved to encourage

3. In 2000, the FTC concluded that industry measures were far from adequate and that national privacy legislation was needed. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 38 (2000) [hereinafter FED. TRADE COMM'N, PRIVACY ONLINE 2000], *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

4. *Id.* at 2, 9–10.

5. *Id.* at 36–38 ("The proposed legislation would set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites . . . .").

industry self-regulation.[6] The move saw some initial success. The continuing threat of legislative or regulatory mandates was serious enough for large online firms to implement voluntary privacy practices and publish privacy policies that explained, at least in general terms, what types of information were being collected and how that information was used. Although smaller online firms were initially reluctant to follow, many changed their policies after several large firms announced that they would no longer advertise or link to websites that did not publish their privacy policies.[7]

The FTC lauded this move toward greater transparency in its market-driven solution.[8] Privacy policies could be found on countless websites and they fostered an impression among the general public that most websites collected only information that was needed for internal purposes, that the personal information would not be sold, traded, or used for other purposes, and that adequate security measures were in place. When the policies were read, however, there was often little privacy protection being promised. Thus, despite the proliferation of privacy policies online, consumers' privacy interests were no better protected than they were the decade before.

The FTC took a similar approach in other areas where emerging technologies were raising privacy concerns. In 2005, the FTC encouraged a self-regulatory privacy regime that focused largely on disclosure of Radio Frequency Identification (RFID)

6. *See* Timothy J. Muris, Chairman, Fed. Trade Comm'n, The Privacy 2001 Conference: Protecting Consumers' Privacy: 2002 and Beyond (Oct. 4, 2001) [hereinafter Muris, The Privacy 2001 Conference], *available at* http://www.ftc.gov/speeches/muris/privisp1002.htm(concluding that it is too soon for the FTC to fashion workable legislation to address strong consumer privacy concerns); *see also Challenges Facing the Federal Trade Commission: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Prot. of the H. Comm. on Energy and Commerce*, 107th Cong. 10–34 (2001) (testimony of Timothy J. Muris, Chairman, Fed. Trade Comm'n), *available at* http://ftp.resource.org/gpo.gov/hearings/107h/76308.pdf (noting a majority of the Commission did not support online privacy legislation at that time and the FTC's focus would remain on the enforcement of current laws).

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

8. *See* Muris, The Privacy 2001 Conference, *supra* note 6 ("One of the agency's successes has been encouraging Internet sites to post privacy notices."). Indeed, in 1998, only two percent of all sites had some form of privacy notices. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 27 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf. By 2000, virtually all of the most popular commercial websites had privacy notices. *See* FED. TRADE COMM'N, PRIVACY ONLINE 2000, *supra* note 3, at 10.

presence and consumer choice on the subject of the expanding use of RFID technologies in retail and other consumer settings:

> Commission staff agrees that industry initiatives can play an important role in addressing privacy concerns raised by certain RFID applications. *The staff believes that the goal of such programs should be transparency. For example, when a retailer provides notice to consumers about the presence of RFID tags, the notice should be clear, conspicuous, and accurate.* The notice should advise consumers if an RFID tag or reader is present and if the technology is being used to collect personally identifiable information about consumers. This clarity is particularly important when a disclosure concerns an unfamiliar technology, as is the case with RFID. Similarly, if a company's program provides consumers with *the option of removing the RFID tag*, the company's practices should make that option easy to exercise by consumers.[9]

EPCglobal, an industry-sponsored organization created to promote worldwide adoption and standardization of the Electronic Product Code (an essential part of RFID technology in its current form), adopted "Guidelines on EPC for Consumer Products" in 2005.[10] Consistent with the FTC's approach, the Guidelines call for consumer notice and education about RFID use in consumer transactions, but little in the form of substantive controls on the collection and use of information.[11] Privacy and civil liberties

9. FED. TRADE COMM'N, RADIO FREQUENCY IDENTIFICATION: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS 22–23 (2005) (emphasis added) (citations omitted), *available at* http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf. Legislators in several states and the U.S. Congress have introduced legislation requiring that consumers be notified when RFID tags and readers are present in public locations, but no laws have been enacted to date. *See* Laura Hilder, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133, 151–52 (2006) (exploring RFID technology and legislation strategies to protect consumer privacy); Kyle Sommer, *Riding the Wave: The Uncertain Future of RFID Legislation*, 35 J. LEGIS. 48, 68–70 (2009) (analyzing privacy concerns and legislation specific to RFID technology).

10. *Guidelines on EPC for Consumer Products*, GS1US.ORG, http://www.gs1us.org/epcglobal_us/consumer_awareness/guidelines_on_epc_for_consumer_products (last visited April 16, 2011).

11. Under the Guidelines, companies using RFID tags on products or packaging should include a label or identifier indicating the presence of the tag. *See id.* EPCglobal has developed a template label that companies can use to inform consumers of the presence of RFID tags. *Retailers Tool Kit*, GS1.ORG, http://www.gs1.org/epcglobal/public_policy/retailers_tool_kit (follow "Images" hyperlink) (last visited Mar. 8, 2011). The template label discloses that a

groups maintained that in many circumstances it is insufficient simply to notify consumers that RFID technology is being employed. Both the Center for Democracy and Technology and the Electronic Privacy Information Center encouraged a stronger privacy protection regime, particularly when data collected through RFID technology can be stored and linked to personal information about an individual collected either through the RFID system itself or in combination with other databases.[12] Their complaints went unheeded by EPCglobal, the FTC, Congress, and most state legislatures.

With respect to behavioral advertising online, in 2009 the FTC issued a staff report supporting the development of stronger self-regulatory privacy practices, focusing again on the disclosure of privacy practices and the opportunity for consumers to opt-out of certain behavioral advertising practices on websites that use them.[13] Except for the collection and use of highly sensitive information, such as medical information, the report included few substantive privacy mandates.[14]

particular product or package contains an RFID tag that in most cases may be discarded by a consumer after purchase. *Id.* The Guidelines' second requirement, "Consumer Choice," provides that consumers should be "informed of the choices that are available to discard or remove or in the future disable RFID tags from the products they acquire." *See Guidelines on EPC for Consumer Products*, GS1US.ORG, *supra* note 10. The Guidelines explain that, "for most products, the EPC tags would be part of disposable packaging or would be otherwise discardable." *Id.* The third prong of the Guidelines provides that consumers should have "the opportunity easily to obtain accurate information about EPC and its applications." *Id.* The Guidelines state that companies using EPC in a consumer setting should "familiarise consumers with the EPC logo and . . . help consumers understand the technology and its benefits." *Id.* More information about the template label is available on the EPCglobal website, along with an explanation of RFID technology for consumers.

12. *CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology*, CDT.ORG, http://www.cdt.org/privacy/20060501rfid-best-practices.php (last visited Mar. 8, 2011); GUIDELINES ON COMMERCIAL USE OF RFID TECHNOLOGY, ELEC. PRIVACY INFO. CTR. 2–4 (2004), *available at* http://epic.org/privacy/rfid/rfid_gdlnes-070904.pdf.

13. FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

14. *Id.* at 42 ("[C]ompanies should only collect sensitive data for behavioral advertising after they obtain affirmative express consent from the consumer to receive the advertising.").

When the FTC released the new Proposed Framework at the end of 2010 after it had conducted several workshops and solicited comments from stakeholders, including many privacy advocates, some hoped that the agency would signal a shift in its approach and advocate mandatory privacy norms with less reliance on notice and consent. While it is still unclear what direction the agency intends to move, except for the "do not track" proposal, the report largely maintains the status quo.[15] There is a noticeable change in rhetoric, which may portend a different strategy down the road, but little more. Signaling what could be a move toward stronger substantive privacy mandates in the future, the report states that "companies should adopt a 'privacy by design' approach by building privacy protections into their everyday business practices."[16] Companies should maintain reasonable security for consumer data, collect only the data needed for a specific purpose, retain data only as long as necessary, and implement reasonable procedures to promote data accuracy.[17] The agency recognized that "[s]uch concepts are not new,"[18] but the Proposed Framework suggests that a company's failure to take such measures could attract agency attention. It remains to be seen whether the agency will develop rules or guidelines to implement the "privacy by design" concept and bring enforcement actions under its unfairness jurisdiction to demonstrate that "privacy by design" implies justiciable standards—not merely laudatory goals.

Most of the other proposals assume that notice and choice should be the dominant approach to privacy protection online, and that the model need only be improved at the margins to be more effective. For example, the report proposes that companies provide choices to consumers about their data practices in a simpler form that would be easier to understand.[19] Consumers

15. The "do not track" proposal, while controversial, does not signal a significant shift away from notice and consent. It is one application of a notice and consent approach that allows individuals to opt-out of data sharing by using a browser utility that would block certain data collection functions. PROPOSED FRAMEWORK, *supra* note 1, at 66. It is only controversial because it makes opting out of data collection much easier than other largely unsuccessful notice and consent mechanisms that require considerably more effort to (a) realize that there is some disclosure and an opt-out opportunity, and (b) navigate the steps necessary to exercise the option.

16. *Id.* at v (citation omitted).

17. *Id.*

18. *Id.*

19. *Id.* at 52–53.

should be able to make more "informed and meaningful choices" about what information they share and with whom.[20] Opt-out opportunities should be more clearly described and offered at a time when the consumer is making a decision about disclosing personal information.[21] Privacy policies should be "clear, concise, and easy-to-read."[22] The assumption is that if consumers can better understand privacy notices and are given more opportunities to make informed choices about sharing information, their interests will be adequately safeguarded. The guiding principle is that there is an effective market for information sharing that can be enhanced by better disclosure and more opportunities for people to make information sharing choices; for example, consumers could make informed decisions about revealing information as they interact with online firms.[23]

The ongoing effort to tweak the notice and choice model is not surprising. Since the Organization for Economic Cooperation and Development (OECD) guidelines on privacy in 1980, notice and choice regimes have been recognized as the central part of fair information practices regardless of the technology being used to collect and store data.[24] The generally accepted norms guiding the regime are openness and transparency in the collection, storage, and use of personal information, and faith in the ability of people to act in their best interests. It assumes that consumers can assert their privacy preferences if they are given sufficient information.

While notice and choice may have been a viable approach to protecting privacy in 1980, it is no longer viable following three decades of technological advancement that have brought us to the point where we have access to information whenever we want it, wherever we happen to be, and with the ability to share it almost instantaneously with anyone we choose. Giving consumers opportunities to opt-out of information sharing does not justify

20. *Id.* at vi.

21. *Id.* at 57.

22. *Id.* at vii. *See generally* George R. Milne, Mary J. Culnan & Henry Greene, *A Longitudinal Assessment of Online Privacy Notice Readability*, 25 J. PUB. POL'Y & MARKETING 238 (2006) (evaluating the readability of 312 online privacy notices and arguing that such readability should be improved as a matter of marketing and public policy).

23. *See* Milne, Culnan & Greene, *supra* note 22, at 238.

24. *See, e.g.*, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980) (recognizing the importance of notice and disclosure for privacy concerns internationally).

excessive data collection, transfers of personal information to others for uses not contemplated by the individual who revealed it, or failure to create and maintain reasonable storage security measures. Notice and choice must be supplanted by responsible information practices throughout the data collection and storage process, mandated by law if necessary. The FTC's approach to privacy is essentially backwards: a privacy regime should be most concerned with limiting the collection and dissemination of personal information in the first place because once the information is collected its subsequent use cannot be controlled. Questions of informed consent should only be considered at the margins.

Under the FTC's self-regulatory principles, protecting consumer privacy is largely the responsibility of individuals who are expected to learn about the privacy practices of data collectors and take steps to minimize privacy risks.[25] This self-policing model could be made effective by enhanced notice and choice opportunities if individuals were capable of protecting their privacy preferences. Unfortunately, for many reasons, they are not.

I. LACK OF TRANSPARENCY MAKES DECISION MAKING PURE GUESSWORK

The data collection, storage, and manipulation industry is becoming more sophisticated and less transparent every day. The vast majority of data collection and sharing practices occur outside public view.[26] Our personal information is stored, searched, and transmitted every day; yet, we have no idea what the ramifications may be (good or bad) or what decisions are being made in reliance on it. If we do not understand what is going on behind the scenes, then information practices that many of us would object to will largely go undetected.[27] No matter how much notice we are given,

25. PROPOSED FRAMEWORK, *supra* note 1, at 40 ("For example, although the proposed framework provides for notice and choice, it aims to simplify how companies present such notice and choice and to reduce the degree to which privacy protection depends on them.").

26. *See generally* Victoria Bellotti, *Design for Privacy in Multimedia Computing and Communications*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 63, 64–66 (Philip E. Agre & Marc Rotenberg eds., 1997) (discussing how ubiquitous computing and new user-friendly interfaces obscure data collecting intrusions on privacy).

27. *Cf.* Robert LaRose & Nora J. Rifon, *Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior*, 41 J.

we cannot evaluate the risk of potential harms, make informed decisions, seek redress, or stop harms from recurring because we cannot comprehend the benefits or the risks at the time when a decision has to be made.[28]

II. VALUING PRIVACY IS VIRTUALLY IMPOSSIBLE

Even with more information and choices available, individuals cannot effectively value their personal information. Notice and choice solutions presume that we can value our privacy rights in some meaningful way.[29] Only then can we make self-interested choices about whether and how to share information, and whether to take the time or expend the effort to safeguard that information. When it is impossible to know where our information will end up and how it will be used, it is difficult to assess the risks associated with releasing information or failing to monitor its use once we have given someone access to it. We might think we are only providing harmless facts and boring details, and we may perceive the risk as small compared to the benefits being offered by a data collector, not knowing how or when the seemingly harmless information might be shared or used in a way that will cause us harm.[30] There is a high degree of information asymmetry; collectors of information know what they intend to do with the data, but individuals who provide the data do not.[31] Under these

CONSUMER AFF. 127, 128 (2007) (suggesting that consumers do not understand the implications of sharing personal information because of inadequate privacy policies and seals).

28. *See* Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 103 (2002) ("Once an individual has sold her personal information, she loses much control over it. . . . Because of the immense amounts of data about any given individual already in the public domain, how would that individual verify when a contract was broken?").

29. *See generally* Curt J. Dommeyer & Barbara J. Gross, *What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies*, 17 J. INTERACTIVE MARKETING 34 (2003) (discussing a study on consumer awareness and use of privacy protection strategies).

30. *See* LaRose & Rifon, *supra* note 27, at 129 ("Internet privacy poses something of a paradox, some say even a fallacy. Surveys show that concerns about online privacy are widespread. . . . [But] Internet users willingly divulge personal information to obtain 'free' information, personalized content, customized discounts, prizes, loyalty program memberships, cajoling interactions with automated shopping 'agents,' or some other form of 'fair exchange.'" (citations omitted)).

31. *See generally* HAL R. VARIAN, MICROECONOMIC ANALYSIS 440 (3d ed. 1992) (providing a microeconomic analysis of how asymmetric information affects

conditions, individuals may undervalue (or overvalue) its release because they are unaware of the risks and benefits. Because they have no basis for valuing their information, decisions will nearly always be less than optimal.

III. AGGREGATION OF DATA IMPOSES UNKNOWABLE RISKS

A related problem is the difficulty in valuing specific pieces of personal information out of context. How does one value one's holiday shopping habits? To value this information with even rough accuracy (e.g., assess the risk of future harm resulting from someone having access to the data), one needs to know how the information will be used. The information might be sold to a marketing firm in the aggregate (along with data from other anonymous shoppers) without any personal identification, in which case its value to any particular person is nominal because the risks of future harm are small. Opting out of such data sharing is totally unnecessary, and from a societal point of view, the decision is inefficient because it deprives the data collector of potentially useful information while not remotely benefiting the individual. On the other hand, if the information is transferred and aggregated with other information that can link the data to an individual, we might value it much higher. If a person thought it could lead to identity theft, the information might not be released at any price.[32] The problem is that once information is stored and is capable of being accessed, we lose control over its use, and we seldom have enough knowledge to evaluate the risk of future harm. Making meaningful choices under these circumstances is impossible.

behaviors and strategic interactions between persons).

32. *Cf.* Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 CORNELL J.L. & PUB. POL'Y 661 (1999) (describing identity theft methods and the importance of one's identity). *See generally* Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423 (2001) (describing how identity theft occurs and ways to prevent it).

IV. LACK OF ACCOUNTABILITY RENDERS PRIVACY DECISIONS LESS MEANINGFUL

There are insurmountable accountability problems with today's data collection and sharing practices. Tracing harm to a particular source or data breach will usually be impossible. If a person is affected in some way by the unexpected misuse of personal information, even noticing the problem may be difficult, and tracing the problem to a particular release of information will be nearly impossible because information about us resides in so many databases.[33] Without accountability, market forces cannot effectively curb wrongful behavior. Moreover, injury resulting from data collection and sharing, while economic in some cases, can be impossible to undo even if it is discovered and traced to a particular source. Many injuries resulting from identity theft, lost employment opportunities, and reputation damage cannot be compensated even if the harmful information can be traced to a particular source. Most importantly, without accountability, individuals faced with decisions about sharing personal information are left essentially with two unappealing choices: (1) prohibit the release of information wherever possible because one never knows where it will end up; or (2) do not be concerned with the release of information because such collection and use is inevitable and injuries are untraceable, so you can expect no redress for any adverse effects. With either decision, the choice is ill-informed and not likely to be consistent with the best interests of the individual.

V. ACCURATE CHOICES ARE COMPROMISED BY COMPETING GOALS

When making decisions about whether to divulge personal information, people compromise between their desire for complete accuracy (balancing the costs and benefits of the decision) and their desire to achieve other rational goals.[34] Other than

33. Hahn & Layne-Farrar, *supra* note 28, at 103 ("How do I know, for example, where a firm obtained my email address? Was it from me or some other available source that was legal? Vast amounts of personal data are already in the public domain. Consider, for example, telephone directories, employee personnel databases, credit reports, and other public or semi-public sources.").

34. *Cf.* Ellen C. Garbarino & Julie A. Edell, *Cognitive Effort, Affect, and Choice*, 24 J. CONSUMER RES. 147, 148 (1997) (examining cognitive effort and its influence

maximizing the accuracy of the decision, another important decision-making goal is the minimization of cognitive effort.[35] When making decisions, people tend to expend only as much effort as they need to reach what they perceive is a satisfactory decision, even if it is not optimal.[36] Unless the decision is of great importance, people tend to make choices that are easier to implement, though less accurate, because important factors are left out of the decision-making process.[37] Thus, giving individuals more disclosure and better opportunities to opt-out of information sharing is not likely to lead to more accurate decisions. Except for the most obviously sensitive information, people are not likely to expend the cognitive effort necessary to weigh the pros and cons. They will not perceive the stakes being high enough, so they will not even try to make a decision that serves their best interests.

VI. PRACTICAL PROBLEMS MAKE PRIVACY LESS SALIENT

Even when someone wants to evaluate privacy alternatives and make self-interested decisions, practical problems create obstacles that impede optimal decision making. The most important are time constraints. When people feel that they should make a decision quickly, people switch from more careful decision-making strategies to simpler ones that result in a faster decision.[38] While

on choice outcomes). *See generally* Jacob Jacoby, *Is It Rational to Assume Consumer Rationality? Some Consumer Psychological Perspectives on Rational Choice Theory*, 6 ROGER WILLIAMS U. L. REV. 81 (2000) (examining the limitations of rational choice theories); Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFF. 100 (2007) (discussing the privacy paradox and public policy about preserving one's sense of privacy).

35. James R. Bettman, Mary Frances Luce, & John W. Payne, *Constructive Consumer Choice Processes*, 25 J. CONSUMER RES. 187, 192–93 (1998) (providing a framework for understanding constructive consumer choice).

36. Garbarino & Edell, *supra* note 34, at 148.

37. *Id.* at 149; *see* Eric J. Johnson, John W. Payne & James R. Bettman, *Information Displays and Preference Reversals*, 42 ORG. BEHAV. & HUM. DECISION PROCESSES 1, 2 (1988) (discussing the frequency and occurrence of preference reversals and implications for information displays); Denis A. Lussier & Richard W. Olshavsky, *Task Complexity and Contingent Processing in Brand Choice*, 6 J. CONSUMER RES. 154, 154 (1979) (reporting results of a study on consumer choice strategy).

38. *See also* Bettman, Luce & Payne, *supra* note 35, at 200 (discussing the effects of time pressure on choice processes); Peter Wright, *The Harassed Decision Maker: Time Pressures, Distractions, and the Use of Evidence*, 59 J. APPLIED PSYCHOL. 555 (1974) (studying the effects of time pressure and distraction on an individual's decision-making process). *See generally* John W. Payne, James R. Bettman & Mary

there may be plenty of time to read the privacy practices of each website visited and make a choice about information sharing on each one, to do so would frustrate one of the principal benefits of going online—a fast and convenient way to learn, communicate, and purchase goods and services. Surfing the Internet would take forever if the privacy practices and opt-out procedures were explored at each site. Regardless of time constraints, as people make choices about whether and how to interact with a particular website, privacy concerns have to be perceived as important enough to capture their attention. If other attributes of the site are deemed more important (e.g., site content, ease of use, desirable interactive features), privacy alternatives are not likely to be explored before information is shared with the site.

VII. BEHAVIORAL HEURISTICS IMPACT PRIVACY CHOICES

Several behavioral factors make it unlikely that decisions about information sharing will be made with an accurate balancing of the benefits and risks.

Inferences play an important role in a person's decision whether to share information, yet they often lead to inaccurate privacy choices. If the information necessary to making an informed decision is difficult to obtain, people infer the missing information from information that is more readily available. People may assume that a particular attribute is similar across brands (e.g., the privacy practices of all banks are probably about the same), or people may infer a value that corresponds to the values they assign to other attributes of the party with whom they are interacting (e.g., if my personal banker is trustworthy and caring, the bank's privacy practices are likely trustworthy as well).[39]

Frances Luce, *When Time Is Money: Decision Behavior Under Opportunity-Cost Time Pressure*, 66 ORG. BEHAV. & HUM. DECISION PROCESSES 131 (1996), *available at* http://faculty.fuqua.duke.edu/~jrb12/bio/Jim/46.pdf (investigating decision processes in environments where there is time stress due to the opportunity-cost of delaying decisions); Rik Pieters, Luk Warlop & Michel Hartog, *The Effect of Time Pressure and Task Motivation on Visual Attention to Brands*, 24 ADVANCES IN CONSUMER RES. 281 (1997) (discussing a study of consumer choices under various time pressure settings), *available at* http://www.acrwebsite.org/volumes/display.asp?id=7883.

39. *See, e.g.*, Gary T. Ford & Ruth Ann Smith, *Inferential Beliefs in Consumer Evaluations: An Assessment of Alternative Processing Strategies*, 14 J. CONSUMER RES. 363, 370 (1987) (discussing results of a study that shows consumers employ a same-brand strategy in inference formation); Richard D. Johnson & Irwin P. Levin, *More*

Some inferences may be justified, but others will lead to privacy decisions that do not reflect the person's actual preferences.

Framing effects may also adversely affect the accuracy of decisions. People tend to process information in a way that is consistent with how it was presented to them, accepting it in its presented form without questioning the details or inquiring further.[40] These framing effects are well-known in the marketing industry[41] and are most pronounced when the cost of accepting a particular presentation on its face is perceived to be low.[42] Only if the cost of acceptance is perceived to be high, or if the information is presented in a confusing way, will people discount the form of the presentation and seek additional information before making a decision. This is one reason why many links to privacy policies and opt-out opportunities contain language such as, "We value your

Than Meets the Eye: The Effect of Missing Information on Purchase Evaluations, 12 J. CONSUMER RES. 169 (1985) (exploring the effect of missing information on the processes of evaluation and decision making); Birger Wernerfelt, *Umbrella Branding as a Signal of New Product Quality: An Example of Signalling by Posting a Bond*, 19 RAND J. ECON. 458 (1988) (discussing "umbrella branding" in which a multiproduct firm uses its reputation and established products to introduce a new product); Michael D. Smith & Erik Brynjolfsson, *Consumer Decision-Making at an Internet Shopbot* 11 (MIT Sloan Sch. of Mgmt. Ctr. for eBusiness, Working Paper No. 137, 2001) (finding that brand is an important determinant of consumer choice), *available at* http://ebusiness.mit.edu/research/papers/137_erikbinternetshopbots.pdf.

40. *See* James R. Bettman & Michel A. Zins, *Information Format and Choice Task Effects in Decision Making*, 6 J. CONSUMER RES. 141, 142 (1979) ("[C]onsumers appear to process information in ways congruent with the presentation format, processing the information as it is structured, without rearranging it."); *see also* Paul Slovic, *From Shakespeare to Simon: Speculations—and Some Evidence—About Man's Ability to Process Information*, 12 OR. RES. INST. 12 (1972) (summarizing research experiments on decision making and explaining their implications), *available at* http://www.decisionresearch.org/pdf/dr36.pdf; W. Kip Viscusi, Wesley A. Magat & Joel Huber, *An Investigation of the Rationality of Consumer Valuations of Multiple Health Risks*, 18 RAND J. ECON. 465, 477–78 (1987) (describing consumers' responses to risk valuations); W. Kip Viscusi, *Individual Rationality, Hazard Warnings, and the Foundations of Tort Law*, 48 RUTGERS L. REV. 625, 634–36 (1996) (citing the frame of reference as one factor that affects the utility of hazard warnings).

41. *See, e.g.*, Irwin P. Levin & Gary J. Gaeth, *How Consumers Are Affected by the Framing of Attribute Information Before and After Consuming the Product*, 15 J. CONSUMER RES. 374 (1988) (discussing the implications of framing effects on consumer behavior in marketing products).

42. *See* Eloise Coupey, *Restructuring: Constructive Processing of Information Displays in Consumer Choice*, 21 J. CONSUMER RES. 83, 96–97 (1994) (summarizing the differing reasons for consumer restructuring).

privacy,"[43] rather than "You are about to divulge information that could harm you in the future. Click here to be sure you want to proceed." If the presentation form appears safe and unthreatening, individuals are less likely to dig beneath the surface and determine the strength of the site's privacy practices for themselves.

Another behavioral tendency is that people overreact to risks that are well-known because of news coverage or other events that bring the subject to their attention. Such risks are "available" in people's minds, and they therefore think the matter is important enough to make an informed decision.[44] Conversely, people tend to underreact to risks when they are not in the forefront of the mind. This availability heuristic becomes most relevant when people make decisions based on the perceived probability of certain events happening. People underestimate the likelihood of certain events occurring if those events do not come to their attention very often. 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 a fair amount of publicity about security leaks and unauthorized access to consumer databases, consumers seldom hear about the actual harms resulting from those privacy practices. Hearing about the occasional database breach raises a general societal concern about privacy, but we seldom hear that any particular consumer problem was traced to a specified data breach, or that particular types of information disclosure are more dangerous than others. 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 in our daily lives. If people do not see a particular information disclosure as a risky activity, they will not

43. *See, e.g.*, *We Value Your Privacy*, MY WORK BUTTERFLY, http://www.myworkbutterfly.com/page/we-value-your-privacy (last visited Feb. 25, 2011) (containing the privacy policy of Butterfly, a working mothers' social network). After the "We Value Your Privacy" title and introductory language, the policy states that if it acquires or is acquired by another business, the site "reserve[s] the right to transfer all of MyWorkButterfly.com's User information, including email addresses, to a separate entity or Platform." *Id.*

44. *See generally* Timur Kuran & Cass R. Sunstein, *Availability Cascades and Risk Regulation*, 51 STAN. L. REV. 683, 685 (1999) ("The purpose of this article is to identify a set of interlinked social mechanisms that have important, sometimes desirable, but at other times harmful effects on risk regulation.").

invest time and effort deciding whether the disclosure is actually in their best interest.

People are not good at making accurate decisions about low-probability risks—which are particularly important to privacy decisions. People tend to either overestimate the probability and take unnecessary precautions or ignore the risk and do nothing. Unless the unlikely occurrence is potentially catastrophic (e.g., the slight risk of a home burning causes us to purchase fire insurance), we are not willing to invest much time, money, or effort to reduce or evaluate a risk we think is not likely to occur.[45] People tend to view low-probability risks as either safe or unsafe, and overestimate or underestimate the likelihood of the event occurring.[46] This is one reason why some people refuse to reveal personal information whenever they are asked to do so, regardless of how harmless it may be (e.g., zip code request at a check-out register), while others do not think twice before disclosing private information to strangers. In addition, people are more likely to make the effort to evaluate risks (whether high- or low-probability) if they have prior experience with that type of risk.[47] Thus, people who have been victimized by identity theft may take time to exercise more opt-out rights, while those who have not do not bother.

Finally, if there is immediate and concrete feedback about the accuracy of a decision, people tend to spend more effort trying to get that decision right.[48] Conversely, if feedback about the accuracy of a decision is delayed or never comes, less effort is made to make

45. Gary H. McClelland, William D. Schulze & Don L. Coursey, *Insurance for Low-Probability Hazards: A Bimodal Response to Unlikely Events*, 7 J. RISK AND UNCERTAINTY 95, 109 (1993) (concluding that "[i]ndividuals appear either to dismiss low-probability risks . . . or to worry about the risk [too] much").

46. For example, when asked about the risks of lung cancer to smokers, both smokers and nonsmokers generally overestimate the risk. W. Kip Viscusi et al., *Smoking Risks in Spain: Part III—Determinants of Smoking Behavior* 2 (Harv. Law Sch., John M. Olin Ctr. for Law, Econ., and Bus., Discussion Paper No. 306, Nov. 2000), *available at* http://www.law.harvard.edu/programs/olin_center/papers/pdf/306.pdf.

47. *See* Bettman, Luce & Payne, *supra* note 35, at 188 ("People are most likely to have well-articulated preferences when they are familiar and experienced with the preference object, and rational choice theory may be most applicable in such situations.").

48. *See id.* at 193 (listing one of the most important goals for consumer decision making is maximizing the accuracy of the choice); *see also* Hillel J. Einhorn, *Learning from Experience and Suboptimal Rules in Decision Making*, *in* COGNITIVE PROCESSES IN CHOICE AND DECISION BEHAVIOR 1, 2 (Thomas S. Wallsten ed., 1980) (noting "outcome feedback" is the main source of information for evaluating the quality of decision making).

a decision that best fits our interests. This is important because the correctness of any decision about revealing personal information usually will not be apparent until long after the transaction has ended or, more likely, never. Only rarely will someone be able to trace the spam, identity theft, profiling, pop-up advertisement, junk mail, or other effects of information sharing to a particular data collector's privacy practices. Without feedback on our decisions about disclosing information, we have no way of knowing whether our decisions were good or bad. If the results of the decision will likely never be known, we do not invest much time trying to make the right choice.

VIII. CONCLUSION

In the last few years, much has changed about the way people reveal personal information. Today, a vast number of individuals access information from portable laptops, handheld phones, e-readers, and other devices at all hours of the day, from land, air, and sea locations throughout the world. Whether we are interacting on social networks or researching the latest news story online, we are constantly giving and receiving information about ourselves, whether knowingly or not. It is not surprising that firms have developed technologies and business plans that use our information in ways that were unimaginable a short time ago.

The FTC should be commended for issuing the Proposed Framework. In particular, the FTC's foundational principles of "privacy by design," if they are more than hopeful aspirations, may lead to meaningful substantive controls on the collection and use of personal information in the years to come. The Proposed Framework states that protecting privacy online should be the default position, information should only be collected and stored as needed, privacy should be protected throughout the information life cycle, and privacy practices should be designed with respect for individual interests from the start.[49] If these principles are widely adopted, companies will build applications that only gather and share information as needed, and they will build in privacy protections with individual users in mind. This would be a fundamental shift, but without legal mandates, one wonders

49. *See generally* PROPOSED FRAMEWORK, *supra* note 1 (calling on companies and policymakers to promote consumer privacy, simplified consumer choice, and greater transparency of data practices).

whether it will actually happen.

If the substantive controls of "privacy by design" are not widely adopted (e.g., if the FTC does not undertake an aggressive enforcement program to ensure adoption), all that remains in the Proposed Framework is an enhanced notice and choice regime that requires us to police our own privacy interests in situations where we are increasingly ill-equipped to do so. No matter how clear, conspicuous, and timely privacy notices and opt-out opportunities may be, people will seldom make decisions that accurately reflect their privacy preferences. Insurmountable problems regarding the transparency of privacy and data aggregation practices, the inability to hold firms accountable for harms caused by maintaining suboptimal privacy practices, and the practical realities and behavioral tendencies of individuals making decisions about privacy matters in an online environment all render even an enhanced notice and choice approach to privacy wholly ineffectual. If the FTC is serious about privacy protection, it will move aggressively to ensure that the substantive controls in its "privacy by design" initiative become the norm and abandon the outdated notion that personal information can be adequately protected by disclosure and individual decision making.