Protecting Privacy with Deceptive Trade Practices Legislation

Jeff Sovern

Recommended Citation
Available at: http://ir.lawnet.fordham.edu/flr/vol69/iss4/4
PROTECTING PRIVACY WITH DECEPTIVE TRADE PRACTICES LEGISLATION

Jeff Sovven*

INTRODUCTION

Informational privacy—the rights consumers may have to prevent the sale or use of their personal information—is much in the air these days. It has attracted considerable attention from the legal media,1 the general media,2 and various governmental entities.3

---

* Professor of Law, St. John’s University School of Law. A.B., J.D. Columbia University. The author thanks St. John’s University School of Law for its research support.


Commentators have proposed different approaches to addressing consumer privacy.4

One frequent theme of writers on informational privacy is whether existing law bars certain informational practices engaged in by various companies without the consent of affected consumers—chiefly the collection and sale of information about consumers and the use of this information to solicit consumers to make purchases. Many writers have opined on whether the invasion of privacy torts prohibit these practices.5 But few have discussed the possibility that these informational practices violate deceptive trade practices legislation.6 The purpose of this article is to do just that.


4. See, e.g., Bibas, supra note 1, at 591-92 (arguing for a contractual approach); Kang, supra note 1, at 1246-65 (arguing that the default rule for cyberspace privacy should be determined by economic efficiency and dignity); Posner, supra note 1, at 393 (using a law and economics approach to argue that common law has treated privacy correctly); Joel R. Reidenberg, Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?, 44 Fed. Comm. L.J. 195, 237-38 (1992) (suggesting that European systems offer guidance) [hereinafter Reidenberg, Privacy in the Information Economy].

For a list of those urging expansion of existing common law privacy doctrines to cover informational privacy, see infra note 54. For arguments seeking application of certain fairness considerations to privacy, see infra note 19. For those arguing that American privacy laws should be modified to accommodate European law, see infra note 24.

5. See infra notes 53-55 and accompanying text.

6. There is one recent exception. The Center for Democracy and Technology, Consumer Action, Privacy Rights Clearinghouse, and Private Citizen, Inc. petitioned the FTC to act concerning certain Pentium chips that reveal information about the users. See Complaint and Request for Injunction, Request for Investigation, and for Other Relief, available at http://www.cdt.org/privacy/issues/pentium3/990226intelcomplaint.shtml (Nov. 16, 2000).
I. THE TRADE IN PERSONAL INFORMATION

Information about consumers is obtained and used in a myriad of ways. Some companies notify consumers that they are collecting information, but many do not. Paul Schwartz has described the information business on the Internet as "a privacy horror show," but the offline information trade is hardly better.

Some businesses have acquired information in ways that are particularly troublesome. Three examples illustrate such objectionable practices. First, the manufacturer of a product for incontinent women invited people to call a toll-free line to receive samples. The manufacturer later attempted to peddle the list of the more than four million consumers who responded. Similarly, after a woman spent a night at a lodge, she began receiving solicitations targeted at lesbians. Apparently the lodge was frequented by lesbians, and it sold the names of guests to a lesbian mailing list.

7. I have discussed this in greater detail in Jeff Sovern, Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information, 74 Wash. L. Rev. 1033 (1999) [hereinafter Sovern, Opting In, Opting Out].


9. Kevin DeMarrais, Big Brother is Watching Your Database, The Record (Bergen N.J.), Apr. 30, 1995, at A1. For other examples of such behavior, see Jeffrey Rothfeder, Privacy for Sale 92-93 (1992) (describing lists of consumers who called toll-free numbers for pollen count by zip code and consumers who called to receive Thanksgiving turkey cooking tips); Evan Hendricks, Companies Exploiting Internet's Ability to Track Consumer Habits, Privacy Times, July 3, 1995, at 3, 4 (describing company which runs "Free Offer Outlet" on computer services and not only harvests names, addresses, and phone numbers of people who accept free offers but also provides information to sponsors for market research and follow-up; harvesting from one computer service alone said to generate over 300,000 leads in four months); Evan Hendricks, Rising Traffic in Prescription Info Causes Backlash in D.C., Privacy Times, Feb. 20, 1998, at 1 (indicating that drug companies capture phone numbers from consumers calling toll-free numbers for various medications); O'Harrow, A Hidden Toll, supra note 2 ("In one recent campaign, Merck & Co. worked with football coach Dan Reeves to promote a booklet about heart disease. When individuals call to get the booklet, they are asked their names, addresses and a series of questions about age, health history, insurance coverage, and smoking and exercise habits—all of which go into a database.").

10. Tye, supra note 2.
Finally, in what is sometimes called "spyware," when consumers buy and install certain computer programs—such as children's educational programs or financial planning software—the programs automatically forward to manufacturers, via the Internet, information about the consumers, such as details of Web-surfing habits or identifying personal information.\(^{11}\)

The number of such lists—that is, lists of people with particular characteristics or purchasing histories—is staggering. A leading trade group, the Direct Marketing Association, has estimated that more than 15,000 lists of consumers exist.\(^{12}\) The lists available include those based on ethnicity, political views, and sexual orientation.\(^{13}\)

Other businesses combine information obtained from various sources to create profiles of consumers, which can then be used to predict purchasing behavior and assist marketers in deciding which consumers to target with particular offers.\(^{14}\) Information about the average American is said to appear in 25 to 100 databases at any given moment and to move from one computer to another five times every business day.\(^{15}\)


12. Squires, supra note 2.

13. U.S. Dep't of Commerce, Privacy and the NII, supra note 3, at A3 ("'Arabs, In Their Native Lands, Who Gamble and Invest'; 'Doctors Who Are Known to Have Gambled'; and 'Jewish Philanthropists and Investors.'"); Reidenberg, Setting Standards, supra note 1, at 519-20, 523 (political conservatives and liberals); Headden, supra note 2, at 42 (sexual orientation and ethnicity); Smith, supra note 2 (Hispanic New Movers File); Tye, supra note 2 (Italian lineage, Japanese lineage, Jewish lineage); Zahn & Knoche, supra note 2 (subscribers to gay and lesbian magazines; Jewish households).

14. See generally Roger Clarke, Profiling: A Hidden Challenge to the Regulation of Data Surveillance, 4 J.L. & Info. Sci. 403 (1993) (defining and describing profiling and its social implications). One news story offers several examples of consumer profiles: Vacuumed into huge databases around the country is information about how many times you went out to eat last month, about whether your dog prefers Alpo to Purina . . . . Details like these are sorted, digested and compiled so that computers can plop you into neatly defined categories to help determine the likelihood that you'll pay your Visa bill on time or buy a new brand of detergent or cigarettes within the next few months . . . cashing in a coupon [can put your name and address on a list because] some that arrive at your home are encoded with digits that will identify you when you trade them in.


15. See Rothfeder, supra note 9, at 17; Robert Moskowitz, Protecting Your Privacy Requires Planning, Investor's Bus. Daily, Sept. 16, 1994, at 1; Shapiro, supra note 2, at 12.
Many are not troubled by the trafficking in personal information. Noted privacy commentator Alan F. Westin, after presiding over numerous privacy polls, has concluded that about a fifth of the public is not concerned with privacy. But others have reacted with dismay. Westin believes that about a quarter of the public is deeply concerned about privacy issues; the remainder—making up slightly more than half of consumers—are more pragmatic, with shifting views depending on various considerations.

Those seeking to block certain information practices have identified a number of rationales. Some privacy advocates have discussed

16. Westin calls these people "Privacy Unconcerned." Alan F. Westin, "Whatever Works" The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues, in U.S. Dep't of Commerce, Privacy and Self-Regulation in the Information Age (1997), available at http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F [hereinafter Westin, Whatever Works]. Polling data amply support Westin's view that some consumers are not concerned about informational privacy, though the precise size of that group may be harder to determine. For example, a 1996 survey found that 27% of the public was not at all concerned about having their name on mailing lists while 23% was slightly concerned. Beth Negus, You're Not Welcome: Direct Survey has Alarming Findings About "Junk" Views and Data Protection, Direct, June 15, 1996, at 1, 60. The same survey found that half of all consumers like to get mailings on products and services of interest to them. Id. at 61. Another 1996 poll found that 43% of respondents say that though they rarely use mail offers, they do not see them as a problem, while 12% view mail offers as a useful opportunity. Louis Harris & Assocs., Inc., 1996 Equifax/Harris Consumer Privacy Survey 72 [hereinafter 1996 Equifax/Harris Consumer Privacy Survey]. The Executive Summary of the 1996 report is available online at http://www.equifax.com/consumer/parchive/svry96/docs/summary.html (last visited July 28, 1998). In 1991, 46% of respondents saw mail offers as a nuisance. 38% rarely used them but did not see a problem, and 6% regarded mail offers as useful. Harris-Equifax Consumer Privacy Survey 1991 16-17 [hereinafter 1991 Harris-Equifax Consumer Privacy Survey]. A 1990 Equifax poll found that 16% of the respondents did not view the sharing of information by companies as a problem. Alan F. Westin, Louis Harris & Assocs., The Equifax Report on Consumers in the Information Age 18 (1990) [hereinafter 1990 Equifax Report].

17. Westin calls this group "Privacy Fundamentalists" and describes them as tending to reject the notion that organizations are entitled to obtain personal information. Westin, Whatever Works, supra note 16. Polls confirm that some consumers are indeed privacy fundamentalists. Thus, the 1996 Direct survey also found that half the public is somewhat or greatly concerned about having their name on mailing lists and that about half do not wish to receive any mail solicitations at all. Negus, supra note 16, at 61. Similarly, 37% of the respondents to the 1996 Equifax poll primarily considered mail offers as a nuisance, while 39% of those responding to the 1990 Equifax survey believed the sharing of information by companies in the same industry to be a major problem and 43% called it a minor problem. See 1996 Equifax/Harris Consumer Privacy Survey, supra note 16, at 74; 1990 Equifax Report, supra note 16, at 18.

18. Westin labeled this group "Privacy Pragmatists." Westin, Whatever Works, supra note 16. Westin believes that the views of Privacy Pragmatists shift according to whether they trust the particular industry, the value to themselves and society of the particular program calling for the information, whether the information is relevant for the purpose sought, and what safeguards have been instituted to protect the information. Id. For additional discussion of different views of privacy elicited by various surveys, see Sovern, Opting In, Opting Out, supra note 7.
fairness considerations,\textsuperscript{19} sometimes citing a number of documents adopted by various governmental or quasi-governmental entities calling for widely-accepted fairness practices.\textsuperscript{20} Though these fairness practices are articulated in different ways, the FTC offers a typical formulation:

(1) \textit{Notice} – data collectors must disclose their information practices before collecting personal information from consumers;

(2) \textit{Choice} – consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided;

(3) \textit{Access} – consumers should be able to view and contest the accuracy and completeness of data collected about them; and

(4) \textit{Security} – data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.\textsuperscript{21}

Some of these fairness practices have been adopted by trade organizations.\textsuperscript{22}


Others seeking privacy protections have relied on economic justifications. Before the United States and the European Union reached an accord on the treatment of consumer privacy, these commentators argued that the United States was not in compliance with the European Directive on Privacy. They claimed that failure to comply with that directive would affect the ability of transnational businesses to forward information to their United States operations, which would impair the functioning of certain American businesses.


Finally, I have argued elsewhere that the current system both permits information-gatherers to inflate consumer transaction costs in preventing the use of personal information, and gives businesses an incentive to do so. This practice frustrates consumers who wish to protect their privacy.

What do these critics of current information practices seek? Many have suggested that existing laws should be interpreted to prevent companies from engaging in certain information practices, or that the law should be changed. In the remainder of this article, I discuss legal restraints on the commercial use of consumer information.

II. REGULATION OF THE TRADE IN PERSONAL INFORMATION

Legal restraints on the commercial use of private information could derive from four potential sources: the common law invasion of privacy torts; the FTC acting pursuant to its authority under the FTC Act; existing state deceptive trade practices statutes; or new state or Federal legislation. Of these, legislation—or something like it, perhaps in the form of an FTC trade regulation rule—seems the best choice, for a number of reasons.

A. Statutes

One reason to prefer legislation to case law in formulating privacy regulations is that case law decisions are generally retroactive in application. Hence, if a court were to impose liability on the seller of a mailing list, for example, the court would expose thousands of mailing list sellers to liability to millions of consumers for sales that have already occurred and that took place at a time when such sales were not known to be prohibited. That outcome seems unfair and unnecessary. If the trade of personal information is to be regulated, it ought to be done in a way that allows list-sellers fair warning of their exposure to liability. Legislation provides such prospective application.

A second reason why legislation seems preferable to case law in this arena is rooted in one of the most important justifications for regulation of the trade in personal information: regulation seems the best way to accommodate the conflicting preferences of consumers. Public opinion surveys have consistently and overwhelmingly demonstrated that on many privacy issues consumer preferences are

---

25. Sovern, Opting In, Opting Out, supra note 7, at 1045-51.
26. See infra note 54 and accompanying text.
Accordingly, I have argued elsewhere for rules that permit different consumers to act in accordance with their different preferences. Generally, the legislature, a political body, seems better suited than the courts both to mediate among society's desires and enact a mechanism to balance those desires. To be sure, legislatures are subject to lobbying by special interests—which undoubtedly include those who profit from the sale of information—and so are sometimes paralyzed. But that consequence is one of the prices we pay for having a democracy, and it would seem strange to accomplish the will of the majority not through the democratically-elected legislature but through undemocratically-selected judges.

Congress has, in fact, acted on occasion to protect privacy, though in very limited ways. It has barred the sale of such things as the names of videotapes an individual has rented and the movies the individual has viewed on a pay-per-view basis from the cable provider. The Telephone Consumer Protection Act of 1991, Telemarketing and Consumer Fraud and Abuse Prevention Act, and the FTC's Telemarketing Sales Rules, all require that telemarketers allow consumers to put their names on "Do Not Call" lists. A person can

29. See supra notes 16-18 and accompanying text; see also Sovern, Opting In, Opting Out, supra note 7, at 1033.
30. See Sovern, Opting In, Opting Out, supra note 7, at 1094.
31. Cf. Benjamin Cardozo, The Nature of the Judicial Process 60-61 (1921) ("Judges do not feel the same need of putting the imprimatur of law upon customs of recent growth, knocking for entrance into the legal system, and viewed askance because of some novel aspect of form or feature, as they would if legislatures were not in frequent session, capable of establishing a title that will be unimpeached and unimpeachable.").
32. Fenrich, supra note 1, at 978-82; see also Graham, supra note 1, at 1423-25 (arguing that courts are better suited than legislatures for making privacy rules because across-the-board legislative remedies are "inadequate to deal with the fluid nature of the information economy," whereas judicial remedies are more flexible).
37. One report claims that in 1996, consumers recovered more than $54,000 from companies that did not maintain "Do Not Call" lists and still made telemarketing calls. See Garfinkel, Database Nation, supra note 2, at 175; see also Stephanie Gallagher, Telemarketers, Buzz Off!, Kiplinger's Pers. Fin. Mag., Apr. 1999, at 62 (noting that one consumer recovered $8,000 from companies calling in violation of the Telephone Consumer Protection Act, and in 1998 members of Private Citizen collected $76,000 for violations). A number of states also have enacted "Do Not Call" list legislation. See Fla. Stat. Ann. § 501.059(3) (West 1997) (consumers can have name placed on state-maintained "Do Not Call" list for $10 charge); Ga. Code Ann. § 46-5-27(d)(1) (Supp. 2000) (consumers can put name on "Do Not Call" list maintained by Public Service Commission); 815 Ill. Comp. Stat. Ann. 413/15(b)(3)
have his or her name removed from certain mailing lists by notifying the Postmaster General.38

Similarly, when Congress amended the Fair Credit Reporting Act in 1996, it created an opt-out system—allowing firms to sell information about consumers unless consumers object—for a process called pre-screening where ultimately, consumers' information is sold provided they meet certain qualifications.39 By contrast, Congress has required states to refrain from selling consumer motor vehicle data for the purpose of soliciting consumers unless consumers affirmatively permit the sale—an opt-in system.40 In 1998, Congress acted to protect children's privacy online.41 Most recently, Congress required financial institutions wishing to share certain consumer information with nonaffiliated third parties to notify consumers clearly and conspicuously of their right to opt out of that disclosure.42 In sum,


39. 15 U.S.C. § 1681 (Supp. IV 1998). The 1996 amendments took effect in 1997. When companies use pre-screening, they ask credit bureaus to furnish them with the names and addresses of consumers who meet certain criteria so that the companies can solicit such consumers to obtain, for example, credit cards. The statute forbids consumer reporting agencies to use information about consumers who object to the pre-screening process. 15 U.S.C. § 1681b(e); see also Mass. Ann. Laws ch. 93, § 51A (Law. Co-op. 2000) (allowing removal from pre-screening lists). The federal law also requires consumer reporting agencies to establish a notification system for consumers to opt-out. 15 U.S.C. § 1681b(e)(5). Consumer reporting agencies must maintain toll-free telephone numbers for consumers to express their preferences and advertise the availability of the opt-out system. Id. Those who obtain the names and addresses of consumers through pre-screening must notify the consumers whom they solicit of the consumer's right to opt out. 15 U.S.C. § 1681m(d)(1)(D), (E).

The Fair Credit Reporting Act ("FCRA") generally governs the use of consumer reports. The FTC has held that the FCRA applies to certain marketing lists created from certain consumer credit data compiled by a credit bureau, regarding the data in such cases as "consumer reports" within the meaning of the statute. See 15 U.S.C. § 1681a(d); In re Trans Union Corp., No. 9255, available at http://www.ftc.gov/os/2000/transunionfinord.htm (Feb. 10, 2000). Trans Union has indicated that it intends to file a petition for review of the FTC's Order with the Court of Appeals. However, many marketing lists do not contain credit information and are not based on information compiled by a credit bureau.


42. See 15 U.S.C.A. § 6802 (West Supp. 2000). The statute has been implemented
Congress has protected consumer privacy in certain sectors of the economy but has left consumer privacy in other sectors completely unprotected by federal regulation.  

Some states have also passed privacy statutes. For example, in certain limited circumstances, Virginia prohibits merchants from selling information gathered "solely as the result of any customer payment by... credit card" unless the merchant gives notice to the consumer. California requires credit card issuers that sell consumer information to notify the cardholder and offer the cardholder the opportunity to opt out. Some states also maintain their own "Do Not Call" lists.


44. For a discussion of the merits of national rather than state-by-state privacy regulation, see Lauretta E. Murdock, Comment, The Use and Abuse of Computerized Information: Striking a Balance Between Personal Privacy Interests and Organizational Information Needs, 44 Alb. L. Rev. 589, 610-13 (1980). See also Fenrich, supra note 1, at 986-89 (discussing information politics at the state level).

45. Va. Code Ann. § 59.1-442 (Michie 1998). The statute bars merchants, meaning those “engaged in the sale of goods from a fixed retail location in Virginia,” from selling “to any third person information which concerns the purchaser and which is gathered in connection with the sale, rental or exchange of tangible personal property to the purchaser at the merchant’s place of business.” Id. The merchant may give that notice “by the posting of a sign or any other reasonable method.” Id. Merchants who give the requisite notice still may not sell consumer information about any consumer who objects to the sale. The statute has several limitations. First, it does not apply to services. Second, it is limited to merchants with a retail outlet in Virginia. Third, it is not clear whether the statute extends to mail-order sales or sales made over the telephone—are such sales made to the purchaser at the merchant’s place of business? Virginia’s Governor’s Commission on Information Technology has also suggested criminalizing a number of practices associated with the sending of unsolicited commercial e-mail (“UCE”), including falsification of e-mail header information in UCE and subscribing to an internet service provider for the purpose of harvesting e-mail addresses for UCE. See The Governor’s Comm’n on Info. Tech., A Legislative Framework For The Virginia Internet Policy Act 13, 26 (Dec. 2, 1998), available at http://www.sotech.state.va.us/intpol.com.htm.

46. Cal. Civ. Code § 1748.12(b) (West 1998). The card issuer must either provide cardholders with a preprinted opt-out form or maintain a toll-free telephone number for that purpose. Id. The statute does not apply to information furnished to credit reporting agencies by the card issuer. Id. § 1748.12(e)(2).

California’s Constitution describes the right to privacy as an inalienable right. Cal. Const. art. I, § 1 (“All people are by nature free and independent and have inalienable rights. Among these are ... privacy.”). California has interpreted its constitutional right to privacy as conferring a cause of action not only against
Other states have regulated unsolicited commercial e-mail, often called spam. Some states require that unsolicited e-mail advertisements inform recipients how to bar additional e-mail advertisements from the sender. A number of states bar the knowing transmission of unsolicited commercial e-mail if the header information—the source and subject line of the message—contains misleading information about the source or subject of the message.

governmental entities, but also against private entities that invade one’s privacy. See, e.g., Hill v. NCAA, 865 P.2d 633, 644 (Cal. 1994). See generally Maureen S. Dorney, Privacy and the Internet, 19 Hastings Comm. & Ent. L.J. 635, 649 (1997) (“[T]he objective of [California’s constitutional] privacy right is to protect against . . . ‘the overbroad collection and retention of unnecessary personal information by government and business interests . . . [and] the improper use of information properly obtained for a specific purpose.’” (citing White v. Davis, 533 P.2d 222, 234 (Cal. 1975)).

47. See supra note 37.
48. See generally Derek D. Simmons, Comment, No Seconds on Spam: A Legislative Prescription to Harness Unsolicited Commercial E-Mail, 3 J. Small & Emerging Bus. L. 389 (1999) (reviewing various state and federal efforts to control spam and culling elements from them to propose more effective federal legislation).

A San Francisco Superior Court ruled the California statute unconstitutional in an as yet unpublished decision, Ferguson v. Friendfinder. The decision is discussed in Evan Hansen, Court Kills Key Parts of Bulk E-mail Law, at http://news.cnet.com/news//0-1005-200-2047482.html (June 9, 2000).

Some have even made sending spam a criminal act in certain circumstances, while Tennessee and California require the subject headings of spam to begin with the letters “ADV:” or “ADV: ADLT” depending on the nature of the items offered.

Nevertheless, Congress and the state legislatures have generally resisted calls for legislation on informational privacy issues, forcing privacy advocates to look elsewhere for sources of regulation. Many have explored the common law privacy torts, and the next section now discusses those briefly.

B. Common Law Privacy Torts

In discussing the common law privacy torts, Prosser’s classic taxonomy remains a useful starting point. According to Prosser, the four actionable types of invasion of privacy are: placement of someone in a false light; public disclosure of private facts; intrusion upon a person’s seclusion or solitude; and appropriation of a person’s name or likeness.

Though some have urged that these common law privacy torts could or should be stretched to cover sales of personal information,
others have disagreed, or at least expressed reservations. Because others have extensively discussed application of these torts to the information industry, I will devote little space to discussing them. I do agree that the invasion of privacy torts seem malleable enough to cover the privacy concerns discussed in this article, if a court is

\textit{supra} note 1, at 1412-13, 1427-31 (concluding that privacy torts as currently construed do not cover informational privacy but suggesting that they could be stretched to protect informational privacy, though ultimately arguing that a new tort should be created); John A. McLaughlin, Comment, \textit{Intrusions Upon Informational Seclusions in the Computer Age}, 17 J. Marshall L. Rev. 831 (1984) (arguing intrusion upon seclusion privacy tort should cover informational intrusion). For the argument that spam also constitutes a trespass to chattel, see Anne E. Hawley, Comment, \textit{Taking Spam Out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising via Electronic Mail}, 66 UMKC L. Rev. 381, 382-95 (1997).

55. For example, Joel Reidenberg writes:

In isolation, each of [the right to privacy] torts does not provide broad restriction on the circulation and treatment of personal information. Together, however, they do suggest a somewhat more active role of law in regulating conduct between citizens in comparison to the traditional constitutional preferences regulating conduct between the state and its citizens. The combination of narrow rights still does not offer more than a small set of targeted restrictions on information flows.

Reidenberg, \textit{Setting Standards}, \textit{supra} note 1, at 505 (footnotes omitted); see also, e.g., Schwartz & Reidenberg, \textit{supra} note 1, at 329, 334 (remarking that “[s]urreptitious collections of personal information without notice or consent are not likely to be sufficiently ‘objectionable’” to amount to violation of intrusion privacy tort; public disclosure of embarrassing private facts tort “difficult to sustain” because courts usually rule that “restricted distribution of personal information to narrow groups of recipients does not qualify as public disclosure” (footnotes omitted)); Bibas, \textit{supra} note 1, at 596-97 (The invasion of privacy “torts only cover highly offensive, private matters of no legitimate public concern. Typically, data dissemination does not involve publicity as courts have defined the term, and it rarely involves highly offensive matters”(footnotes omitted)); Gandy, \textit{supra} note 19, at 126 (“tort without substance”); Gindin, \textit{supra} note 19, at 1194 (“The traditional right of privacy torts have [sic] not always been persuasive in redressing invasions of informational privacy.”); Overton & Giddings, \textit{supra} note 1, at 44 (“[N]one of the privacy torts is likely to provide relief for the unauthorized commercial sale or compilation of personal information.”); Reidenberg, \textit{Privacy in the Information Economy}, \textit{supra} note 4, at 221-27 (expressing general pessimism about whether courts will interpret the invasion of privacy torts to cover information practices of companies, but noting the possibility that courts might ban certain uses); Scott Shorr, Note, \textit{Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment}, 80 Cornell L. Rev. 1756, 1794 (1995) (“Despite the common law’s reputation for adaptability to changing social conditions, the privacy tort seems structurally incapable of securing for consumers the control over personal information that they need to prevent computer-assisted commercial privacy violations.”). Another author states:

While appropriation, false light, and intrusion may not, by definition, apply to the indiscriminate use of information compiled in private sector computers, public disclosure of private facts is a tort under which one might possibly recover for another’s abuse of personal computer information. Two elements of this tort may defeat this attempt, however. Public knowledge of the private facts must be highly objectionable, and the facts must be published.

disposed to cover them, and that may account for the differing views expressed by commentators. But court decisions considering the matter have generally declined to extend the doctrines that far. For example, in *Shibley v. Time, Inc.*\(^{56}\) the court—focusing especially on the appropriation strand of the invasion of privacy tort—rejected plaintiff's claim that selling subscription lists containing the plaintiff's name without obtaining plaintiff's permission constituted an invasion of privacy.\(^{57}\)

---


In *Perry v. Moskins Stores, Inc.*, the court found no invasion of privacy when a wife left her husband because the retailer had sent the husband and other prospective customers a postcard on which was written, in feminine handwriting, only the words “Please call Wabash 1492 and ask for Caroline.” 249 S.W.2d 812, 813-14 (Ky. 1952). The court commented, “Modern day advertising techniques have come to be accepted and are in effect a limitation on the individual's right of privacy. Such methods are not actionable so long as they are not unreasonable.” *Id.; see also* Bradshaw v. Mich. Nat'l Bank, 197 N.W.2d 531, 532 (Mich. Ct. App. 1972) (sending unsolicited credit card is not invasion of privacy).

In *McCormick v. Haley*, a surviving spouse, and the children of the decedent, sued a doctor for invasion of privacy after the doctor sent a mailing addressed to the decedent that said “A check-up will keep you smiling ... Missed You!” 307 N.E.2d 34, 35 (Ohio Ct. App. 1973). The court stated that no actionable invasion of privacy claim existed if the mailing was only negligent. *Id.* at 38. However, because two similar mailings were sent after the doctor was sued for wrongful death, if those mailings were sent intentionally for the purpose of harassment, an invasion of privacy action would lie. *Id.; cf. Polin v. Dun & Bradstreet, Inc.*, 768 F.2d 1204 (10th Cir. 1985) (finding no false light invasion of privacy when defendant sent consumers' credit report to seventeen subscribers over three years because no publicity was given to credit report).

In *Lamont v. Comm'r of Motor Vehicles*, the plaintiff sued the state for selling motor vehicle registration information and sued the private company that compiled and re-sold information for violating his constitutional right to privacy. 269 F. Supp. 880 (S.D.N.Y. 1967), *aff'd*, 386 F.2d 449 (2d Cir. 1967). The court dismissed the case, stating:

The short, though regular, journey from mailbox to trash can ... is an acceptable burden, at least so far as the Constitution is concerned. And the bells at the door and on the telephone, though their ring is a more imperious nuisance than the mailman's tidings, accomplish more peripheral assaults than the blare of an inescapable radio.

*Id.* at 883. The *Shibley* decision is criticized in Fenrich, *supra* note 1, at 990-91.

While the literature on informational privacy contains extensive discussion of the privacy torts, it has generally overlooked the FTC Act. The next part now turns to the FTC Act.

III. THE FEDERAL TRADE COMMISSION ACT

Though the FTC Act does not mention privacy—it prohibits unfair and deceptive trade practices\textsuperscript{58}—it could in fact offer more informational privacy protection than the privacy torts because of the extraordinary scope given its language. To understand how the FTC Act has been applied, it is first necessary to understand the role of the FTC in interpreting the FTC Act. For a variety of reasons, the FTC has considerable latitude in determining whether particular conduct violates the FTC Act.\textsuperscript{59}

---

Another plaintiff sued for invasion of privacy, intentional or reckless disregard of safety, fraud, unjust enrichment, infliction of emotional distress, breach of contract, and negligent entrustment in \textit{Dennis v. Metromail Corp.} Gindin, supra note 19, at 1191. The plaintiff had completed a survey which the defendant company then had processed by a prison inmate. The inmate later sent the plaintiff an offensive letter. The plaintiff also objected to the defendant's sale of information and the process by which the defendant obtained the information in question. \textit{Id.} Similarly, Michael Worsham completed postal forms which permit consumers to object to mail and require the Postal Service to send Prohibitor Orders to mailers. Evan Hendricks, \textit{Holy Pandering! Dynamic Duo Takes on the Junk Mailers}, Privacy Times, Sept. 6, 1995, at 3, 4. Among the marketers Worsham objected to are Wal-Mart, Macy's, and Val-Pak. \textit{Id.} at 4. Worsham reportedly claims that one of the mailers violated the order and intended to seek a Postal Service hearing. \textit{Id.} The saga of one victorious consumer began when he purchased an item at a store and observed the clerk typing his name. The consumer secured the clerk's agreement not to enter his name on a mailing list and wrote on his check that the store agreed not to send him mailings and that if the store did so the damages would equal $1,000. See Evan Hendricks, \textit{After Small Claims Win, Man Embarks on Junk Mail 'Jihad'}, Privacy Times, Jan. 19, 1996, at 5. After the store sent the consumer several mailings, the consumer won a judgment of $1,000 in Small Claims Court. \textit{Id.; see also} Cyndee Miller, \textit{Telemarketing Foes: Don't Reach Out to Us}, Marketing News, July 3, 1989 at 1 (Consumer told companies that he would charge them for telemarketing. After company continued to call, consumer went to court and won $38.97, plus court costs and payment for one month's charge for an unlisted number. Consumer has since obtained $250 from ten companies and founded Private Citizen, Inc., a company that has more than 1,000 subscribers paying $15 each per year to maintain directory of their names sent to telemarketers as people who object to telemarketing and will charge companies $100 per telemarketing call.).


A. The FTC's Role in Interpreting the FTC Act

First, Congress has delegated enormous power to the FTC in this field. The FTC Act does not define "deception," thus leaving it to the courts and the FTC to determine the meaning of that word.

Second, in addition to this broad congressional delegation of power, courts treat Commission decisions with great deference; as a result, it has fallen largely to the FTC to decide what constitutes deception. Until 1994, the FTC Act similarly did not define unfairness. And when Congress amended the FTC Act in 1994 to limit the FTC's unfairness power, it merely codified the standards for unfairness previously articulated by the FTC.

Third, only the FTC itself can enforce the FTC Act. Thus, simply


61. For example, one opinion notes, [The FTC has accumulated much expertise. We are not to lightly set aside agency action based on the exercise of such accumulated expertise merely because, were we trying the matter anew, we might reach a different result. We are not to set aside the Commission's action unless it is apparent that it is unsupported by substantial evidence or is arbitrary, capricious, an abuse of discretion or otherwise not in accordance with the law.


This section is intended to codify ... the principles of the [FTC's Policy Statement]. Since the FTC's policy statement itself is based on the FTC's decided cases and rules, this section codifies existing law. The incorporation of these criteria should enable the FTC to proceed in its development of the law of unfairness with a firm grounding in the precedents decided under this authority, and consistent with the approach of the FTC and the courts in the past.


63. Among the cases that have ruled that the Act may not be enforced through private actions are Bott v. Holiday Universal, Inc., 1976-2 Trade Cas. (CCH) ¶ 60,973,
by deciding when to proceed and when not to, the FTC can shape jurisprudence under the FTC Act.

Fourth, the Commission also possesses the quasi-legislative power to promulgate regulations prohibiting conduct as unfair or deceptive.\textsuperscript{4} With this power, the FTC has made a multitude of rules on disparate subjects, including such things as mail order transactions and the classic holder in due course doctrine in consumer transactions.\textsuperscript{6} In short, the FTC enjoys such broad discretion in defining deceptive and unfair conduct that if the FTC could produce colorable arguments that the information practices discussed in this article violate the FTC Act, it is very likely that courts would sustain that judgment.

The FTC has taken the position that the FTC Act regulates the collection of personal information in two circumstances: first, when affirmative misrepresentations are made in the collection of information,\textsuperscript{6} and second, in some circumstances when information is collected from children online.\textsuperscript{6}\textsuperscript{7}


\textsuperscript{7} Thus, in 1998, the Commission reached an agreement with GeoCities, a popular site on the internet. The agreement was confirmed in a consent order entered in 1999. \textit{In re GeoCities, Inc.,}\textsuperscript{99} No. C-3850, \textat http://www.ftc.gov/os/1999/9902/9823015.do.htm (Feb. 5, 1999). The FTC charged GeoCities with, among other things, selling information to third parties that GeoCities stated it would not disclose to outsiders without permission. The consent order prohibited GeoCities from making certain misrepresentations. It also contained certain terms, described by the Commission as “fencing in provisions,” which require GeoCities to post a clear notice on its web site explaining its information practices, including what information is being collected, its intended uses, how the consumer can obtain access to the information, and how the consumer can have the information deleted. The complaint, an analysis of the proposed order, and other documents can be found at http://www.ftc.gov/os/1998/9808 (last visited Sept. 24, 1998).

In another action which ended in a consent order, \textit{In re Liberty Financial Co.,}\textsuperscript{99} No. 982-3522, \textat http://www.ftc.gov/os/1999/9905/lbrtycmp (May 6, 1999), the FTC charged
the company with, among other things, representing that information collected from children would be "totally anonymous" when in fact the information was maintained in a database in an identifiable form. Ultimately, the company agreed to a consent order in which it did not admit wrongdoing. The complaint, an analysis of the proposed order, and other documents can be found at http://www.ftc.gov/os/1999/9905 (last visited Jan. 16, 2001).

In FTC v. Toysmart.com, LLC, the FTC filed a complaint against Toysmart.com in Massachusetts federal district court seeking to enjoin the company, which had promised on its web site not to disclose personal information to third parties, from selling customer lists after the company solicited bids for its customer lists. First Amended Complaint For Permanent Injunction and Other Equitable Relief, at http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm (last visited Nov. 16, 2000) [hereinafter Amended Complaint, FTC v. Toysmart.com]. The FTC and Toysmart.com reached an agreement under which the company could sell its customer lists only to a business that purchased the company's entire web site and that agreed to be the company's successor-in-interest as to the customer information. See Judge: No One Wants to Play with To'ysmart's List, CNETNews.com, at http://news.cnet.com/news/0-1007-200-2549755.html (Aug. 17, 2000). The judge, however, declined to approve the agreement because no buyer for the information had surfaced. She left open the possibility that the agreement would be approved when a buyer appears. Id. The original Toysmart.com complaint is available at http://www.ftc.gov/os/2000/07/toysmartcmp.htm (last visited July 11, 2000). A press release announcing the agreement, and accompanying documents, including an amended complaint, the agreement, a dissenting statement by Commissioner Swindle, and separate statements by Commissioners Anthony and Thompson, appear at http://www.ftc.gov/opa/2000/07/toysmart2.htm (last visited Dec. 4, 2000). See also Stipulated Order for Permanent Injunction, FTC v. Rennert, No. 992-3245, at http://www.ftc.gov/os/2000/07/toysmart.htm (July 12, 2000) (FTC filed suit and reached agreement with online pharmacies that promised that information supplied to pharmacies would be used solely to supply customers with requested products; services later used information to send its customers unsolicited commercial e-mail). The complaint, final orders, statements by some of the Commissioners, and a press release can be found at http://www.ftc.gov/opa/2000/07/ftcout.htm (last visited July 19, 2000). Cf. In re Equifax, 96 F.T.C. 844 (1980), order set aside in part on other grounds, 678 F.2d 1047 (11th Cir. 1982) (stating that it is deceptive for information collectors to misrepresent who their employers are; it is also deceptive to represent inaccurately that medical information would be released only to insurance companies); FTC, Public Workshop on Consumer Information Privacy, Session Three: Consumer Online Privacy 15 (June 12, 1997), available at http://www.ftc.gov/bcp/privacy/wkshp97/index.html (remarks of Commissioner Varney and David Medine, Associate Director for Credit Practices, agreeing that e-mails containing inaccurate removal instructions may be within FTC's existing fraud or deception authority).

Though consent orders are less authoritative than opinions that were the products of litigation, FTC consent orders are still more authoritative than conventional settlements. When the FTC issues a complaint, the Commission determines that the complained-of practice, if proven, violates one of the laws it is charged with enforcing. See Jonathan Sheldon & Carolyn L. Carter, Unfair and Deceptive Acts and Practices § 3.4.5.3, at 133 (4th ed. 1997); Jeff Sovern, Good Will Adjustment Games: An Economic and Legal Analysis of Secret Warranty Regulation, 60 Mo. L. Rev. 323, 375 (1995) [hereinafter Sovern, Good Will]; see also FTC v. Mandel Bros., 359 U.S. 385, 391 (1959) ("[FTC interpretation of statute] entitled to great weight ... even though it was applied in cases settled by consent rather than in litigation."); People ex rel. Hartigan v. Maclean Hunter Publ'g Corp., 457 N.E.2d 480, 487 n.1 (Ill. App. Ct. 1983) ("[C]onsent orders are not authoritative as adjudications, but they are not without precedential value."). For example, the FTC's order in GeoCities notes that the Commission has "determined that it had reason to believe that the respondent has
Writing in the context of online privacy, the Commission has repeatedly said "[a]s a general matter, however, the Commission lacks authority to require firms to adopt information practice policies or to abide by the fair information practice principles on their Web sites, or portions of their Web sites, not directed to children." At least one violated the [FTC Act]." In re Geocities, Inc., No. C-3850, (Feb. 5, 1999), at http://www.ftc.gov/os/1999/9902/9823015.do.htm.

(a) It is a deceptive practice to represent that a site is collecting personal identifying information from a child for a particular purpose (e.g. to earn points to redeem a premium), when the information will also be used for another purpose that parents would find material, in the absence of a clear and prominent disclosure to that effect; and
(b) It is likely to be an unfair practice to collect personal identifying information, such as a name, e-mail address, home address, or phone number, from children and to sell or otherwise disclose such identifying information to third parties, or to post it publicly online, without providing parents with adequate notice and an opportunity to control the collection and use of the information through prior parental consent.

Id. The Report also states that:
To assure that notice and choice are effective, a Web Site should provide adequate notice to a parent that the site wishes to collect personal identifying information from the child, and give the parent an opportunity to control the collection and use of that information. Further, according to the staff opinion letter, in cases where the information may be released to third parties or the general public, the site should obtain the parent's actual or verifiable consent to its collection.
The content of the notice should... take into account the fact that online activities may be unique and unfamiliar to parents. Thus, a notice should be sufficiently detailed to tell parents clearly the type(s) of information the Web site collects from children and the steps parents can take to control the collection and use of their child's personal information.

Id. (footnotes omitted). The FTC's position on children's privacy in the 1998 report was foreshadowed by a 1997 staff letter that opined:
It is a deceptive practice to represent that a Web site is collecting personally identifiable information from a child for a particular purpose... when the information will also be used for another purpose which parents would find material, in the absence of a clear and prominent disclosure to that effect... We believe that it would likely be an unfair practice in violation of Section 5 to collect personally identifiable information... from children and sell or otherwise disclose such identifiable information to third parties without providing parents with adequate notice... and an opportunity to control the collection and use of the information.


68. Privacy Online 2000, supra note 21, at 34; see also Privacy Online 1998, supra note 3, at 41. Chief Commissioner Pitofsky gave testimony before the Senate:

[Senator] WYDEN: Do you believe that you have existing rulemaking
recent case, *FTC v. ReverseAuction.Com, Inc.*,\(^69\) raises questions, however, about whether the FTC can be persuaded to go beyond these limits in some circumstances, though the Commission seems unprepared to acknowledge that. Indeed, recently the FTC has concluded that some regulation of online privacy is needed, but that Congress, not the Commission, should be the source of that regulation.\(^70\)

In fact, colorable arguments can be made that the trafficking in personal information—whether online or offline—about adults

authority under your underlying statute, the organic statute, to protect consumer privacy?

[Chief Commissioner] PITOFSKY: No. No, we do not; that's the point. It seems to me we need the kind of legislation that we've recommended and then you and Senator Burns have offered in order to engage in rulemaking. We could call invasions of privacy unfair, but I do not believe that we could sustain that position.

*Internet Privacy Hearing Before the Sen. Commerce Comm.,* 107th Cong. 31 (2000), available at 2000 WL 699924. Chairman Pitofsky also gave testimony concerning scope of the FTC's power before a House Subcommittee:

Currently, the Commission has limited authority to prevent abusive practices in this area. The [FTC Act] grants the Commission authority to seek relief for violations of the Act's prohibitions on unfair and deceptive practices in and affecting commerce, an authority limited in this context to ensuring that Web sites follow their stated information practices.

Statement of the FTC on "Consumer Privacy on the World Wide Web" Before the Subcomm. on Telecommunications, Trade and Consumer Protection of the House Comm. on Commerce, 105th Cong. n.23 (July 21, 1998), available at http://www.ftc.gov/os/9807/privac98.htm; see also Roscoe B. Starek, III & Lynda M. Rozell, *The Federal Trade Commission's Commitment to On-Line Consumer Protection*, 15 J. Marshall J. Computer & Info. L. 679, 697 (1997) (stating in an article co-authored by FTC Commissioner, "There are no plans for the Commission to issue privacy guidelines or regulations. Instead... the Commission is looking first to businesses to address privacy issues through voluntary measures... "); BNA Special Report, *Privacy Rights Advocates Urge FTC to Regulate Marketing Directed to Kids*, 72 Antitrust & Trade Reg. Rep. (BNA) 600, 600 (1997) (quoting FTC Commissioner Roscoe B. Starek, III, on privacy, that "[w]e cannot and should not dictate the forms of your self-regulation or attempt to regulate by threat of commission action in areas where we lack authority"). When the FTC approved the order in *GeoCities*, see *supra* note 66, Commissioner Orson Swindle wrote a concurring statement in which he stated that he had voted in favor of final issuance of the consent order in this matter because its provisions are appropriate to remedy the alleged violations of the law by GeoCities, Inc. However, I want to emphasize that my support for these provisions as a remedy for alleged law violations in this particular case does not necessarily mean that I would support imposing these requirements on other commercial Internet sites through either legislation or regulation.


without their knowledge, and perhaps even consent, already violates the FTC Act’s prohibition on unfair and deceptive trade practices.\textsuperscript{71} Whether it would be desirable for the FTC to take that position, is, of course, another question. The following sections turn to these issues. Subpart B will first discuss generally the FTC’s power under the unfairness prong of the FTC Act. Subpart C then turns to the FTC’s power to bar deceptive practices, and Subpart D addresses FTC cases dealing with privacy.

B. Unfairness

The word “unfair” is so vague—and so common in legal arguments—that it may be more helpful to start by identifying the goals of the FTC’s unfairness doctrine. One thoughtful observer of the FTC, Michael M. Greenfield, has identified two such goals, one of which is particularly applicable to sales of personal information. Greenfield has written:

One is the effectuation of clearly established public policy . . . . The other, more prominent, concern is the maintenance of a properly functioning free market. Hence, the Commission intervenes when sellers or creditors create impediments to the operation of a competitive market or when they take advantage of impediments that exist independently of their efforts.

Critical to the operation of a free market is the ability of the consumer, based on complete information, to choose freely whether or not to enter a transaction with a seller or creditor. The Commission has stated the essential characteristics of a free market to be competition, availability of information, lack of excessive

\textsuperscript{71} One former FTC Commissioner suggested while still in office that the FTC’s existing authority reaches this far, at least insofar as the internet is concerned, though the remarks came in a context that raises doubt about whether they reflect a considered opinion. See FTC, Public Workshop on Consumer Information Privacy, Session Two: Consumer Online Privacy 159 (June 11, 1997), available at http://www.ftc.gov/bcp/privacy/wkshp97/volume2.pdf.

Janlori Goldman (Visiting Scholar, Georgetown University Law Center): But for those bad actors; they are not saying anything about what their information practices are, they are not giving any kind of notice, and so it seems to me that either the FTC’s jurisdiction and authority should be expanded, not just to look at people who are making misrepresentations but who are acting in a way which would be considered to be unfair.

Commissioner Varney: Our jurisdiction may not need to be expanded to do that. We do have authority in unfairness.

\textit{Id.}; cf. \textit{id.}, Session Four: Database Study 87-88 (June 13, 1997) (quoting remarks of Commissioner Varney: “I think we all agree that if a site says it’s collecting information for one purpose and is using it for a different purpose, that is either fraudulent, deceptive or unfair. I don’t think you have got any disagreement about that.”).
transaction costs, lack of costs and benefits external to the decision process, and mobility of resources.72

For many consumers, the free market has not functioned to give them a choice as to whether their personal information will be sold. Many consumers remain unaware that a trade in their personal information exists.73 Of those consumers who do know about the trade in personal information, many do not know that they can opt out of that trade.74 Lastly, even those aware both of the trade and the

72. Michael M. Greenfield, Consumer Law 95 (1995) (footnotes omitted); see also Averitt, supra note 60, at 248 (“[T]his analysis would ask whether the consumer problems at issue were caused by a market failure, so that government intervention should replace the usual reliance on market forces as a corrective.”).

73. See Privacy Rights Clearinghouse, First Annual Report (1994), available at http://www.privacyrights.org/AR/annrep1.html (“Most [consumers] are unaware of the ways in which personal information is . . . used and distributed . . . .”); H. Jeff Smith, Managing Privacy 4 (1994) (“[C]onsumers tend to be quite uninformed regarding the actual [privacy] policies and practices of industries with which they deal regularly.”); Frank V. Cespedes & H. Jeff Smith, Database Marketing: New Rules for Policy and Practice, Sloan Mgmt. Rev., Summer 1993, at 7, 8 (“Our interviews with consumers . . . suggest that they are still largely unaware of how information about them is gathered and used . . . .”); Schwartz, supra note 8, at 1683 (noting that “individuals are likely to know little or nothing about the circumstances under which their personal data are captured, sold, or processed” on the internet); Simson L. Garfinkel, How Computers Help Target Buyers, Businesses Screen and Identify Potential Customers with Information from Credit-Bureau Databases, Christian Sci. Monitor, July 25, 1990, at 13 (quoting Bonnie Guiton, Special Adviser for Consumer Affairs to President Bush, as saying “A major concern of mine is that consumers are uninformed. . . . In most cases, they don’t even know that [information on them] is being collected.”) [hereinafter Garfinkel, How Computers Help]; O’Harlow, Data Firms, supra note 14 (quoting Leslie L. Byrne, former director of the U. S. Office of Consumer Affairs as saying “most people don’t have a clue what’s being gathered about them”); Ticked Off At AmEx, USA Today, May 26, 1992, at 10A (revealing that consumer assumed personal data provided to credit card companies and other lenders was protected by a business ethics code); Westin, Whatever Works, supra note 16 (reporting on 1997 survey concerning online privacy finding “71% of respondents online were not aware of their services’ information policies . . . and that most visitors to web sites were not aware of the policies those sites followed in collecting visitors’ personal information”); cf. Gandy, supra note 19, at 107 (“Consumers generally were not aware that calls made to 800 and 900 number information services, especially to ‘976’ or other sexually oriented services, generated transaction records.”). Peter Swire has pointed out that consumer ignorance of company use of their personal information may have significant costs:

Because the company internalizes the gains from using the information, but can externalize a significant share of the losses, it will have a systematic incentive to over-use private information. In terms of the contract approach, companies will have an incentive to use private information even where the customers would not have freely bargained for such use.


74. For example, one survey reveals:

The percentage of people who report being aware of any procedures that allow one to remove one’s name from direct mail lists for catalogs, products, and services has remained constant from 1991 to the present at 44%....
possibility of opting out experience significant—even overwhelming—
difficulties in preventing the collection and sale of data pertaining to
them.\textsuperscript{75} Elsewhere, I have argued that businesses have the capacity to
inflate transaction costs incurred by consumers in opting out, and, in
some instances at least, reason to do so.\textsuperscript{76}

Until 1980, in its attempt to translate these goals into legal
standards, the FTC used three criteria to decide if a practice was
unfair:

- (1) Whether the practice, without necessarily having been previously
  considered unlawful, offends public policy as it has been established
  by statutes, the common law, or otherwise—whether, in other
  words, it is within at least the penumbra of some common-law,
  statutory, or other established concept of unfairness;

- (2) whether it is immoral, unethical, oppressive, or unscrupulous;

\textsuperscript{75} Notably, only 29\% of those who consider mail offers an invasion of privacy
are aware of the procedures that would allow them to remove their names
from direct mail lists.

1996 Equifax/Harris Consumer Privacy Survey, \textit{supra} note 16, at 10; \textit{see also} 1991
Harris-Equifax Consumer Privacy Survey \textit{supra} note 16, at 18; Alan F. Westin, Louis
Harris & Assoc., \textit{Commerce, Communication, and Privacy Online} 23 (1997)
(indicating that 57\% of computer users aware of procedures that allow them to
remove names from direct mail lists for catalogs, products, and services, and 25\% of
online service and internet users who send or receive e-mail know of procedures for
removing their e-mail addresses from companies that send e-mail offers); Mary J.
Culnan, "\textit{How Did they Get My Name?}: An Exploratory Investigation of Consumer
Attitudes Toward Secondary Information Use, MIS Q., Sept. 1993, at 341, 357
(showing 78\% of participants unaware of procedures to allow mailing list removal);
\textit{cf.} Gerald Tolchin, \textit{Personal Privacy and Access to Information on a College Campus:}
\textit{A Preliminary Report,} 29 Psychol. J. Hum. Behav. 12, 14 (1992) (finding that about
half the students surveyed were aware of or seemed to understand certain of their
privacy rights under the Family Education Rights and Privacy Act of 1974). On the
willingness of the FTC to intervene in such circumstances Averitt states:

For \[a\ consumer's\] decision to be meaningful... it must be based on full and
accurate knowledge of the alternatives. Some sellers have undermined this
process by either withholding or failing to generate critical data about their
products, thus making it difficult or impossible for consumers to make
informed comparisons. The Commission has found these practices to be
unfair under certain circumstances.

See Averitt, \textit{supra} note 60, at 258.

75. \textit{See, e.g.,} Sovern, \textit{Opting In, Opting Out, supra} note 7, at 1074-76. Anne Wells
Branscomb comments:

\[A\]ttempting to get out of the clutches of the database managers is almost a
full-time job. I can vouch for this, because I have spent the last five years
trying to withstand the assault of direct mail marketers on the post office box
I rented to relieve the overstuffed mailbox at my home address.

Anne Wells Branscomb, \textit{Who Owns Information?} 11 (1994); \textit{see also} Privacy Rights
(illustrating an instance where consumer still received junk mail after having written
over 2,000 letters seeking deletion from mailing lists); G. Bruce Knecht, \textit{Junk-Mail
(describing a consumer who for years has requested companies to delete his name
from their mailing lists and still receives one to seven solicitation letters each day).

76. \textit{See} Sovern, \textit{Opting in, Opting Out, supra} note 7, at 1081.
(3) whether it causes substantial injury to consumers . . . 77

However, in 1980, the Commission produced a Policy Statement which recast the unfairness doctrine as a more economics-oriented approach, focusing on cost-benefit analysis.78 This Policy Statement emphasized that the most important of the three criteria was whether there had been a consumer injury. It then refined the definition of consumer injury, and Congress ultimately codified this refinement in 1994. The 1994 codification of the unfairness doctrine prohibited the FTC from barring a practice as 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.”79 I now consider each of these criteria in turn with regard to the sale of personal information.

1. Substantial Injury

Does the sale of personal information without notice to consumers amount to a substantial injury? In other areas, small injuries, widely shared, can qualify.80 The FTC has found in the past that a failure to disclose other types of information can be unfair.81 Nor does it matter


80. See S. Rep. No. 103-130, at 13 (1994), reprinted in 1994 U.S.C.C.A.N. 1776, 1788; In re Orkin Exterminating Co., 108 F.T.C. 263, 362 (1986), aff’d, 849 F.2d 1354, 1366 (11th Cir. 1988) (“We are not concerned with trivial or merely speculative harms, but an injury may be substantial if it does a small harm to a large number of people. Over $7.5 million in increased renewal revenue in an approximately four year period at the unjustified expense of consumer, is not insubstantial.” (footnotes omitted)); Averitt, supra note 60, at 246.

81. See, e.g., Trade Regulation Rules, 16 C.F.R. § 423 (2000) (stating that the Care Labeling Rule requires clothing to bear permanent labels on how to care for garment, such as “cold water wash only” and explained at Care Labeling of Textile Wearing Apparel, Promulgation of Trade Rule and Statement of Basis and Purpose, 36 Fed. Reg. 23,883-23,889 (1971) (“It is unduly oppressive and unfair to consumers to withhold information essential to the ordinary use of a product” because many consumers experience “substantial economic loss because of erroneous assumptions about care of clothes”)); 16 C.F.R. § 306 (2000). (explained in Posting of Minimum Octane Numbers on Gasoline Dispensing Pumps, Statement of Basis and Purpose, 36
that the information may be used after the purchase that generated
the information; post-purchase practices can still be unfair.82

Some consumers are not bothered by the trade in their personal
information;83 presumably, they have not suffered a substantial injury. But others are troubled by it—some, deeply so—and many are so
concerned that they have invested time and money in trying to stop
the use of their information.84 The sale of adults’ personal
information without notice may be less injurious than the sale of
information about children—which Congress and the FTC have

Fed. Reg. 23,871, 23,877 (1971) (stating that the rule requires posting of standardized octane ratings of gasoline to prevent confused consumers from buying more expensive gasoline with higher octane than necessary; the rule is based on both unfairness and deception power). See generally Pridgen, Consumer Protection, supra note 78, § 9.05[2] (commenting on the Care and Labeling Rule and the FTC rule
requiring the posting of octane ratings).

82. See In re Orkin Exterminating Co., 108 F.T.C. at 341-42 (ruling that it was an unfair practice for an exterminating company, contracted for lifetime pest control at particular rate, to later seek to raise rates); In re Spiegel, Inc., 86 F.T.C. 425, 437 (1975) (holding practice of mail order company of suing consumer in company’s home state rather than consumer’s home state was unfair); In re All-State Indus. of N.C., Inc., 75 F.T.C. 465, 490 (1969) (finding practice unfair when seller did not disclose to consumers that it routinely assigned consumer credit contracts to third party, thus
immunizing third party from most consumer claims and defenses and obligating consumer to pay under holder in due course doctrine even when seller did not perform).

83. See supra note 16 and accompanying text.

84. For example, many consumers pay telephone companies so that their phone
numbers and addresses will not be listed. See Eli M. Noam, Privacy and Self-
Regulation: Markets for Electronic Privacy, in U.S. Dep’t of Commerce, Privacy and
Self-Regulation in the Information Age (1997), available at http://www.ntia.doc.gov/reports/privacy/selfregl.htm (reporting that 55% of California residences have unlisted numbers while 24% of New York State residents are not listed). Some 30,000 Americans called, or wrote, to Lotus Development or
Equifax or both when the two proposed to create a product—Marketplace:
Households—which would have made the names, addresses, personal buying habits,
and income levels of many consumers more available to local businesses. Daniel
Mendel-Black & Evelyn Richards, Peering into Private Lives, Wash. Post, Jan. 20,
1991, at H1. The two companies dropped the plan after the protests. See also Evan
Hendricks, Capital Insights, Privacy Times, June 28, 1996, at 1 (discussing how Lexis-
Nexis dropped plan to make consumer Social Security numbers available to
subscribers after complaints); Evan Hendricks, Capital Insights, Privacy Times, May 2,
1996, at 1 (detailing how after receiving complaints, Database America and Yahoo!
deleted 90 million unlisted numbers from what was to be a compilation of 175 million
names and addresses); Pac Bell Backs-off Selling Lists, Alameda Times Star, Apr. 16,
1986, at 6 (showing how company reversed decision to sell customer names and
addresses after receiving more than 75,000 customer protests); Seth Schiesel, America
Online Backs Off Plan to Give Out Phone Numbers, N.Y. Times, July 25, 1997, at D1
(reporting that company abandoned plan to provide lists of phone numbers to
telemarketers and others within 24 hours after plan became widely known and
consumers complained). Many Americans claim they have decided against applying
for something, such as a job, credit, or insurance, to preserve confidentiality of their
data. The 1990 Equifax Report, supra note 16, at 13 (30%). See generally Sovern,
Opting In, Opting Out, supra note 7.
regulated—but given the concern that sale has drawn from consumers, it is difficult to argue that it does not amount to a substantial injury, at least to many consumers.

However, the legislative history of the 1994 codification offers a stumbling block in finding the injury substantial. The Senate Report explains:

In accordance with the FTC’s December 17, 1980, letter, substantial injury is not intended to encompass merely trivial or speculative harm. In most cases, substantial injury would involve monetary or economic harm or unwarranted health and safety risks. Emotional impact and more subjective types of harm alone are not intended to make an injury unfair.  

The type of injury suffered here may at first glance seem emotional and subjective. But for many it is more than that. Many consumers have spent money to protect their privacy. Even for those who have not, however, this may be the rare case in which the injury, though not monetary or health- or safety-related, is still far more than “trivial or speculative” and so FTC action is appropriate. Because the Senate Report closely tracks the 1980 Policy Statement in many respects, it is useful to look to the Policy Statement to flesh out the meaning of the phrase, substantial injury. The only example of emotional impact and other more subjective types of harm provided in the text of the 1980 Policy Statement sheds some light on the FTC’s intended meaning. The Commission wrote: “Thus, for example, the Commission will not seek to ban an advertisement merely because it offends the tastes or social beliefs of some viewers . . . .” That type of emotional impact is so different from the type experienced by consumers in the privacy context that it suggests that the Commission meant something altogether different when it wrote of emotional impact.

A footnote to the Policy Statement offers even more aid to those seeking help from the FTC under the unfairness doctrine. That footnote states: “In an extreme case, however, where tangible injury could be clearly demonstrated, emotional effects might possibly be

85. See supra note 41.
87. See supra note 84.
88. 1980 Policy Statement, supra note 78, at 6. The remainder of the paragraph also helps in interpreting the Senate Report: First of all, the injury must be substantial. The Commission is not concerned with trivial or merely speculative harms. In most cases a substantial injury involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defenses arising from the transaction. Unwarranted health and safety risks may also support a finding of unfairness. Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair.
Id. (footnotes omitted).
considered as the basis for a finding of unfairness.”

The footnote then cites, with a cf., the Fair Debt Collection Practices Act (“FDCPA”), and refers specifically to the FDCPA provision barring harassing late-night telephone calls. The note does not define “tangible injury.” Conceivably, tangible injury means that there must be some physical manifestation of the emotional effect, as was required by some older cases in which plaintiffs sought damages for intentional infliction of emotional distress. But it is more likely that tangible injury means only that it must be clear that the conduct is of a sort that causes injury, as the citation to the FDCPA suggests. Moreover, the reference to harassing late-night telephone calls seems remarkably like one of the objectionable characteristics of telemarketing, and so offers support for the argument that at least some injuries suffered by consumers at the hands of marketers fall within the FTC Act’s unfairness prong.

In sum, rather than dismissing the harm to consumers from the trade in their personal information as merely emotional or subjective, the better argument is that the injury is substantial.

2. Reasonably Avoiding the Injury

Could consumers reasonably avoid the injury? Consumers who do not even know that information about them is being used, or how it is being used, lack the opportunity to avoid the injury. While many

---

89. Id. at 6 n.16.
91. See generally W. Page Keeton, Prosser and Keeton on Torts 64 (1984) (“A few cases have said flatly that physical illness or some other nonmental damage is essential to the existence of the tort, and there are other cases which look as if it were considered indispensable. On the other hand, there are numerous decisions which have found liability for mere mental disturbance without any evidence of physical consequences.” (footnotes omitted)).
92. Under the FDCPA, courts may award statutory damages even when the consumer fails to prove actual damages. See 15 U.S.C. § 1692k(a) (1994) (allowing statutory damages up to $1,000).
93. Harassing late-night telephone calls are addressed in the FTC’s Telemarketing Rules. See 47 C.F.R. § 64.1200 (e)(1) (2000) (prohibiting telemarketing calls after 9:00 p.m.); 16 C.F.R. § 310.4 (2000) (outlining abusive telemarketing acts or practices that are barred by the Rule). Those rules do not address the trade in consumer information.

A problem with relying on the footnote to the Policy Statement is that it was not carried forward into the Senate Report, which may imply congressional rejection of the message in the note. But it probably means only that the Senate did not view the point as important enough to merit congressional attention: it was, after all, confined to a note. Given Congress’s enthusiastic adoption of much of the Policy Statement, I would hesitate to say that Congress rejected any of it, unless a clearer intent was demonstrated. See S. Rep. No. 103-130, at 12 (1994), reprinted in 1994 U.S.C.C.A.N. 1776, 1787 (“This section is intended to codify, as a statutory limitation on unfair acts or practices, the principles of the FTC’s December 17, 1980 policy statement on unfairness.”).
consumers know in some general way that the information they provide in a transaction may be used, it appears that many, if not most, do not understand just how that information will be exploited. In the 1980 Policy Statement, the Commission explained:

[I]t has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary. Most of the Commission's unfairness matters are brought under these circumstances. They are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking.

The lack of complete information, which deprives many consumers of the opportunity to reasonably avoid injury in the privacy situation, is analogous to the FTC's *In re International Harvester Co.* decision. Harvester manufactured tractors that were subject to fuel geysering, the forceful ejection of hot gasoline through a loosened gas cap. The Commission found Harvester's failure to notify consumers of this possibility unfair. In discussing whether the injury was one that consumers could reasonably avoid, the Commission wrote:

Farmers may have known that loosening the fuel cap was generally a poor practice, but they did not know from the limited disclosures made, nor could they be expected to know from prior experience, the full consequences that might follow from it. This is therefore not a situation in which the farmers themselves are primarily responsible for their own accidents.

Just as in *Harvester*, consumers' vague knowledge that some of their information is used by businesses does not permit them to avoid the injury.

Indeed, the Commission has found this prong satisfied even when consumers had in their possession a writing that indicated that their rights were being violated. In the case of *In re Orkin Exterminating Co.*, Orkin, an exterminator, offered its customers "lifetime" contracts at fixed rates. Over the years, inflation jeopardized the profitability of the arrangement, and Orkin raised its rates. When some customers objected, Orkin adopted a policy of rescinding the price rise to complaining customers if the customer could show that it had relied on Orkin's promise not to increase the fee. Orkin did not, however, offer a similar arrangement to customers who failed to

94. *See supra* note 73.
97. *Id.* at 1066.
98. *Id.*
100. *Id.* at 286-90, 367.
complain. The FTC intervened and ultimately determined that the non-complaining customers could not reasonably have mitigated the injury they suffered. In affirming, the Eleventh Circuit observed that "consumer information is central to this prong of the unfairness inquiry." If consumers could not protect themselves in the Orkin and Harvester cases, then surely consumers are in no better position to prevent the unauthorized use of their personal information.

3. Is the Injury Outweighed by Countervailing Benefits?

The third prong of the unfairness test is whether the injury is outweighed by any countervailing benefits. The FTC has also characterized this inquiry as whether the conduct is harmful "in its net effects." The issue here is not whether firms are using personal information, but rather whether the failure to disclose the possibility that information will be used causes an injury that outweighs the benefits of nondisclosure.

I have argued elsewhere that our existing system—where failures to disclose to consumers the nature of information practices are commonplace—is generally harmful in that it prevents consumers from acting consistently with their preferences and thus produces a suboptimal equilibrium. The failure to disclose makes it impossible for some consumers to protect their privacy, and there is ample reason to believe that some consumers are deeply troubled by the use of their personal information. Moreover, the benefits of nondisclosure do not seem great. Indeed it is difficult to argue that disclosure is troublesome, as even trade groups are now calling for disclosure of the uses to which the information will be put and making opt-out devices available. Hence, given that the injury is significant to some and the benefits of non-disclosure seem slight, this prong comes out in favor of disclosure.

101. Id. at 366-68.
102. Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1366 (11th Cir. 1988).
103. See also In re Amrep Corp., 102 F.T.C. 1362 (1983) (finding that buyers of land located far away from their homes could not reasonably avoid injury because they lacked information about subdivisions in question).
104. In re Int'l Harvester Co., 104 F.T.C. 949, 1061 (1984) ("In analyzing an omission this part of the unfairness analysis requires us to balance against the risks of injury the costs of notification and the costs of determining what the prevailing consumer misconceptions actually are."); see also S. Rep. No. 103-130, at 13 (1994), reprinted in 1994 U.S.C.C.A.N. 1776, 1788; cf. In re Southwest Sunsites, Inc., 105 F.T.C 7, 154 (1985) ("There can be no benefit to society from the dissemination of misrepresentations that induce consumers to continue making payments that they might very well have terminated if they had not been misinformed.").
105. See generally Sovern, Opting In, Opting Out, supra note 7.
106. See supra note 17.
107. See supra note 22 and accompanying text.
108. Richard Craswell has synthesized the FTC unfairness decisions dealing with non-disclosure as follows:
Does it matter that the offending practice is widely-practiced or represents customary business conduct? Apparently not: the FTC has intervened to bar industry-wide conduct as well as practices that had existed for decades.°

C. Deception

FTC rulings have made it more difficult to argue that undisclosed sales of personal information are deceptive than to argue that those sales are unfair. In a 1983 Policy Statement, the FTC toughened its standard of deception. The FTC now considers conduct deceptive "if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."°°°° The conduct must also qualify as

---

[T]he Commission's decisions suggest that the failure to disclose information... will be unfair if: (1) consumers currently lack the information in question; (2) consumers would choose differently if they had the information, thus facing sellers with a different set of demand curves; and (3) the benefits of better consumer decisions and improved seller performance are not outweighed by the costs of supplying the information.

Craswell, supra note 77, at 123. The undisclosed use of personal information seems to meet that standard.

109. See, e.g., Moog Indus., Inc., v. FTC, 355 U.S. 411, 413 (1958) (affirming FTC's regulatory authority to end price discrimination within industry); FTC v. Algoma Lumber Co., 291 U.S. 67, 79 (1934) (noting that although sellers called wood by botanically-incorrect name for forty years or more, the FTC still rightfully exercised its authority to prevent misbranding); In re Peacock Buick, Inc., 86 F.T.C. 1532, 1563 n.12 (1975) (rejecting defense that it was a common practice among car dealers to drop a deceptive service charge if a consumer complained).

No showing is required that the manufacturer made a false statement, or that any deception was intended, or that anyone was deceived or even injured.

Examples discussed previously, wherein a consumer's request for a free sample results in the consumer's name being sold on a list of those who are incontinent, a consumer's stay in a lodge causes the consumer to be listed as having a particular sexual orientation, or a consumer's purchase of software results in the consumer's personal information becoming available to others without the consumer's knowledge, all sound like omissions "that [are] likely to mislead the consumer acting reasonably in the circumstances." Few consumers would anticipate those particular consequences of such behavior.

Of course, much information collected from consumers that is sold is not used in such an extreme fashion. But even in other situations, unexplained use may satisfy the test for deception. As noted above, many consumers simply do not know how their personal information is used. How many consumers must be misled before their confusion can be said to be reasonable? The Commission has explained that "[a]n interpretation may be reasonable even though it is not shared by a majority of consumers in the relevant class, or by particularly sophisticated consumers. A material practice that misleads a significant minority of reasonable consumers is deceptive." It seems very likely that the information practices of many companies meet that standard.

Is the deception to the consumer's detriment? Again, while some consumers would not find it objectionable, many would. The failure to disclose here is analogous to a seller's failure to disclose that the

---

111. FTC 1983 Policy Statement, supra note 110, at 5.
112. Statements can be deceptive even though they are literally true. See, e.g., Bockenstette v. FTC, 134 F.2d 369, 371 (10th Cir. 1943) ("Words and sentences may be literally and technically true and yet be framed in such a setting as to mislead or deceive."); In re Thompson Med. Co., 104 F.T.C. 648, 788 (1984) (noting that the crucial issue was whether claims were likely to mislead reasonable consumers).
114. See Resort Car Rental Sys. v. FTC, 518 F.2d 962, 964 (9th Cir. 1975); Montgomery Ward & Co., Inc., v. FTC, 379 F.2d 666, 670 (7th Cir. 1967); Charles of the Ritz Distrib. Corp. v. FTC, 143 F.2d 676, 680 (2d Cir. 1944).
115. See FTC v. Raladam Co., 316 U.S. 149, 152 (1942); Sterling Drug Inc., 317 F.2d at 674.
116. See supra note 9 and accompanying text.
117. See supra note 10 and accompanying text.
118. See supra note 11 and accompanying text.
120. See supra note 73.
consumer's promissory note or contract might be sold in the regular course of business—and the FTC has ruled that deceptive.\textsuperscript{122}

Whether the FTC would view the conduct as deceptive is likely to depend on whether the failure to disclose the manner in which the consumer's information is being used is seen as a half-truth or a "pure omission." While the Commission offers only slight protection against deceptive "pure omissions," the FTC has ruled many times that half-truths fall afoul of the FTC Act.\textsuperscript{123} An example: the FTC acted to bar Kraft from advertising—truthfully—that each slice of its cheese was made from five ounces of milk, when the ads did not disclose that thirty percent of the calcium in the milk was lost during processing.\textsuperscript{124} The ads had also pointed out—again, truthfully—the value of calcium in building bones.\textsuperscript{125} Though it is a bit of a stretch, the Commission could, if it wanted to, see as a half-truth a seller's description of the offer as an exchange of a product for money rather than an exchange of a product for money plus information.\textsuperscript{126}

The FTC formerly viewed a merchant's failure to correct a consumer's normal, but erroneous expectations about a product as deceptive, even in situations in which the seller had not spoken—the so-called "pure omission."\textsuperscript{127} For example, the FTC has taken the position that a seller acted deceptively when the seller sold 1970 model year cars in that model year or the following year at nearly full price without disclosing that the cars were used, given that consumers

\textsuperscript{122} All-State Indus. of N.C., Inc., v. FTC, 423 F.2d 423, 425 (4th Cir. 1970).

\textsuperscript{123} See, e.g., In re Int'l Harvester Co., 104 F.T.C. 949, 1057 (1984) ("[I]t can be deceptive to tell only half the truth, and to omit the rest."); see also Nat'l Bakers Servs., v. FTC, 329 F.2d 365, 367 (7th Cir. 1964) (holding that a baker's truthful advertisement that its bread contained "only 46 calories per slice" was found deceptive because it created the illusion that the bread was a special diet food, when in fact the bread was only sliced more thinly than other breads).

\textsuperscript{124} See Kraft, Inc. v. FTC, 970 F.2d 311 (7th Cir. 1992).

\textsuperscript{125} Id.

\textsuperscript{126} See Murphy, supra note 1, at 2402 ("[T]he typical transaction between a merchant or seller and a consumer increasingly can be characterized as an exchange of goods or services for money and information.").

\textsuperscript{127} See, e.g., Statement of Basis and Purpose and Regulatory Analysis, Trade Regulation Rule, Funeral Industry Practices, 47 Fed. Reg. 42,260, 42,274-77 (1982) (declaring that the FTC sees as deceptive, failure of funeral directors to correct consumer misconceptions about need for embalming and need for caskets for cremation even though funeral directors themselves did not create misconceptions); Statement of Basis and Purpose, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8,324, 8,352 (1964) ("The principle crystallized in [cases] is that Section 5 [of the FTC Act] forbids sellers to exploit the normal expectations of consumers in order to deceive just as it forbids sellers to create false expectations by affirmative acts."). See generally Pridgen, Consumer Protection, supra note 78, § 10.07 (discussing the concept and consequence of deception by omission); Ivan L. Preston, The Federal Trade Commission's Identification of Implications as Constituting Deceptive Advertising, 57 U. Cin. L. Rev. 1243, 1277-81 (1989) (addressing product claims that contain no explicit qualifications, and thus falsely imply that no material qualifications exist).
would normally expect cars sold in such circumstances to be new.\(^{128}\) In the privacy context, such normal but incorrect expectations probably also arise. For example, many consumers provide the personal information sought on warranty cards. Some probably assume that the information is needed to register the purchase, but in fact much of the information is instead used to generate data about consumers that can be used for marketing purposes.\(^{129}\)

In recent years, however, the Commission has been less protective of consumers when it finds the omission before it to constitute a "pure omission" rather than a half-truth.\(^{130}\) In the controversial 1984 *International Harvester* decision, in which it found an omission unfair but not deceptive, the Commission wrote that because of the many misconceptions different consumers might have about a variety of matters, some of them bound to be idiosyncratic, "it would be both impractical and very costly to require corrective information on all such points."\(^ {131}\) However, the FTC will continue to view a business's behavior as deceptive if the business is silent "under circumstances

\(^{128}\) *In re* Peacock Buick, Inc., 86 F.T.C. 1532, 1552, 1557-58 (1975); see also *In re* Simeon Mgmt. Corp., 87 F.T.C. 1184, 1230 (1976) ("It is deceptive... to fail to disclose in advertisements promoting [a] weight reduction program that the treatments employ prescription drugs not approved for weight reduction by FDA. Some consumers will reasonably believe, and indeed have a right to assume, that controls are exercised by the government over the promotion and use of prescription drugs.").

\(^{129}\) *See, e.g.*, Joshua Quittner, *Invasion of Privacy*, Time, Aug. 25, 1997, at 33 ("Think twice before filling out warranty cards or entering sweepstakes. These are data mines for marketers. Besides, most products are guaranteed by your sales receipt."). O'Harrow states:

An Arkansas company that provides information to marketers has amassed 135 million consumer telephone numbers—including about 20 million that are unlisted—to help identify and profile people who call toll-free lines to shop or make an inquiry.

When someone makes a toll-free call to a client of Acxiom Corp. of Conway, Ark., a telemarketing agent can learn who the caller is and where he or she lives, even before answering the call. The agent also can often find out the kind of home the caller lives in, the type of cars the people in that household drive, whether they exercise—even whether they own a cat. . . .

Company officials won't detail exactly how they gather the 20 million unlisted numbers, which they said represent about half of all unlisted numbers in the nation. They acknowledged that some of the information comes from "self-reported sources." Industry specialists said that could include surveys, product registration cards and credit card applications.


\(^{130}\) *See In re* Int'l Harvester Co., 104 F.T.C. 949, 1059-60 (1984) ("[P]ure omissions are not appropriately characterized as deceptive or reached through deception analysis... However, the Commission does not treat pure omissions as deceptive.").

\(^{131}\) *Id.* at 1059. The decision is sharply criticized in Greenfield, *supra* note 72, at 81-84.
that constitute an implied but false representation . . . [which] may arise from . . . the circumstances of a specific transaction.  

Is the omission here, where personal data provided by the consumer is put to other uses, such as compiling marketing lists, more properly characterized as a half-truth or a pure omission? If you use the standard meanings of those phrases, it is probably a pure omission. But even if this is the case, the omission should still be seen as deceptive. This is not the situation at which the pure omission standard seems aimed, where many consumers have different expectations of what would be disclosed. Rather, we know from the available evidence that many consumers have the same expectation—that their information will not be sold—and that that expectation is not being met. In any event, given the ambiguity, a better focus would not be on what type of omission this is, but on whether the conduct in question is in fact deceptive, and so should be regulated. As discussed above, it frequently is deceptive. Consumers acting reasonably in consumer transactions are often unaware of the uses to which their personal information is being put. Hence the FTC could, if it wishes, intervene.

For the trade in consumer information to constitute deception, it would also have to meet the materiality requirement. Something is material if it is "likely to affect consumers' conduct or decision with regard to a product." If consumers have been honest about what they are telling the pollsters, then we know that the trade in consumer information has affected some consumers' purchasing decisions. It thus appears that the materiality requirement is satisfied.

132. Int'l Harvester, 104 F.T.C. at 1058. In In re Figgie Int'l, Inc., the Commission offered an example of an implied representation, stating: "the very act of offering goods for sale creates an implied representation that the goods are reasonably fit for their intended uses and free of gross safety hazards." 107 F.T.C. 313, 379 n.17 (1986). One author argues that sellers should have obligations to disclose under state deceptive trade practices statutes, when an information source knows or has reason to know that disclosure of a fact would correct a mistake about a basic assumption upon which the other party is operating in entering into a transaction . . . [or] when an information source knows or has reason to know that there is a high probability that a buyer is ignorant of a fact that the buyer subjectively believes is material to the transaction and the information source can provide information about the fact efficiently and at a lower cost than the buyer. 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).

133. Int'l Harvester, 104 F.T.C. at 1056; see also In re Southwest Sunsites, Inc., 105 F.T.C. 7, 149 (1985).

134. See supra note 84 and accompanying text.
D. FTC Privacy Interventions

The FTC has occasionally intervened to remedy misbehavior in information practices. Recently, the FTC acted to prevent companies from affirmatively misrepresenting their information practices, and filed suit to prevent an information broker from obtaining personal information about consumers under false pretenses by, for example, calling a bank and pretending to be the depositor to learn financial information. In another case, the FTC reached a consent agreement with a company that had sent deceptive unsolicited commercial e-mail using e-mail addresses it had harvested from a competitor's Web site; the company agreed to refrain from such practices in the future, among other things. In older cases, discussed below, the FTC stepped in when a merchant attempted to use personal information seemingly collected for one purpose, for a different purpose.

An example of one of these older cases is In re Metromedia, Inc., a case that terminated in a consent order. Metromedia had sent consumers a form letter along with a questionnaire and invited them to complete and return the questionnaire to be eligible for prizes. The mailing explained that the questionnaire "is being sent to a number of people in your area to obtain information about habits and characteristics of people living in different sections of the country." It added, "[t]here is nothing to buy, and we assure you that no salesman will call on you." The FTC's complaint charged Metromedia with representing, either directly or impliedly, that the purpose of the mailing was for something other than selling goods and services, and that respondents would not be solicited to buy things. It viewed that as deceptive.

The FTC also claimed that Metromedia had behaved both deceptively and unfairly in:

135. See supra note 66.
139. Id. at 333.
140. Id.
141. Id.
142. Id. at 337.
seek[ing] to elicit responses in the manner aforesaid and to fail to disclose clearly and conspicuously the purpose for which the information contained on said questionnaire was being requested, and to fail to disclose that it was in the business of compiling mailing lists which are for sale or rent to mail-order advertisers and sellers of merchandise and services, and that the information requested would be used, together with the name and address of the addressee in the compiling of such lists.¹⁴³

The complaint also acknowledged the significance of the consumer interest in privacy:

A substantial portion of the purchasing public has a preference that their names not appear on mailing lists. This preference arises out of various individual and personal reasons such as, but not limited to, the unauthorized invasion of personal privacy; being subjected to the repeated importuning of promoters, advertisers and sellers of merchandise, services and schemes; and being exploited by respondent and the users of said ... mailing list.¹⁴⁴

Normally a complaint is of no precedential value whatever. But, as discussed above, FTC consent orders are in a different category.¹⁴⁵ At a minimum, the complaint and consent order indicate that the FTC thought the challenged conduct, if proven, would have violated the FTC Act. To be sure, Metromedia's actions are arguably distinguishable from the conduct discussed in this article. Metromedia allegedly sought to create an impression at odds with its true purpose, while the sellers of consumer information today often do not do that; they simply use information obtained in one transaction for another. But it is a short step from saying that sellers who seek information for direct mail solicitations cannot say what Metromedia supposedly did—that they want information about habits and characteristics of people, and that no salesperson will call on the consumer—to saying that merchants who wish to use information about consumers, and who know that the consumers have misconceptions about what will be done with their personal information, must dispel those misconceptions.

Another vintage case sheds further light on FTC information jurisprudence. During the sixties, Beneficial, a lender, entered the tax preparation business, motivated in part to generate customers for its loan business.¹⁴⁶ At first, Beneficial used the information provided by the taxpayer to solicit the taxpayer to borrow from Beneficial; for example, Beneficial, having learned from the taxpayer what loans the taxpayer had, might urge the taxpayer to consolidate debts with a

¹⁴³. Id.
¹⁴⁴. Id.
¹⁴⁵. See supra note 66.
Beneficial loan.\footnote{147} After Congress passed a statute making it a crime for commercial tax-preparers to use taxpayer data for non-tax purposes without the taxpayer's consent,\footnote{148} Beneficial adopted procedures designed to generate loan customers without violating the criminal statute. Thus, Beneficial required tax preparation customers to fill out a form authorizing Beneficial to solicit the customer for "any business" in which Beneficial might engage and to agree that information appearing on a loan application was not given for tax preparation.\footnote{149}

Using pre-1980 standards, the Commission found Beneficial's conduct unfair, noting that "[p]ersonal financial data is the private business of the individual to whom it relates."\footnote{150} Though the FTC focused especially on the nature of tax confidentiality, in a note it observed:

In light of the pervasive and specific policy of tax confidentiality, we ... have no need to decide whether a broader consideration of personal privacy could govern this case. In declining to reach that issue, however, we do not suggest that a generalized right of personal privacy and personal control over private data is an inadequate foundation on which to ground a finding of unlawfulness under Section 5. In fact, the right of privacy has become a widely-valued public policy, with constitutional and statutory underpinning .... Its violation in a commercial context would likely be unlawful under the Federal Trade Commission Act.\footnote{151}

The FTC also found Beneficial's conduct deceptive. Using the pre-1983 standards for deception, the Commission wrote:

Although the public expects the fiduciary character of a taxpayer-tax preparer relationship to be honored, Beneficial entered such relationships with no intention of guarding tax information from unauthorized use, and in fact converted tax data for its own profit. Beneficial's failure to disclose these conditions had the capacity to mislead consumers into believing that the information they provided would only be used for preparing their tax returns. Such an omission of facts which are material to an intelligent purchasing decision is unlawful ....\footnote{152}

\begin{footnotes}
\footnote{147}{In re Beneficial Corp., 86 F.T.C. at 169.}
\footnote{149}{In re Beneficial Corp., 86 F.T.C. at 169.}
\footnote{150}{Id. at 172.}
\footnote{151}{Id. at 172, n.9.}
\footnote{152}{Id. at 173. In another case, In re H & R Block, Inc., 80 F.T.C. 304 (1972), the FTC entered into a consent order prohibiting a tax preparer from using customer information obtained through the tax preparation process for purposes unrelated to preparation of tax returns, except with the consent of the taxpayer. The complaint alleged that H & R Block had provided the information to other entities which used the information to solicit consumers. By entering into the settlement, H & R Block did not admit that it had violated the law. The consent order was modified later in light of the enactment of 26 U.S.C. § 7216. In re H & R Block, 100 F.T.C. 523 (1982).} \end{footnotes}
A later decision casts doubt on how broadly Beneficial can be read. Beltone, a manufacturer of hearing aids, required dealers whose relationship to Beltone was terminated to supply to Beltone the names and addresses of customers to whom they had sold a Beltone product. The administrative law judge found this an unfair practice, citing Beneficial, and analogizing the relationship between hearing aid users and dealers to that between physician and patient. The Commission reversed, finding Beneficial distinguishable. It saw Beneficial as based on two things. The first was a breach of "the widely recognized and manifested concern for the confidentiality of individual tax information . . . " In Beltone, by contrast, the FTC wrote that "whatever public policy exists favoring preservation of confidentiality in the user-dealer relationship, it does not nearly approximate the broad policy and statutory mandate that provided the basis for the Beneficial decision." Second, the Commission viewed Beneficial as resting on a deliberate breach of a fiduciary relationship. It apparently found no such breach in Beltone. The Commission noted also the absence of a record to justify an inference of consumer injury: "While we do not necessarily endorse the practice of rental of hearing aid customer names (a practice that ceased in 1973), there is insufficient information in this record upon which to find substantial injury resulting from it." In a footnote, the Commission identified a third distinction from Beneficial: the only information transmitted to the manufacturer in Beltone was the customer's name, while in Beneficial, the loan division had access to all of the information in the tax returns.

Beltone offers ambiguous support to those trading in consumer information. Conventional information transfers among merchants, like those in Beltone, do not implicate a fiduciary relationship or involve tax returns. On the other hand, many sales of consumer information involve considerably more information than a consumer's name and address. Sometimes the information conveyed is as private as the information contained in tax returns. Some regard information about a person's likes and dislikes, their religion and sexual orientation, and their purchases as highly personal. If an attempt were made to demonstrate injury to consumers from the disclosure of information—an attempt which could well succeed given the survey

For a discussion of the effect of FTC consent orders, see supra note 66.
154. Id. at 220.
155. Id.
156. Id.
157. Id. at 220, n. 67. Beneficial is also distinguishable from the situations described in this article in another respect: the company seemed involved in a scheme intended to circumvent an explicit federal statute. Moreover, Beneficial was decided using outmoded standards. See supra note 150 and accompanying text.
data now available\textsuperscript{158}— the Commission could, if it were so inclined, find \textit{Beltone} distinguishable.\textsuperscript{159}

The Commissioners recently had occasion to debate the scope of \textit{Beneficial}. When the Commission filed suit in \textit{FTC v. Rapp},\textsuperscript{160} in which the FTC accused the defendants of having wrongfully identified themselves to financial institutions as account holders to obtain personal information for sale to others, Commissioner Swindle dissented. The remaining Commissioners, Chairman Pitofsky, Commissioners Anthony and Thompson, issued a statement explaining their decision to initiate the suit, noting that "we have previously recognized that the misuse of certain types of private financial information can be ‘legally unfair,’ [citing \textit{Beneficial}]. Thus, no new theory of consumer injury is advanced here."\textsuperscript{161} Thus, three Commissioners view \textit{Beneficial} as relevant to information practices beyond tax return information.

Commissioner Swindle found the citation of \textit{Beneficial} inapposite, arguing that \textit{Beneficial} was based on the fiduciary relationship between the customer and tax preparer.\textsuperscript{162} Commissioner Swindle

\begin{footnotes}
\item[158] See supra notes 17-18, 84.
\item[159] \textit{Beltone} may also be distinguishable from the common situation in which information is sold by one company to another in that the relationship between manufacturer and dealer is closer than that between two unaffiliated companies whose only business dealings involve the sale of information.
\item[160] Complaint for Injunction and Other Equitable Relief, FTC v. Rapp, No. 99-WM-783, at http://www.ftc.gov/os/1999/9904/touchtonecomplaint.htm (Apr. 22, 1999) [hereinafter Complaint, FTC v. Rapp]. The case terminated in a settlement. In the Stipulated Consent Agreement and Final Order, the court found that "[t]he Complaint states a claim upon which injunctive relief may be granted against the defendants under... the FTC Act..." but also stated that "[t]his agreement is for settlement purposes only and does not constitute an admission by defendants that the law has been violated as alleged in the Complaint or that the facts as alleged in the Complaint, other than jurisdictional facts, are true." Consent Agreement, FTC v. Rapp, supra note 136. After the FTC brought the case, Congress enacted a statute limiting to certain circumstances the practice of misrepresenting oneself to obtain financial information, also known as "pretexing." See Gramm-Leach-Bliley Act, § 521, Pub. L. No. 102-106, 113 Stat. 1338 (1999) (codified at 15 U.S.C.A § 6821 (Supp. 2000)); cf. Commonwealth v. Source One Assocs., 1999 WL 975120, at *12 (Mass. Super. Ct. 1999) ("[O]btaining private financial information by pretext for the resale to others in the circumstances found here constitutes unfair and deceptive acts in trade or commerce.").
\end{footnotes}
also questioned Beneficial's precedential value in light of the changes in the FTC Act since the case was decided. However, in remarks delivered to the Direct Marketing Association Government Affairs Conference, Commissioner Swindle warned that Rapp "advances a new theory of consumer injury based solely on the disclosure of 'private' financial information" and that the case "could establish the principle that an invasion of a consumer's privacy is injury, with no need to show that any substantial resulting harm to the consumer is likely."\textsuperscript{163}

Another recent case sheds additional light on the Commission's use of its unfairness power to protect consumer privacy. An online auction house, ReverseAuction.com, sent deceptive e-mails soliciting business to e-mail addresses it had harvested from eBay, a competitor site. This violated the eBay User Agreement—to which ReverseAuction had apparently subscribed—which prohibits eBay users from employing information obtained from the eBay site for sending unsolicited commercial e-mail. The FTC charged ReverseAuction with engaging in both deceptive and unfair practices.\textsuperscript{164} ReverseAuction and the FTC entered into a consent agreement under which ReverseAuction agreed to refrain from similar practices in the future and to provide certain notices both to those it had solicited and on its Web site.\textsuperscript{165}

FTC Commissioners Swindle and Leary filed a Statement in which they both concurred and dissented.\textsuperscript{166} While they agreed that ReverseAuction had acted deceptively, the Commissioners concluded that ReverseAuction's use of eBay's user information did not rise to the level of a substantial injury within the meaning of the statute, and so did not violate the unfairness prong of the FTC Act. The two Commissioners repeated the language that appeared in the FTC Policy Statement on unfairness and was carried forward into the 1994 Senate Report on the amendments to the FTC Act, about trivial or speculative harms.\textsuperscript{167} And, they explained:


\textsuperscript{167} See text accompanying supra note 86. Commissioners Swindle and Leary noted:

The Commission is not concerned with trivial or merely speculative harms.
Consumers do not have a substantial privacy interest in the e-mail addresses and other information that ReverseAuction harvested since consumers had already agreed to make this information available to millions of other eBay members (albeit with restrictions on using it for commercial solicitations). Moreover, a substantial portion of this information is available without restriction to non-members who visit eBay's web site. Merely obtaining consumers' e-mail addresses without their explicit consent and sending them e-mail solicitations does not cause substantial injury.... This standard for substantial injury overstates the appropriate level of government-enforced privacy protection on the Internet, and provides no rationale for when unsolicited commercial e-mail is unfair and when it is not. We are troubled by the possibility of an expansive and unwarranted use of the unfairness doctrine.1

The pair left the door open to other unfairness-based privacy cases, however, noting that "[w]e do not say that privacy concerns can never support an unfairness claim."169

Commissioner Thompson responded that an unfairness claim was more appropriate than a deception claim.170 He explained that:

the harm caused in this case is especially significant because it not only breached the privacy expectation of each and every eBay member, it also undermined consumer confidence in eBay and diminishes the electronic marketplace for all its participants. This injury is exacerbated because consumer concern about privacy and confidence in the electronic marketplace are such critical issues at this time.171

Addressing the quote from the Policy Statement, Commissioner Thompson wrote that "the injury caused by ReverseAuction's conduct, far from being speculative, is a tangible misappropriation of personal protected information that enabled the company to send personalized deceptive e-mail messages to scores of consumers."172

ReverseAuction thus significantly supports those who believe that invasions of privacy can cause substantial injury within the meaning of

---

In most cases a substantial injury involves monetary harm .... Unwarranted health and safety risks may also support a finding of unfairness. Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair.


168. Swindle & Leary Statement, FTC v Reverseauction.com, supra note 166 (citation omitted).

169. Id.


171. Id. Commissioner Thompson also wrote, in connection with the standards for unfairness, that "the injury could not have been avoided by those members [of eBay], and it was not outweighed by countervailing benefits." Id.

172. Id.
the FTC Act. But it does not necessarily mean that all privacy invasions come within that statute. In his statement, Commissioner Thompson limited the scope of the case. He wrote:

[T]he Commission does not here declare that sending unsolicited commercial e-mail . . . is unfair in all circumstances, nor does it suggest that privacy invasions cause substantial injury in all circumstances. Instead, the Commission posits that, under the facts presented here, it is unfair for ReverseAuction to improperly obtain personal information for its use. Accordingly, a majority of the Commission believes that the specific relationship, obligations, and expectations of this electronic community make ReverseAuction's behavior "unfair" under Section 5.\textsuperscript{173}

Still, ReverseAuction may serve as a springboard to find privacy violations in many other situations. Probably few eBay users read the User Agreement, and so it is likely that many users were unaware of the protections afforded their privacy by that agreement. Even those who read the agreement might not have expected other users to adhere to the privacy protections it promised. E-mail direct marketers are notorious for misbehavior, often ignoring requests to be removed from e-mail marketing lists and sometimes even flaming those who make such requests.\textsuperscript{174} Thus, many consumers who provided their e-mail address to eBay may have expected it to be treated even less privately than information obtained about them in other consumer transactions. After all, as Commissioners Swindle and Leary pointed out, consumer information is not normally available to millions of others, unlike information posted on Ebay.\textsuperscript{175}

If using an e-mail address that is available to millions to solicit business constitutes a substantial injury, wouldn't using much more private information—such as urinary incontinence—which is not

\textsuperscript{173} Id.
\textsuperscript{174} See, e.g., FTC, Public Workshop on Consumer Information Privacy Session Two: Consumer Online Privacy 11 (June 12, 1997), available at http://www.ftc.gov/bcp/privacy/wkshp97/index.html (remarks of Jason Catlett, Chief Executive Officer, Junkbusters Corp., stating that some spammers "actually maintain their own pseudo-remove addresses but simply use the results as an additional source of addresses to spam"). One article on information privacy warns:

Spammers often punish those who try to opt out of getting unsolicited e-mail by "flaming" them—sending them nasty messages online, sometimes in overwhelming numbers. Just ask David Aronson, a Dulles, Va. software engineer and outspoken spam critic. On top of the 20-odd spams he receives at work and home on an average day, Aronson showed MONEY a stream of filthy, utterly unprintable flames from someone who described himself as a "gay atheist commie spammer." Warns Aronson: "Never, ever reply directly to spammers. It tells them your e-mail address is valid. They will sell it, and you'll get more spam."

Dowd, Protect Your Privacy, supra note 2, at 110.

\textsuperscript{175} Swindle & Leary Statement, FTC v. ReverseAuction.com, supra note 166.
known by the consumer to be available to others, also constitute a substantial injury?  

In sum, putting together Beneficial, Rapp, Metromedia, and ReverseAuction yields a number of precedents for FTC intervention in transactions involving consumer information. In one—ReverseAuction—the path to a misrepresentation seems fairly attenuated, depending on a promise made not to those whose e-mail addresses were used, but rather in a User Agreement with eBay, which had in turn asked those whose information was used to enter into the same form Agreement, which the consumers might not even have remembered. In Metromedia, the misrepresentation merely made express what consumers often assume—that by providing personal information, they are not facilitating their own solicitation. If the FTC has the power to step into these cases, as it surely does, it is hard to deny it also has the power to intervene in cases in which consumers are misled by sharing commonly-held assumptions.

Should the FTC exercise that power? That question is bound up with issues of resources and politics. As for the resources issue, given the Commission’s scarce resources, it must make choices about which matters merit its attention, and certainly the Commission could find other matters that it regards as more critical. But privacy is important as well, and the FTC has already turned its attention to privacy.

The political aspects of the issue are far more complex and beyond the scope of this article. Ideally, a matter that concerns consumer preferences would be resolved by the legislature, the body best equipped to convert popular preferences to policy judgments. Legislators have in fact introduced bills, and some have made progress towards becoming law. But if Congress fails to act, as it has to date,
what then? Should the Commission take the position that these matters should be resolved exclusively by Congress, and if Congress does not do so, the Commission should also not act? Or should the FTC intervene if Congress does not act within a certain period of time? The FTC has acted in the past on matters that could have been left to Congress. For example, the FTC has, by trade regulation rule, essentially abolished the holder in due course doctrine.\textsuperscript{179} The FTC’s power to promulgate trade regulation rules enables it to avoid the problem of retroactive rule-making referred to above as a drawback of judicial regulation of the trade in personal information.\textsuperscript{180} If the Commission can craft a trade regulation rule that properly mediates among the conflicting interests, that resolution seems preferable to the current situation in which consumers who wish to opt out face great difficulties in doing so.\textsuperscript{181}

IV. LITTLE FTC ACT ACTIONS

As discussed above, only the FTC can sue under the FTC Act. But every state has enacted a “little FTC” act, prohibiting, in one form or another, deceptive, and sometimes unfair, trade practices.\textsuperscript{182} While there is considerable variation in the precise wording of the statutes, most either prohibit a list of specified practices and then contain a catch-all—such as section 2(12) of the Uniform Deceptive Trade Practices Act, which bars a person from engaging “in any other conduct which similarly creates a likelihood of confusion or of misunderstanding”—or omit the laundry list and contain only a broadly-worded injunction.\textsuperscript{183} For example, New York’s statute states: “Deceptive acts or practices in the conduct of any ... service in this state are hereby declared unlawful.”\textsuperscript{184}

\textsuperscript{179} See supra note 65 and accompanying text.

\textsuperscript{180} See supra note 27. The FTC’s power to promulgate trade regulations outlawing conduct as unfair or deceptive is codified at 15 U.S.C. § 57a(a)(1) (1994).

\textsuperscript{181} For a discussion of whether privacy regulation should be entrusted to a regulatory agency, see Murdock, supra note 44, at 615-18.

\textsuperscript{182} For a discussion of the characteristics of each state’s little FTC Act, see Sheldon & Carter, supra note 66, at 759-75 app. A.


\textsuperscript{184} N.Y. Gen. Bus. Law § 349(a) (McKinney 1988); see also N.Y. Gen. Bus. Law. § 350 (“False advertising in the conduct of any business trade or commerce or in the furnishing of any service in this state is hereby declared unlawful.”).
These statutes typically provide for a double-barreled enforcement strategy: first, a state agency—perhaps the attorney general—can bring actions on behalf of the state.\textsuperscript{185} Thus, even if the FTC declines to expand its activity in this arena, state enforcement agencies could act. Though that would produce non-uniform rules, we already have that result to a limited extent because some states have legislated on privacy while others have not.\textsuperscript{186}

In addition to enforcement by a state agency, most states provide a private cause of action to consumers who have suffered an injury.\textsuperscript{187} Because the typical recovery sought in consumer claims is not large enough to warrant suit,\textsuperscript{188} the statutes often provide for a bonus for successful consumer plaintiffs in the form of one or more of multiple damages,\textsuperscript{189} punitive damages,\textsuperscript{190} and statutory minimum damages.\textsuperscript{191}


\textsuperscript{186} See \textit{supra} notes 37, 44-52 and accompanying text.

\textsuperscript{187} Most states have created a private cause of action by statute; in a handful of states the statute is silent on private claims but the courts have ruled that the statute implies a private cause of action. See \textit{e.g.}, Sheldon & Carter, \textit{supra} note 66, §§ 7.1-7.2, at 453-56, 759-75 app. A; Sovern, \textit{Private Actions, supra} note 59, at 446-49.

\textsuperscript{188} See, \textit{e.g.}, Missouri \textit{ex rel.} Danforth v. Independence Dodge, Inc., 494 S.W.2d 362, 370 (Mo. Ct. App. 1973) ("[I]ndividual action by consumers is much too costly in that the expense of litigation usually outweighs the amount of likely recovery."); William A. Lovett, \textit{State Deceptive Trade Practice Legislation}, 46 Tul. L. Rev. 724, 725 (1972) ("[U]nder the traditional rules of the game, it was less expensive to suffer most deceptive trade practices than to remedy them through legal action.").


The statutes generally contain attorneys' fees provisions as well. Consequently, if the information practices described in this article violate a state's little FTC Act, defendants could face significant exposure.

Do defendants in fact face any risk? Some may think so; in several recent cases in which marketers' practices were challenged, they quickly abandoned the practice. They may have good reason. As discussed above, it can be argued persuasively that the trade in personal information violates the FTC Act. Courts interpreting little FTC acts have found interpretations of the FTC Act enormously influential. Indeed, some state statutes explicitly direct the courts to


192. See Cole, supra note 185, at 130 ("All of those states that have private rights of action now have provisions for attorneys' fees.") See generally Sheldon & Carter, supra note 66, § 8.8, at 555-82 (analyzing state law provisions for attorney fees in depth).


194. See, e.g., In re Scrimpsher, 17 B.R. 999, 1015 (Bankr. N.D.N.Y. 1982) (making "synonymous" findings under New York law and the FTC Act); Marshall v. Miller, 276 S.E.2d 397, 401 (N.C. 1981) ("The character of the plaintiff, i.e. whether public or private, should not alter the scope of the remedy under this statute."); Hardy v. Toler, 218 S.E.2d 342, 345 (N.C. 1975) (examining decisions on appeal from the FTC); Commonwealth ex rel. Zimmerman v. Nickel, 26 Pa. D. & C.3d 115, 120 (C.P. Mercer Cty. 1983) (looking to the FTC Act and Commission decisions for guidance); see also Sheldon & Carter, supra note 66, § 3.4.5.1, at 131 ("Courts... show great deference to FTC actions in interpreting UDAP statutes [even] where the statute does not expressly refer to the precedential value of FTC decisions."); Robert D. Cohan, The Rights and Duties of Retail Merchants Under State Consumer Protection Laws: Emergent Doctrines and Strategies of the Defense, 18 New Eng. L. Rev. 297, 301
take into account interpretations of the FTC Act.\textsuperscript{195} Accordingly, colorable arguments can be made that selling the personal information of consumers also violates the little FTC acts of at least some states.

The fact that states base their interpretations on the FTC Act plays out in a number of ways. For example, just as with interpretations under the FTC Act, many states do not regard the fact that a practice is common within an industry as a defense under little FTC acts.\textsuperscript{196} But in one respect, many states have been more generous to consumers than has the FTC. Many states continue to use the deception standards the FTC employed before 1983, which permit courts to find deception more readily, at least in theory.\textsuperscript{197} Under

\begin{itemize}
\item \textsuperscript{195} For example, West Virginia's law states:

\begin{quote}
[T]he purpose of this article is to complement the body of federal law governing ... unfair, deceptive and fraudulent acts or practices ... It is the intent of the legislature that, in construing this article, the courts be guided by the interpretation given by the federal courts to the various federal statutes dealing with the same or similar matters.
\end{quote}


\item \textsuperscript{197} Among those expressing the view that the change in language may have no significance in application are Greenfield, supra note 72, at 71 ("It is unclear whether the new articulation changes the standard of deception ... "); Sheldon & Carter, supra note 66, § 4.2.9, at 145; Crawford, supra note 110, at 305 (commenting that the
those standards, deception requires only that the offending practice have a capacity or tendency to deceive the credulous consumer.\textsuperscript{195} Hence, even if the FTC concludes that practices pass muster under the FTC Act, it is still at least theoretically possible for a state to find the practices deceptive under their own legislation.

A number of cases support the conclusion that at least some information practices may be actionable. For example, Maryland defines something as material if a significant number of unsophisticated consumers would consider the information important in deciding on a course of action.\textsuperscript{199} As the survey evidence discussed above demonstrates, many consumers view the disclosure of their personal information as important.\textsuperscript{200}

Some states have ruled that, in some circumstances at least, the seller's failure to disclose a benefit received from the sale violates a little FTC act. For example, courts have found deception when sellers did not inform a car buyer that the car had previously been advertised at a lower price,\textsuperscript{201} or that the seller was charging excessive dealer preparation charges in light of the work done by the seller,\textsuperscript{202} or that securing a new loan would be much less costly than refinancing an old loan.\textsuperscript{203} Though each of these cases is distinguishable, they demonstrate a willingness by states to hold sellers' feet to the fire on disclosure issues when the seller benefits from non-disclosure.\textsuperscript{204} Hence, in light of the benefits sellers receive from trading in consumer

\textsuperscript{195} See, e.g., FTC v. Sterling Drug, Inc., 317 F.2d 669, 674 (2d Cir. 1963) ("[l]t has been consistently held that advertising falls within [the FTC Act's] proscription... when there is a likelihood or fair probability that the reader will be misled.").


\textsuperscript{200} See supra notes 17-18 and accompanying text.


\textsuperscript{204} See also Besta v. Beneficial Loan Co. of Iowa, 855 F.2d 532, 535, (8th Cir. 1988) (finding finance company violated statute prohibiting unconscionable behavior when it financed loan over six years without informing borrower of the option to borrow for three years on better terms); T.J. Fox v. Indus. Cas. Ins. Co., 424 N.E. 2d 839, 842 (Ill. App. Ct. 1981) (stating insurer could be liable under state little FTC act for acts of insurer's agent in selling insurance without informing insured that better and less expensive insurance was available); Browder v. Hanley Dawson Cadillac Co., 379 N.E.2d 1206, 1212 (Ill. App. Ct. 1978) (reversing dismissal of claims that auto dealer violated common law fiduciary duty and little FTC act by selling insurance without telling consumer that consumer could obtain cheaper policy with comparable coverage). But see Gershon v. Hertz Corp., 626 N.Y.S.2d 80, 81 (N.Y. App. Div. 1995) (relying on guidelines of National Association of Attorneys General to find no violation of statute when car rental agency did not tell customer that rates charged would be lower if customer made reservation at least two hours in advance of rental).
information, courts may also be willing to require sellers to disclose their information practices.\footnote{205}

It is quite clear that many little FTC acts make sellers' omission of material facts actionable. Some states have written this directly into their statutes. For example, Maryland proscribes the "[f]ailure to state a material fact if the failure deceives or tends to deceive."\footnote{206} A number of states limit the prohibition on omissions to knowing omissions,\footnote{207} but often sellers who also sell personal information have the requisite scienter.

A number of states have statutes that do not expressly extend to omissions, but have interpreted their statutes as barring omissions. Some have done so through regulations. For example, Massachusetts prohibits the failure "to disclose to a buyer or prospective buyer any fact, the disclosure of which may have influenced the buyer or prospective buyer not to enter into the transaction."\footnote{208} Missouri's regulations also bar omission of material facts,\footnote{209} while Idaho's prohibit omitting material or relevant facts that directly, or by implication, have the capacity and tendency or effect of deceiving buyers in certain circumstances.\footnote{210}

Other states have used case law to establish that omissions can be deceptive. For example, in \textit{McRae v. Bolstad},\footnote{211} defendants sold plaintiff a house without disclosing that the house had chronic sewage and drainage problems. The court affirmed a judgment for the plaintiffs under the Washington State little FTC act, which does not explicitly refer to a duty of disclosure.\footnote{212} Similarly, in \textit{Johnson v.}\footnote{213}

\begin{footnotes}
\item[207.] \textit{See}, e.g., Tex. Bus. & Com. Code Ann. § 17.46(b)(23) (Vernon 1987) (prohibiting "the failure to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed").
\item[210.] Idaho Rules of Consumer Protection, Idaho Admin. Code 04.02.01.030 (2000). The section, entitled "False, Misleading or Deceptive Conduct in General" states: An omission of a material or relevant fact shall be treated with the same effect as a false, misleading, or deceptive claim or representation, when such omission, on the basis of what has been stated or implied, would have the capacity, tendency, or effect of deceiving or misleading a consumer acting reasonably under the circumstances.
\item[Id.] 676 P.2d 496 (Wash. 1984).
\item[212.] \textit{Id.} at 501; \textit{see also State v. Ralph Williams' N.W. Chrysler Plymouth, Inc.}, 553
\end{footnotes}
Beverly-Hanks & Associates, a real estate broker hired an inspector whom the sellers had previously hired to inspect the same building. The court ruled the broker's failure to disclose that fact to the buyer a deceptive trade practice.

Any consumer suing on this ground would have to come to grips with Dwyer v. American Express Co. In Dwyer, plaintiffs unsuccessfully alleged that defendants' practice of renting to others information about consumers' purchasing habits violated the Illinois little FTC act. Though the court rejected the claim, its opinion nevertheless suggests that in other circumstances, plaintiffs' claim might succeed. The court acknowledged that "[i]t is highly possible that some customers would have refrained from using the American Express Card if they had known that defendants were analyzing their spending habits." Accordingly, the court concluded, albeit in dicta, that plaintiffs had adequately alleged that defendant's failure to disclose its information practices was material and deceptive, and that defendants intended for plaintiffs to rely on the nondisclosure.

Nevertheless, stating "the only damage plaintiffs could have suffered was a surfeit of unwanted mail," the court held that plaintiffs had failed adequately to allege damages. The court explained:

We reject plaintiffs' assertion that the damages in this case arise from the disclosure of personal financial matters. Defendants only disclose which of their cardholders might be interested in purchasing items from a particular merchant based on card usage. Defendants' practice does not amount to a disclosure of personal financial matters. Plaintiffs have failed to allege how they were damaged by defendants' practice of selecting cardholders for mailings likely to be of interest to them.

How useful Dwyer will be to defendants remains unclear. The case arguably misconceives the role of little FTC acts, which given their application to consumer transactions are intended to be used when the damages approach triviality—that is why so many of them provide for statutory damages. Indeed, other courts have been quicker to look to the consumer's mental state than Illinois. For example, a New

P.2d 423, 441 (Wash. 1976) (finding seller's failure to tell joint obligors of automobile purchase contracts that joint credit life insurance policies could be purchased for a lower price than separate policies was deceptive).

213. 400 S.E.2d 38, 43 (N.C. 1991).
214. Id.; see also Conway v. Am. Excavating, Inc., 676 A.2d 881, 887 (Conn. App. Ct. 1996) (finding purchaser had claim against developer for deception when developer did not tell purchaser that roadway providing access to lot might later be moved and roadway was later moved).
216. Id. at 1357.
217. Id.
218. Id.
219. Id.
220. See supra note 191 and accompanying text.
York court held that a consumer could proceed when the consumer was deceived into thinking a sale price was lower than in fact it was, even though the consumer did not make a purchase,221 while another found it deceptive to run an advertisement for a saw stating “Wrap up a beautiful Christmas” when the store failed to stock enough of the saws to meet the Christmas demand.222 Consumer claims have been sustained when the damages totaled less than $20.223 Some states even permit private suits when plaintiffs have not proved actual damages.224 By contrast, as Dwyer noted, the Illinois Consumer Fraud Act limits private claims to “any person who suffers actual damage.”225

Moreover, the Dwyer court overlooked the evidence suggesting that many consumers are genuinely troubled by the use of their personal information and that they regard preventing this injury as worthy of considerable effort, thus suggesting that in fact invasions of privacy do generate damages.226

Finally, even assuming Dwyer read the law correctly, American Express activities may still be distinguishable from the information practices of some other merchants, suggesting that Dwyer offers scant protection to at least some. American Express had provided the purchasers of its information with less data about consumers than some information-sellers engage in. Specifically, plaintiff had objected to three American Express practices.

First, American Express created six categories, such as “Rodeo Drive Chic” or “Value Oriented” and then applied those labels to cardholders so that information-buyers could target a particular type of consumer.227 Second, American Express offered to create lists that targeted cardholders who bought specific types of items.228 Among the examples given were purchasers of fine jewelry, mail order

226. See supra notes 17-18, 84 and accompanying text.
227. Dwyer, 652 N.E.2d at 1353.
228. Id.
apparel buyers, home-improvement shoppers, electronics shoppers, luxury lodgers, cardholders with children, skiers, frequent business travelers, resort users, travelers to Asia or Europe, luxury European car owners, or recent movers. Third, American Express offered joint marketing arrangements to certain sellers. That kind of information seems much less specific than some of the lists reported to be available, such as lists that focus on race, religion, or a problem with incontinence, or purchases of very specific and personal items, such as skimpy swimwear, wigs, and hair removal products. Hence, conceivably a court, which would find American Express had not injured a consumer, would find that other list-sellers had.

In sum, though it is by no means certain, information practices that are currently in widespread use may indeed violate state little FTC acts. Marketers should think carefully about whether they wish to alter their practices.

CONCLUSION

Information privacy advocates have given considerable attention either to common law invasion of privacy torts or new legislation, both of which have some appeal in addressing privacy concerns. But they have generally overlooked two other sources of privacy regulation: the FTC Act and state little FTC acts, or deceptive trade practices statutes. I have argued that common information practices—collecting transactional information about consumers and selling it to others without the knowledge or consent of the affected consumers—violates both the FTC Act and state statutes.

Thus far, the FTC does not seem disposed to use its powers under the FTC Act to force merchants to obtain consumer consent before trading in their information. As only the FTC has the power to enforce the FTC Act, that ends the matter. But the state statutes can be enforced both by state agencies and, in most states, injured consumers. Marketers of consumer information may soon find themselves under attack from an unexpected direction—one that often provides for statutory damages, multiple damages, and attorneys’ fees for successful plaintiffs.

229. Id.
230. Id.
231. See supra note 13. For reports of these and a variety of other lists, see Sovern, Opting In, Opting Out, supra note 7.
232. A drawback to the use of little FTC acts to determine that information practices are unlawful is that they are likely to be applicable retroactively. See supra note 27 and accompanying text. State authorities can ameliorate that problem by providing notice of their intent to use the statutes in such a fashion. But private litigants, who are likely to be less concerned with the public welfare, may choose not to do that.
Notes & Observations