

June 2002

Enhancing the Privacy Discourse: Consumer Information Gathering as Surveillance

Stan Karas

Follow this and additional works at: <https://scholarship.law.ufl.edu/jtlp>

Recommended Citation

Karas, Stan (2002) "Enhancing the Privacy Discourse: Consumer Information Gathering as Surveillance," *Journal of Technology Law & Policy*. Vol. 7: Iss. 1, Article 2.
Available at: <https://scholarship.law.ufl.edu/jtlp/vol7/iss1/2>

This Article is brought to you for free and open access by UF Law Scholarship Repository. It has been accepted for inclusion in *Journal of Technology Law & Policy* by an authorized editor of UF Law Scholarship Repository. For more information, please contact kaleita@law.ufl.edu.

**ENHANCING THE PRIVACY DISCOURSE:
CONSUMER INFORMATION GATHERING
AS SURVEILLANCE**

*Stan Karas**

I.	INTRODUCTION	30
II.	THE HISTORY OF DIRECT MARKETING	31
	A. <i>From the Mass to the Individual Consumer</i>	32
	B. <i>Database Technology and Aggregation of Personal Data</i> ..	33
	C. <i>Lack of Privacy Protection</i>	34
	D. <i>Expressiveness of Personal Consumption</i>	38
	E. <i>The Effectiveness of Psychographics</i>	39
	F. <i>Direct Marketing Today</i>	41
III.	CONSUMER DATABASES AS A FORM OF SURVEILLANCE	43
IV.	THE EFFECTS OF CONSUMER INFORMATION GATHERING	48
	A. <i>Loss of Control Over Information</i>	48
	B. <i>Retailing of Consumer Information: Back to Old Surveillance</i>	50
	C. <i>Dehumanizing Aspects of Database Marketing</i>	52
	D. <i>Panoptic Effects of Consumer Information Gathering</i>	55
V.	UNPACKING THE PROBLEM, EXPLORING THE OPTIONS	56
	A. <i>Insufficiency of Privacy Law in Dealing with Aggregation of Personal Information</i>	56
	B. <i>Options For Controlling Data Collection</i>	60
VI.	CONCLUSION	63

* J.D., School of Law, University of California, Berkeley (Boalt Hall), 2002; A.B., Stanford University, 1999. Thanks to Andrew Grotto for insightful comments on an earlier draft. For my parents and friends.

I. INTRODUCTION

Much of the legal literature on privacy is concerned with the collection and dissemination of consumer information.¹ Advances in technology have made it easier to compile information on our purchases and, partly because of the e-commerce explosion, there is more such information available.² Owners of consumer information databases grimly and efficiently collect this information, compiling it into comprehensive consumer profiles that are available for sale to corporations and direct marketers. With few exceptions, permission to divulge or use information is never asked; the data is collected, repackaged and sold as a matter of course. It is likely that consumer databases will become even more comprehensive because there is virtually no legal regulation of this practice, and the sale of consumer information often provides a new avenue of profits for retailers. Not surprisingly, many legal scholars have deemed these developments an unprecedented threat to privacy.³

This Article suggests that a focus on privacy in this context is insufficient. The real effects of consumer information gathering (CIG) are best framed as an exercise of power through surveillance. In other words, legal and scholarly attention must be directed to the broader effects of data collection, as opposed to isolated violations of individual privacy.

1. For example, in the past several years *Stanford Law Review* and the *Santa Clara Computer and High Technology Law Journal* presented symposia on privacy in the electronic age. See also Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1408 (2001); Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771 (1999). See also Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 293 (2001) ("Anonymity and the fear of 'Big Brother' tracking one's every move on the Internet have received significant attention from scholars.").

2. See, e.g., Kalinda Basho, Comment, *The Licensing of Our Personal Information: Is it a Solution to Internet Privacy?*, 88 CALIF. L. REV. 1507, 1507 (2000) ("Each day, businesses are collecting sensitive information about consumers' buying habits, occupations, income, families and product preferences."); Elizabeth deGrazia Blumenfeld, *Privacy Please: Will the Internet Industry Act to Protect Consumer Privacy Before the Government Steps In?*, 54 BUS. LAW. 349, 351 (1998).

[E]ach time a user clicks her mouse while on a web site, the potential exists for the company to record the location of her "click" and thus to collect information about her online behavior — where she goes, what she buys, when she buys, and how frequently she buys [T]he Internet's ability to collect such information allows for increasingly accurate and personally targeted marketing.

Id.

3. See generally *supra* note 1.

Part II of this Article traces the various factors that were essential to the rise of database marketing and suggests that no single factor was decisive in bringing about this new form of marketing. Rather, database marketing was made possible by a confluence of social, technological, and cultural influences. Part III frames CIG within the theoretical framework of surveillance, and argues that the techniques of CIG embody the principles behind so-called "new surveillance."

The effects of CIG are explored in Part IV, which posits that legal arguments that do not take into account social and cultural effects of CIG are inadequate. The legal discourse needs to conceptualize CIG broadly, not bound by particular legal doctrines, but rather by asking whether the effects of data collection on individuals justify its protection.⁴ To the extent that surveillance is an exercise of power, one should consider how it "reaches into the very grain of individuals, touches their bodies, and inserts itself into their actions and attitudes, their discourses, learning processes and everyday lives."⁵ Accordingly, this Article is concerned with the effects of CIG on society and on the slightest modifications it may cause in an individual's behavior, and not on isolated cases of violations of consumer privacy. The effects of CIG, as Part IV suggests, are varied and diffuse, ranging from a greater sense of vulnerability from the problems of reducing an individual to a set of data, to the troubling unintended consequences.

Part V of the Article highlights the distinctions between the privacy and the surveillance approaches to the problem and suggests some tentative solutions. Part V acknowledges that CIG may not, and should not, be eliminated. Rather, the nature of the practice should be altered to ensure a more equitable balance of power between the collectors of the information and the consumers.

II. THE HISTORY OF DIRECT MARKETING

Any social phenomenon is always the result of numerous overlapping influences and yet even then is more than the sum of its parts. Direct

4. See Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. (forthcoming July 2002) (advocating a pragmatic, context-specific approach to privacy problems). See also Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 783 (1989) (arguing that the constitutional right to privacy should be construed according to "the real effects that conformity with the law produces at the level of everyday lives and social practices.").

5. Michel Foucault, *Prison Talk*, in POWER/KNOWLEDGE 39 (1980).

marketing,⁶ in its current form, is no exception. It is the product of such factors as: a) sophisticated database technology; b) virtual lack of consumer information protection in the United States; c) shifts in the “marketing imagination” from the mass to the individual consumer; and d) expressive meaning of consumption in our society. Emerging from these diverse influences, direct marketing has become a pervasive presence in our lives: the bulk of our mail consists of correspondence based on consumer database information. This section explains how various social and cultural factors contributed to the rise of direct marketing in the United States.⁷

A. *From the Mass to the Individual Consumer*

The relationship between merchants and consumers has gone through several distinct stages. In the days of small-scale neighborhood stores, the relationship was often personal. The proprietors of neighborhood stores often intimately knew the community they were serving and could easily make recommendations based on prior purchases and lifestyles of customers. However, with the urbanization, mass production, and proliferation of department stores in the early Twentieth Century, methods of marketing changed radically.⁸ Mass production led to volume buying and mass media advertising. Sellers no longer knew their consumers because their products were offered to the mass market, as opposed to a familiar community.⁹

However, toward the Mid-Twentieth Century, corporations shifted their attention from the mass to the individual consumer.¹⁰ In the 1950s, marketing research revealed that different ethnic and socioeconomic

6. Database marketing is a form of direct marketing. Because contemporary direct marketing is highly dependent on database technology, this Article will employ these two terms interchangeably.

7. Although direct marketing exists in other countries, strong privacy protection of personal information tends to decrease the profit margin of this practice. The lack of comparable privacy legislation in the United States allows for greater use of database marketing.

8. See MICHAEL SCHUDSON, *ADVERTISING, THE UNEASY PERSUASION: ITS DUBIOUS IMPACT ON THE AMERICAN SOCIETY* 80-82 (1984). For a comprehensive and provocative history of consumption in the United States, see *CONSUMER SOCIETY IN AMERICAN HISTORY: A READER* (Lawrence B. Glickman ed., 1999). See also *THE CONSUMER SOCIETY READER* (Juliet Schor & Douglas Holt eds., 2000) (providing a more theoretical overview of consumption).

9. See SUSAN STRASSER, *SATISFACTION GUARANTEED: THE MAKING OF THE AMERICAN MASS MARKET* 5-7 (1995).

10. See Solove, *supra* note 1; see also DAVID LYON, *SURVEILLANCE SOCIETY: MONITORING EVERYDAY LIFE* 43 (Open University Press 2001) (“rather than producing for an uncertain market, companies now attempt to customize, to personalize . . . what was once a matter of mass production and mass merchandising is now increasingly individualized.”).

groups responded differently to advertising stimuli. Marketers started employing strategies that were based on psychological and sociological research into the factors that motivate consumers to make a purchase.¹¹ The goal was no longer to get everyone to buy your product — an impossible objective — but to appeal to those consumers most likely to respond.¹² The initial approach was simple: place ads on television or radio shows or with specific magazines that appeal to particular groups deemed the most desirable audience.¹³ This technique was, in essence, mass marketing on a slightly more targeted basis.¹⁴ Marketers needed the power of database technology for personalized marketing to work.

B. Database Technology and Aggregation of Personal Data

Without advances in database technology, which allowed for the storage and sorting of huge amounts of data, database marketing as we know it today would be impossible.¹⁵ Before pre-sorting, direct solicitation of consumers consisted of the indiscriminate mailing of mail-order catalogues, even though some consumers were more likely to respond to such solicitations than others. The lack of technology to sort and assess this data prevented companies from analyzing these differences.

Consequently, “direct marketing remained a fledgling practice and fringe form of marketing for most of the twentieth century.”¹⁶ With the vast majority of solicitations ineffective, direct marketing was a relatively unprofitable endeavor. To increase the low response rate, the lists of solicitation recipients had to be extensively sorted in order to produce

11. See RICHARD C. MADDOCK & RICHARD L. FULTON, *MARKETING TO THE MIND* 9-12 (1996). See also WILLIAM LEISS ET AL., *SOCIAL COMMUNICATION IN ADVERTISING* 291 (2d ed. 1990) (emotional advertising emphasized “the imagistic associations between the product and what is known about individuals and their expectations in life, including their feelings about status, peer-group influence, roles, [and] social mobility . . .”). For an early study of the connection between personality and responsiveness to advertising, see Vance Packard, *THE HIDDEN PERSUADERS* (1957) (describing how advertisers employ the unconscious desires and neurotic complexes of the individual consumer to form a nearly libidinal attachment to a product.). However, the validity of Packard’s conclusions has been disputed. See GUY COOK, *THE DISCOURSE OF ADVERTISING* 208 (2d ed. 2001).

12. See generally CHESTER A. SWENSON, *SELLING TO A SEGMENTED MARKET: THE LIFESTYLE APPROACH* xvi (1990).

13. *Id.*

14. Solove, *supra* note 1, at 1404-05.

15. See Leslie A. Kurtz, *The Invisible Becomes Manifest: Information Privacy in a Digital Age*, 38 *WASHBURN L.J.* 151, 152 (1998) (“Information has long been a commodity, and mailing lists have been bought and sold. But today, it is far easier to generate, organize and deliver this information.”).

16. See ARTHUR M. HUGHES, *THE COMPLETE DATABASE MARKETER* 51 (2d ed. 1996).

names of the most promising prospects. This required more consumer research and was an effective way to collect, store, and analyze information about consumers.¹⁷ The introduction of the computer database gave marketers this ability.¹⁸

As Professor Solove noted, “[T]he database enabled marketers to sort by various types of information and to rank or select various groups of individuals from its master list of customers — a practice called ‘modeling.’”¹⁹ Marketers also studied the profiles of the most profitable customers, and used the gleaned information to search for consumers with similar characteristics.²⁰

At first, marketers looked for particular characteristics, such as recent purchases of certain products, or frequently purchased products. The implementation of the zip code system in 1967 enabled direct marketing to target to those zip codes with the highest response rates.²¹ This marketing strategy, however, was only marginally effective because the company could utilize only its own internal data. To increase the effectiveness of targeted mailings, companies turned to each other to purchase and share their consumer information. Soon, entire companies specializing in consumer information databases emerged.²² The lack of comprehensive privacy laws, and the easy availability and low cost of consumer data greatly contributed to the rise of data collection and direct marketing.

C. Lack of Privacy Protection

The lack of comprehensive legislation protecting personal informational privacy in the United States made database marketing possible.²³ Consumer privacy rights in the United States are protected through a loose patchwork of constitutional, statutory and common law, as well as private sector self-regulation, that does not encompass all or

17. Solove, *supra* note 1, at 1405.

18. *See id.*

19. *Id.*

20. *See* HUGHES, *supra* note 16, at 267-68.

21. *See* DICK SHAVER, *THE NEXT STEP IN DATABASE MARKETING: CONSUMER GUIDED MARKETING: PRIVACY TO YOUR CUSTOMERS, RECORD PROFITS FOR YOU* 27 (1996).

22. *See* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 *SAN DIEGO L. REV.* 1153, 1162 (1997) (observing that currently there are over five hundred companies specializing in selling of consumer information).

23. *See* A. Michael Froomkin, *Cyberspace and Privacy: A New Legal Paradigm? The Death of Privacy?*, 52 *STAN. L. REV.* 1461, 1462 (2000) (quoting Scott McNealy, the CEO of Sun Microsystems, Inc. as saying “You have zero privacy. Get over it.”).

even most data collection practices.²⁴ For example, the Fair Credit Reporting Act (FCRA)²⁵ limited the purposes for which personal information may be released without consent. Still, the FCRA's scope does not extend beyond credit-reporting companies, and the extent of its private remedies is limited.²⁶ Similarly, although the Cable Communications Policy Act of 1984²⁷ requires cable companies to provide annual notification and consent forms to subscribers regarding the use and disclosure of their personal information,²⁸ it affects only cable companies and lacks remedies against third parties that purchase and re-sell the information. Finally, the infamous "Bork law," a statute protecting video rental records, does not cover conceptually similar activities, such as records of purchasing books. In sum, although Congress enacted several other privacy statutes, no piece of legislation generally prohibits the collection and the sale of consumer information to third parties.

The lack of privacy protection legislation in America is even more conspicuous when we consider the European approach to the problem. The European privacy model solves many of the shortcomings of the contemporary American regime. In an effort to synchronize existing laws and protect informational privacy the European Union's Council of

24. See Joel Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 772 (1999) ("For years, the United States has relied on narrow, ad hoc legal rights enacted in response to particular scandals involving abusive information practices. The approach has led to incoherence and significant gaps in the protection of citizens' privacy."). See also Beth Givens, *Privacy Expectations In a High Tech World*, 16 COMPUTER & HIGH TECH. L.J. 347, 348 (2000) ("The United States has taken a sectoral approach to privacy, enacting laws that apply to specific industries and practices.").

There are also those that argue that technology, including that which may violate privacy, is always a step ahead of any common law or legislative response. See Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1322 (1992) (suggesting that technology has outpaced the ability of man to control it). See also David R. Johnson & David G. Post, *Law and Borders — The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1378-79 (1996) (arguing that many established legal principles are inapplicable in cyberspace, and that cyberspace as a place is separate from the real world). This conclusion is a tad rash. Although it is slow on the uptake, eventually the law catches up with technology. Consider, for example, the emergent body of law concerning exercise of personal jurisdiction on the Internet. See Andrew J. Grotto, *Due Process and In Rem Jurisdiction Under the Anti-Cybersquatting Consumer Protection Act*, 2 COLUM. SCI. & TECH. L. REV. 1, 2 (2001).

25. 15 U.S.C. § 1681 (2002).

26. See generally Sandra B. Petersen, Note, *Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?*, 48 FED. COMM. L.J. 163 (1995) (discussing some of the defects and omissions of FCRA).

27. P.L. 98-549, 98 Stat. 2779.

28. *Id.*

Ministers, in 1995, adopted an omnibus European Data Directive (EDD).²⁹ EDD imposes an obligation on European Union governments and private industries to collect and process data only for specified and legitimate purposes.³⁰ Importantly, the term "processing" encompasses collecting, recording, and making data available in any form, thus covering most activities that make database marketing possible in the United States.³¹ EDD also recognizes a property right in personal information, and requires contractual consent to the processing or collection of personal information.³² Finally, to ensure compliance, EDD also imposes considerable sanctions for violators, and establishes governmental agencies to oversee the implementation of the EDD and assure privacy protection.³³

The picture in the United States is considerably different. Not bound by consumer privacy legislation, "[a]n increasing number of companies with databases — magazines, credit card companies, stores, mail order catalog firms, and even telephone companies — are realizing that their databases are becoming one of their most valuable assets and are beginning to sell their data."³⁴ As the use of credit cards expanded during the 1970s and 1980s, credit card companies and credit reporting agencies, using loopholes in the FCRA, developed extensive personal information databases and started offering them for sale. Some credit reporting companies also offer investigative consumer reports that contain details about an individual's lifestyle.³⁵

29. See Council Directive 95/46/EC of July 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J.L. 281 [hereinafter Council Directive]. For a comparison of the online data policies, see Domingo R. Tan, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP. L.J. 661, 665 (1999).

30. Council Directive, *supra* note 29, art. 6, para. (1)(b).

31. *Id.* art. 2, para. (b).

32. *Id.* art. 7, para. (a)-(b).

33. *Id.* art. 12.

34. See Solove, *supra* note 1, at 1408. See also ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? FROM PRIVACY TO PUBLIC ACCESS 3-4 (1994).

A great deal of information we consider to be highly personal, and of interest to ourselves and the town gossip . . . is now being sold on the open market to anyone who believes he or she might be able to use such information to turn a profit. These transactions usually take place without our knowledge or consent.

Id.

35. See Solove *supra* note 1, at 1409 (citing BETH GIVENS, PRIVACY RIGHTS HANDBOOK: HOW TO TAKE CONTROL OF YOUR PERSONAL INFORMATION 83 (1997)).

Lack of privacy protection has also contributed to the creation of companies specializing in the collection and marketing of personal information. Catalina Marketing Corporation, for example, collects information from more than five thousand supermarkets and offers for sale databases containing consumption histories of over thirty million households.³⁶ Aristotle International, Inc. markets a database of voting records of over ninety percent of registered voters in America.³⁷ Winland Services owns a database of over 1000 elements, including behavioral data, on over 215 million Americans.³⁸ Collectively, these companies own data on virtually all American households.³⁹ When databases are combined, the breadth of personal information may be considerable. When two database companies, Doubleclick and Abacus, announced a merger, one of the executives proudly stated, "the goal is to have the most complete picture of the consumer you can."⁴⁰

Occasionally, grassroots efforts stop sales of personal information. For instance, in September of 1995, Marketry, Inc., started marketing a list of over two-hundred fifty thousand email addresses compiled from Internet newsgroups and web sites. The list was segmented into eleven interest categories, including pornography, sports, education, and religion. After this news was posted on a number of bulletin boards on the Internet, consumers protested, and after considerable adverse public reaction, the list was withdrawn. Similarly, in 1990, Lotus Development Corporation and Equifax announced plans to market a CD-ROM based on individual credit reports, making available names, addresses, and the purchasing

36. See Solove, *supra* note 1, at 1408.

37. See Aristotle International, Inc., available at <http://www.aristotle.com> (last visited July 3, 2002).

38. See *id.*

39. See HUGHES, *supra* note 16, at 354.

40. Quoted in Beth Givens, *Privacy Expectations in a High Tech World*, 16 *COMPUTER & HIGH TECH. L.J.* 347, 351-56 (2000). Consolidation of information databases may also happen through sales of consumer lists of defunct dot coms, a phenomenon more common in the current economic climate. Richard A. Beckmann, Comment, *Privacy Policies and Empty Promises: Closing the "Toysmart Loophole,"* 62 *U. PITT. L. REV.* 765 (2001). See also Andrew B. Buxbaum & Louis A. Curcio, *When You Can't Sell to Your Customers, Try Selling Your Customers (But Not Under the Bankruptcy Code)*, 8 *AM. BANKR. INST. L. REV.* 395 (2000) (arguing that under bankruptcy law privacy policies are enforceable); Marjorie Chertok & Warren E. Agin, *Restart.com: Identifying, Securing and Maximizing the Liquidation Value of Cyber-Assets in Bankruptcy Proceedings*, 8 *AM. BANKR. INST. L. REV.* 255, 300 (2000) (discussing how the sale of customer lists during bankruptcy proceedings may be stopped by federal agencies). Cf. Hal F. Morris & Flora A. Fearon, *Texas Attorney General: Privacy Is Not for Sale*, *AM. BANKR. INST. L.J.* (Oct. 2000) (describing the conflict between the privacy rights of consumers and the interests of creditors).

habits of individuals. However, these plans were scrapped after Lotus received over thirty thousand complaints.

Still, these are fairly isolated incidents, prompted by wide-spread negative publicity.⁴¹ Most of the time, data is sold or made available without the consumers ever finding out. This lack of publicity, along with a virtual absence of consumer protection legislation, makes possible compilation of databases containing comprehensive information on virtually every American consumer.

D. Expressiveness of Personal Consumption⁴²

Consumer history databases would be less useful if they did not provide an insight into the personalities and consequently purchasing tendencies, of consumers. An aggregation of isolated transaction records often amount to a personality profile that can be used to predict consumption patterns.⁴³ One of the loci of privacy in consumer information is in the expressiveness of consumer behavior itself.⁴⁴ What consumers buy is how they present themselves to the outside world. Therefore, what consumers buy is, to a large extent, who they are.⁴⁵ Consequently, the act of choosing one product over another is an

41. See LYON, *supra* note 10, at 135. "Negative responses to the colossal growth of surveillance over the past twenty years are minimal and frequently ad hoc." *Id.* For a brief but insightful examination of this phenomenon, see *id.* at 135-40.

42. I discuss the ideas presented in this section in greater length in *Privacy, Identity, Databases* (work in progress, on file with author).

43. This idea is, of course, too complicated to discuss fully in an Article of such limited scope. (For example, we may buy products that express who we would like to be, as opposed to who we are. The self as expressed through such consumption is deceptive.) For insightful observations into the relationship between personal identity and framing of one's self for "public consumption," see ERVING GOFFMAN, *PRESENTATION OF SELF IN EVERYDAY LIFE* (1959). See also OSCAR WILDE, *THE PICTURE OF DORIAN GRAY* (1891) (vividly describing a growing chasm between the title character's physical appearance and private essence). Cf. OSCAR WILDE, *THE CRITIC AS ARTIST* (1891) ("Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth.").

For a more recent analysis of the relationship between products and identity, and authenticity versus representation, see DANIEL J. BOORSTIN, *THE IMAGE: A GUIDE TO PSEUDO-EVENTS IN AMERICA* (1961). For a brilliant cultural and intellectual history of what it means to be true to oneself, see LIONEL TRILLING, *SINCERITY AND AUTHENTICITY* (1971).

44. See ERNEST STERNBERG, *THE ECONOMY OF ICONS: HOW BUSINESS MANUFACTURES MEANING* (1999) ("Inside and outside the store and the mall, . . . products appeal through the figurative meanings they express . . . capitalism is burgeoning from the calculated production of meanings.").

45. See Ronald K.L. Collins & David M. Skover, *Commerce and Communication*, 71 TEX. L. REV. 697, 698 (1993) ("[advertising] messages are more than solicitations to buy — they are the codes of our culture . . . we are largely the sum of what we buy.").

expressive one.⁴⁶ When consumers choose to purchase products of certain brands that are identified with a certain personality trait, for instance insecurity about body image or promiscuity, a sophisticated examiner of those brands may get a blurry, but strikingly accurate, glance at private lives. What is important here is not the record of our purchases, as some privacy theorists claim, but the inferences that an examiner may make about our preference of one brand over another. The choice of brands, and not the choice whether to buy a product or not, is what is expressive, revealing, and useful to marketers.

Without the nexus between identity and consumer behavior, sophisticated psychological profiling of consumers would be difficult to accomplish. However, armed with masses of consumer data and means to sort it out based on the personality of the consumer, direct marketing entered a new age: psychographics.

E. *The Effectiveness of Psychographics*

The effectiveness of direct marketing depends on the ability to produce a fairly accurate psychological profile that may be linked to a statistical likelihood of responding to a particular commercial solicitation. Historically, the use of demographic information to build a psychographic profile proved relatively inefficient. The early databases made assumptions about people based on demographics, such as age, income, race, ethnicity,

46. "Central to postmodern theory is the proposition that consumers no longer consume products for their material utilities but consume the symbolic meaning of those products as portrayed in their images." Richard Elliott, *Symbolic Meaning and Postmodern Consumer Culture*, in *RETHINKING MARKETING* 112 (1999).

Cultural theorists and belle lyrics have been more receptive to this line of reasoning than lawyers. For example, Madame Merle in Henry James' *The Portrait of a Lady* (1888) asserts:

[E]very human being has his shell and that you must take the shell into account There's no such thing as an isolated man or woman; we're each of us made up of some cluster of appurtenances. What shall we call our "self"? Where does it begin? where does it end? It overflows into everything that belongs to us — and then it flows back again [It] is one's expression of one's self; and one's house, one's furniture, one's garments, the books one reads, the company one keeps — these things are all expressive.

The notion of expressiveness of consumption is perhaps most true of fashion. As Quentin Crisp observed, "our clothes are too much a part of us for most of us to be indifferent to their condition: it is as though the fabric were indeed a natural extension of . . . the soul" (*quoted in* JOANNE ENTWISTLE, *THE FASHIONED BODY: FASHION, DRESS AND MODERN SOCIAL THEORY* 9 (2000)). In a more cynical mood Crisp added, "Fashion is what you adopt when you don't know who you are." See also ALISON LURIE, *THE LANGUAGE OF CLOTHES* (1981); FRED DAVIS, *FASHION, CULTURE, AND IDENTITY* (1994).

gender, and location, but could not look deeper into the file of the consumer to distinguish personality traits.⁴⁷

Dissatisfied with demographic information, marketers in the early 1980s turned to psychographics: data about psychological characteristics such as opinions, attitudes, beliefs, and lifestyles.⁴⁸ Although profiles created by psychographics are reductive, often missing the subtleties of our personalities, they have enabled marketers to target their solicitations even more accurately, thus ensuring a higher response rate.

David Shenk's book *Data Smog*⁴⁹ traces the history of targeted marketing to Claritas, the market research company.⁵⁰ In 1976, Claritas introduced the PRIZM database, a comprehensive analysis tool of considerable complexity and ability.⁵¹ The database was organized on a set of sophisticated algorithms designed to extract the statistically relevant similarities between demographic information and geographic location, thus enabling the segmentation of a nation into the sum of its consumption patterns.⁵² This was a considerable improvement over the primitive sorting abilities of early databases.

The links between consumer behavior, psychology, and socioeconomic status proved to be very popular and effective. For example, one company created a complex classification system, with such categories as "Blue Blood Estates," "Bohemian Mix," and "Shotguns and Pickups."⁵³ Another company created lists of groups including "Big-Spending Parents," "First Time Credit Card Holders," "Grown But Still At Home," "Hi-Tech Seniors," "Status Spenders," and "Waist Watchers." Each cluster included a description of a consumer's income, racial or ethnic background, political attitudes, and hobbies.⁵⁴ Analysis of the increasingly detailed⁵⁵

47. Shaun A. Sparks, *The Direct Marketing Model and Virtual Identity: Why the United States Should Not Create Legislative Controls On the Use of Online Consumer Personal Data*, 18 DICK. J. INT'L. L. 517, 517 (2000) ("In recent history, direct marketers have approached the selection of marketing prospects with relatively simple information about individual consumers.").

48. See Solove, *supra* note 1, at 1406-07.

49. DAVID SHENK, *DATA SMOG* (1997).

50. *Id.*

51. *Id.*

52. *Id.* at 115-16.

53. See generally MICHAEL J. WEISS, *THE CLUSTERING OF AMERICA* (1982).

54. See HUGHES, *supra* note 16, at 300.

55. Once you have some information, you need more information. In other words, marketers realize that if a dossier with twenty-five data fields provides some insight into consumer preferences of a person, they will want dossiers with fifty data fields to create a more precise profile; then you need seventy-five data fields to refine the profile, etc.

consumer information and making of ever more minute distinctions and sociocultural assumptions made marketing increasingly precise.⁵⁶

F. Direct Marketing Today

Database marketing is currently a highly promising form of marketing, growing at twice the rate of the U.S. Gross National Product.⁵⁷ A recent book argued, "The old paradigm, a system of mass production, mass media, and mass marketing, is being replaced by a totally new paradigm, a one to one economic system . . . characterized by customized production, individually addressable media, and 1:1 marketing . . ." ⁵⁸ This model is so novel that one commentator noted, "Database marketing is a fundamental philosophical change in the way that marketers approach consumers."⁵⁹ In other words, direct marketing is the synthesis of one-on-one persuasion and mass marketing. On the one hand, database marketing embraces the idyllic idea of targeting particular products to discrete individuals, by taking into account their perceived needs and preferences. On the other hand, database marketing is an inherently impersonal process,

56. The predictive power is uncanny. See Malcolm Gladwell, *The Science of Shopping*, NEW YORKER, Nov. 4, 1996. After taking a simple multiple choice test, Gladwell asked a marketer to predict what type of razor he uses:

The marketer riffed, brilliantly, and without a moment's hesitation. "If you used an electric razor, it would be a Braun," he began.

But, if not, you're probably shaving with Gillette, if only because there really isn't an Intellect safety-razor positioning out there. Schick and Bic are simply not logical choices for you, although I'm thinking, you're fairly young, and you've got that Relief Seeker side. It's possible you would use Bic because you don't like that all-American, overly confident masculine statement of Gillette . . . [b]ut then they've got the technological angle with the Gillette Sensor . . . I'm thinking Gillette. It's Gillette.

He was right, "I shave with Gillette — though I didn't even know that I do."

Id.

57. HUGHES, *supra* note 16 ("It is and will continue to be the hottest growth area in advertising for the foreseeable future.").

58. I.D. PEPPERS & M. ROGERS, *THE ONE TO ONE FUTURE* 4-5 (1993). See also Jennifer Bresnahan, *Personalization, Privacy, and the First Amendment: A Look at the Law and Policy Behind Electronic Databases*, 5 VA. J.L. & TECH. 8, 8 (2000) ("Personalization is the latest darling of the business world.").

59. Sparks, *supra* note 47, at 517.

with the consumer reduced to an address and a statistical figure representing the likelihood of purchasing the pitched product.⁶⁰

This conceptual innovation has proven to be highly successful. A 1996 study found that seventy-seven percent of American companies use direct marketing.⁶¹ One author commented, "Today it's hard to imagine an organization that doesn't use direct marketing in one form or another."⁶² The total amount spent on mailing lists is close to \$3 billion a year.⁶³ "Direct marketing sales to consumers reached \$630 billion in 1996, up from \$458 billion in 1991. Business to business sales were another \$540 billion in 1996, up from \$349 billion in 1991."⁶⁴ The Direct Marketing Association, the largest trade association for consumer information businesses, has more than 4700 member companies from the United States and fifty-three nations worldwide.⁶⁵ A recent study indicated that one of every thirteen jobs in the United States was the result of direct marketing sales activity. Overall, the industry employs more than eighteen million people.⁶⁶

60. The problem may even be more insidious. There is considerable likelihood of discrimination based on collected information. See OSCAR H. GANDY, JR., *THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION* 80-81 (1993) ("The panoptic sort, which depends on ready access to personal information . . . is . . . a discriminatory technology"). See also Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*, 1996 U. CHI. LEGAL F. 77, 78 ("Information about our status, choices, and communication behavior often forms the basis for differentiation, and such difference forms the basis for discrimination."). Cf. LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* 155 (1999) ("Economists will argue that in many contexts this ability to discriminate — in effect, to offer goods at different prices to different people — is overall a benefit . . . [b]ut these values are just one side of the equation. Weighed against them are the values of equality.").

Importantly, discrimination and other dangers discussed in this Article are not merely hypothetical. In one well-publicized case, when a consumer sued a supermarket, he was threatened with the courtroom disclosure of his shopping card records of alcohol purchases. See Ian Goldberg et al., *Symposium Trust Relationships Part 1 of 2: Trust, Ethics, and Privacy*, 81 B.U.L. REV. 407, 420 (2001); WEISS, *supra* note 53.

61. Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1047 (1999).

62. BOB STONE & RON JACOBS, *SUCCESSFUL DIRECT MARKETING METHODS* (7th Ed.) at 4.

63. See William J. Fenrich, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 956 (1996).

64. Seth Safier, *Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 VA. J.L. & TECH. 8 (2000).

65. See <http://www.the-dma.org/aboutdma/whatisthedma.shtml> (last visited May 3, 2002). The size and power of DMA has also influenced privacy legislation before Congress. "The DMA lobbying presence is powerful enough that the organization often works with bill sponsors to help them craft language that prevents the destruction of direct marketers' ability to define and reach specific markets." Craig Martin, *Mailing Lists, Mailboxes, and the Invasion of Privacy: Finding a Contractual Solution to a Transnational Problem*, 35 HOUS. L. REV. 801, 836 (1998).

66. Fenrich, *supra* note 63, at 956.

The Internet is extremely promising for marketing,⁶⁷ and we can already see some emerging trends.⁶⁸ First, the technical infrastructure of the Internet provides a much greater ability to aggregate and consolidate information. Second, the Internet has made it much easier to buy and sell that information. The scandal surrounding DoubleClick's plan to collect and sell Internet surfers' profiles is just a most prominent indication of the industry's expansion strategy.⁶⁹

This is an explosive time in the history of direct marketing.⁷⁰ As one marketer prognosticated, "The time will come when we are well known for our inclinations, our predilections, our proclivities and our wants. We will be classified, profiled, categorized, and our every click will be watched."⁷¹ There is no reason to believe that this vision will not come true.

III. CONSUMER DATABASES AS A FORM OF SURVEILLANCE

As Part II demonstrated, data collection has become an essential feature of many retail commercial transactions and is an invaluable part of the marketing strategies of major corporations. So far, most of the challenges to CIG have come from privacy advocates.⁷² Surveillance implications of this practice have not been thoroughly examined in legal literature, even though it is through that prism that the most socially significant effects of CIG become apparent.⁷³

It may seem odd to describe database marketing in terms of surveillance. After all, that term is intricately linked with notions of

67. "Two factors make the Internet particularly compatible with the database marketing model. First, the Internet presents marketers with the ability to examine consumer behavior at a never-before-realized level of granularity. Second, the Internet's inherent ability to minimize marketing and distribution costs is a powerful competitive advantage . . ." Sparks, *supra* note 47, at 527.

68. These trends have predictably raised serious privacy concerns. See Steven A. Hetcher, *The Emergence of Website Privacy Norms*, 7 MICH. TELECOMM. TECH. L. REV. 97 (2000/2001) ("There is a burgeoning privacy crisis due in large part to the explosive growth of the Internet.").

69. See *supra* notes 40-41 and accompanying text.

70. "Fueled by advances in computer and communications technology, modern database-driven businesses have become more sophisticated; the level of detail with which marketers examine individual customers has increased rapidly." Sparks, *supra* note 47, at 517-18.

71. JIM STERNE, WHAT MAKES PEOPLE CLICK 255 (1997).

72. See, e.g., Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000).

73. Arguably, surveillance may be framed as a type of privacy invasion. Still, it is important to keep the two principles distinct conceptually.

hegemonic power and social control.⁷⁴ It is counterintuitive to view a credit card purchase as similar to more invasive forms of surveillance such as wiretapping, call tracing, or Hitchcockian men in fedoras furtively glancing over tops of newspapers. Moreover, there is no sinister motive behind CIG. Database marketers are not trying to control consumers' behavior — unless we consider promotion of consumerism such an effort. Yet, cataloguing personal information shares characteristics, and has effects similar to, so-called “new surveillance.” This section examines how the psychological and social effects of database marketing mirror those of surveillance.

Before moving further, we must define surveillance, a seemingly unambiguous term. David Lyon defines it as “any collection and processing of personal data . . . for the purposes of influencing or managing those whose data have been garnered.”⁷⁵ This is as good a definition as any, since it establishes the necessary nexus between personal identity, information, and exercise of power. However, this definition applies equally to the kinds of surveillance practiced in the seventeenth and the twenty-first centuries, despite the qualitative differences between the two. Thus, it is further necessary to distinguish “new surveillance” from its predecessor.

The old model of surveillance focused on subjecting the individual to a frequent or constant observation. The gaze of the observer forced a change in the behavior of the observed. Surveillance was associated with the state and was closely related to the intricate process of refining categories of deviance. The most frequently described contexts of “old surveillance” are prisons, insane asylums, and public spaces.

On the other hand, “new surveillance,” as described by authors ranging from Michel Foucault to Stanley Cohen, is less invasive and more reliant on technology, but is equally capable of effecting significant psychological and behavioral changes in its subjects. The very possibility of an observing gaze produces changes in the behavior of the observed. In his well-known

74. See, e.g., GEORGE ORWELL, 1984 (1949). *But see*, Solove, *supra* note 1, (questioning the appropriateness of the Big Brother metaphor for contemporary surveillance practices). The pervasiveness of technologies with surveillance potential has brought about a sizable alarmist literature. See, e.g., CHARLES J. SYKES, THE END OF PRIVACY (1999); REG WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY (2000). *Cf.* DAVID BURNHAM, THE RISE OF THE COMPUTER STATE 151 (Random House, Inc. 1983) (“[E]ven highly educated people are prepared to grant the computer far more power than it actually possesses.”); for a more balanced view, see AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999). *See also* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (Philip E. Agre & Marc Rotenberg eds., 1997) (compiling a thorough and representative selection of articles on the subject).

75. LYON, *supra* note 10, at 2.

book *Discipline and Punish*,⁷⁶ Foucault argued that modernity allows for exercise of power not only by the state, but also by “multitudinous non-state sources.”⁷⁷ The power to surveil is diffused throughout society and includes observers as diverse as corporations, condominium boards, and shopping malls.⁷⁸ Thus, by becoming more available, surveillance became more pervasive and less overtly visible.⁷⁹ Incessant and dispersed collection of information is part and parcel of de-centralized “new surveillance.”⁸⁰

CIG parallels this trend of de-centralization, routinization, and automation of data collection.⁸¹ Indeed, information gathering is subsumed into the most routine activity of all: shopping. The act of swiping a Safeway card, thus releasing information about your brand preferences, is

76. MICHEL FOUCAULT, *DISCIPLINE AND PUNISH* (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1978).

77. *Id.* at 104-05. Foucault’s conception of power is quite complex. For instance, he asserted that liberation from overt repression works only to enmesh the subject deeper in the mechanism of power through a proliferation of specialized discourses. Often the agents of liberation themselves function as instruments of power. See, e.g., MICHEL FOUCAULT, *THE HISTORY OF SEXUALITY: VOLUME 1: AN INTRODUCTION* 93 (Robert Hurley trans., Pantheon Books 1990) (1978) (“Power is everywhere; not because it embraces everything, but because it comes from everywhere”). See also Amy Adler, *The Perverse Law of Child Pornography*, 101 COLUM. L. REV. 209, 268-69 (2001).

Power, as [Foucault] views it, resides not in the hands of the police or of a few government institutions; rather it is diffuse and pervasive, an immanent “bio-power” exercised on all by all. Power works only marginally through repression and prohibition; it exerts itself most strongly through tools of apparent liberation [O]ne way power spreads its grasp is through an “incitement to discourse.”

For further discussion of Foucault’s view of power, see *A CRITICAL READER* (David Couzens Hoy ed., 1986).

78. See Clifford D. Shearing & Philip C. Stenning, *From the Panopticon to Disneyworld: The Development of Discipline*, in *PERSPECTIVES IN CRIMINAL LAW* 347 (A. Doub & E. Greenspan eds., 1984).

79. See GARY T. MARX, *UNDERCOVER: POLICE SURVEILLANCE IN AMERICA* 3 (1988) (“The new forms of social control tend to be subtle, invisible, scattered and involuntary. They are often not defined as surveillance, and many people, especially those born after 1960, are barely conscious of them.”).

80. See Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560 (1995) (collection and processing of information “creates a potential for suppressing a capacity for free choice: the more that is known about an individual, the easier it is to force his obedience.”).

81. Julie E. Cohen, *Examined Lives: Informational Privacy as the Subject and Object*, 52 STAN L. REV. 1373, 1398 (2000) (arguing that in the consumer context each exchange of information is trivial and incremental which has a tendency to minimize its effect).

part of shopping at that supermarket. On the Internet, where every keystroke and cursor movement may be monitored, shopping is surveillance. Importantly, the consumer is often unaware whether information on a particular transaction has been collected. Even if this awareness exists, the consumer often may not completely opt out of CIG. While some transactions may be paid for in cash, a credit card is required to book a flight,⁸² rent a car, and get a video rental card. As more commerce moves to the internet,⁸³ the extent of CIG will grow because credit cards are the principal method of payment online.⁸⁴

As Part II suggested, the routineness of CIG stems from the relative inexpensiveness and availability of the technology that makes it possible.⁸⁵ Once a retailer makes an investment into a database, the cost of recording individual transactions is close to nil.⁸⁶ In cases of credit card companies, the cost per unit of data is actually zero. These companies' account statements containing purchase information are recorded in their databases in order to substantiate claims of fraud or mistake. The sale of transaction information contained in these statements is pure profit.

But these economies of scale are available to more than large credit card companies. Consonant with the principles of "new surveillance," CIG technology is widely available to small-scale retailers and other small businesses. For anyone with proper software, replication of data is as easy as a click of the mouse. Moreover, the data is as easy to send as it is to receive, and modern software capabilities make it fairly easy to store, organize, and analyze.

This ease of data storage and management has produced further parallels between CIG and "new surveillance." Technology has made it possible for the data analyst to be miles away from the location where the data was collected. The remoteness is not only spatial, but also temporal, since transaction records may remain in databases for years before they are analyzed.⁸⁷

82. In fact, paying for a plane ticket in cash is considered a security red flag, and often subjects the flyer to delays or invasive searches.

83. See Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1222-23 (1998) (predicting that computers will soon facilitate many of the commercial transactions currently performed in the physical world).

84. Jerry Berman & Deirdre Mulligan, *The Internet and the Law: Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 551, 562 (1999) ("Most online purchases are made with credit cards, which identify the individual and facilitate the collection of purchasing data.").

85. See Kurtz, *supra* note 15 and accompanying text.

86. *Id.*

87. However, as Part IV explains, just like other methods of new surveillance, CIG has effects on behavior whether or not the data is ever analyzed.

Also congruent with the principles of "new surveillance" is the devolution of ethical responsibility for both the fact and the consequences of data collection. Surveillance via CIG often raises so few ethical concerns precisely because it is so widespread and routine. This, of course, presents a chicken and egg problem: ethical concerns are few because CIG is so routine; CIG is so routine because it has not been challenged with ethical concerns.

Importantly, ethical challenges to CIG are particularly difficult because human beings, with their morals and scruples, are virtually absent from the process. The transaction data is collected, organized, and analyzed according to automated principles and algorithms. Apart from the initial decision whether to collect data at all, the only human decision is whether to sell it. However, just as it is important for companies to collect data to keep up with the direct marketing capabilities of competitors, it is equally important for them to sell it, thus realizing avenues of profit utilized by most other companies. The decision not to sell consumer information to marketers comes at a cost, and since there are very few laws regulating personal data and public outcries over such sales are rare, it is made rather infrequently.

Finally, ethical self-regulation over the sale of data to database marketers is virtually absent because the disagreeable actions (annoying phone calls, psychological profiling, etc.) are often performed by third parties and not the sellers themselves. In other words, the data users and analyzers are often remote in space and time from the data collectors, thus complicating the assignment of ethical responsibility.⁸⁸

To sum up, information merchants collect data on the vast majority of Americans. Data collection is embedded in routine activities and is accepted as a given. Although certainly not every single commercial transaction is recorded,⁸⁹ a large percentage is. Even if a particular transaction is not recorded, the possibility of data collection has the same effect as if it were. In other words, if data collection were suspended,

88. The assertions made in this paragraph are supported by a recent study which concluded that organizations tend to be reactive rather than proactive on privacy issues, concluding that "most executives wait until an external threat forces them to consider their privacy policies." H. JEFF SMITH, *MANAGING PRIVACY* 93 (1994). The study quotes an executive at an insurance company as saying "[W]e've been lazy on the privacy [issues] for several years now, because we haven't had anybody beating us over the head about them." *Id.* at 67.

89. Obviously cash purchases made without the use of discount cards fall outside of the purview of the surveilling gaze. Yet, this exception is not as significant as it may seem. Large purchases are mostly made with credit cards, and a large percentage of stores employ discount cards. Furthermore, the data on all e-commerce transactions is recorded.

consumers would not even notice because data collection is the default social practice. The effect is panoptic: the subject of surveillance need not be actually observed for him to behave as if he were.

IV. THE EFFECTS OF CONSUMER INFORMATION GATHERING

As with any complex social phenomenon, the effects of CIG range from obvious to barely perceptible. This section suggests that these effects are akin to those of surveillance, if that term is defined as the collection of information with the effect of exercising power over the individual.

A. Loss of Control Over Information

One of the most important effects of CIG is that it denies consumers the ability to control the flow of information about themselves. The inability to control one's personal information, specifically the lack of control over how the information is gathered and disseminated, contributes to the overriding feeling of vulnerability.⁹⁰ As Jeffrey Reiman observes, "Those who lose [the] ability and authority [to withhold personal information from others] are thereby told that they don't belong to themselves; they are specimens belonging to those who would investigate them."⁹¹

The proliferation of databases, records, and documents make the individual an object of unseen computerized bureaucracy. Although computerization has made businesses more efficient, this efficiency comes at a price. There are well-publicized cases of computer slip-ups resulting in the denial of a job offer, a higher insurance premium, or a bad credit rating. But more importantly, the real feeling of powerlessness comes not from slip-ups, but from databases normal functioning and the consumer's inability to opt out of the CIG system.⁹² For example, it is virtually impossible to refrain from using credit cards, although doing so implicates

90. As Lawrence Lessig argues "Data is collected but without your knowledge. Thus you cannot . . . choose whether you will participate in or consent to this surveillance . . . Nothing reveals whether you are being watched, so there is no real basis upon which to consent." Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 505 (1999).

91. Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 27, 39 (1995).

92. See generally GANDY, THE PANOPTIC SORT, *supra* note 60.

us in CIG.⁹³ Thus, the problem is not only that personal information is sold if you use credit cards, but also that it is very difficult to extricate yourself from that system and still retain a reasonable range of options as a consumer.

Fundamentally, this entanglement in a system of data collection is a threat to personal autonomy. While consumption is unavoidable in modern society, collection of information for marketing purposes functions as a coercive entanglement of the individual in a consumerist discourse. Ongoing data collection stokes a marketing machine used to pitch an ever greater variety of products directly to the consumer. More pointedly, CIG diminishes the consumer's ability to lessen the presence of the consumerist discourse in his life. The constant barrage of direct mail, telemarketing calls, and personalized advertising, impresses upon the individual that the primary role is as a consumer, not as a citizen.⁹⁴ The white noise of consumption sets the background of the individual's life, thus subtly shaping his identity.⁹⁵ In this way, the loss of control over information facilitates the exercise of power upon the individual. Once a part of this discourse of consumption, it is impossible for the individual to withdraw.⁹⁶

93. *Dwyer v. Am. Express Co.*, 652 N.E.2d 1351, 1354 (Ill. App. 1995). *See also* *Tureen v. Equifax, Inc.*, 571 F.2d 411 (8th Cir. 1978) (holding information disseminated by a credit bureau is insufficient publication to support a claim for disclosure of private fact). *But see* *Virgil v. Time, Inc.*, 527 F.2d 1122, 1127 (9th Cir. 1975) (stating that a public disclosure of private facts is actionable even if the information was provided voluntarily by the plaintiff).

Yet, one Illinois court held, in rejecting a challenge to American Express selling transaction information,

By using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences. We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation.

Dwyer, 652 N.E.2d at 1354.

94. Rachel Bowlby, *Soft Sell: Marketing Rhetoric in Feminist Criticism*, in *THE SEX OF THINGS* 383 (Victoria De Grazia ed., 1996) ("In education, health, housing, . . . voting and many other fields, we are all addressed as 'consumers' now . . . The consumer is fast becoming the model of citizenship itself.").

95. *See id.* at 384 ("the discourse of marketing and consumption" is "dominant" in the discussion of identity/subjectivity formation). *See also* Karas, *supra* note 42 (discussing consumer identity in relation to culture and privacy law).

96. *See* GANDY, *THE PANOPTIC SORT*, *supra* note 60, at 2.

Although there are already some signs of resistance that have emerged in some quarters, the response of the panoptic system is very much like that of a child's

B. Retailing of Consumer Information: Back to Old Surveillance

The retail sale of consumer dossiers is another exercise of power over individuals. Generally, database marketers work from the particular to the general, using distinct bits of data to construct a consumer profile for marketing purposes. Yet, there may well be a retail market for the profile of a particular individual. Currently, web sites such as knowx.com⁹⁷ offer for sale records pertaining to bankruptcy, lawsuits, residences, voter registrations, credit headers, and other such information. These services merely give instantaneous access to information in the public record. But as more information gets compiled into databases, fairly complete consumer profiles may become available for purchase. For example, in a recent lawsuit MetroMail⁹⁸ was ordered to produce a number of consumer profiles that it compiled. One such profile "was twenty-five single-spaced pages and contained information such as her income, marital status, hobbies, medical ailments, her preferred brand of antacid tablets, whether she had dentures, and how often she had used room deodorizers, sleeping aids, and hemorrhoid remedies."⁹⁹ In the absence of comprehensive privacy protection legislation, there is no reason why such individual profiles will not become available for sale just as compilations of public information are.

This development would subject individuals to fairly invasive surveillance. The availability of such profiles may lead to a high tech form of peeking through the neighbor's blinds. The neighbor¹⁰⁰ will also be able to obtain information as private as what medications you have been taking, or as routine as your preferred brand of cereal. The impulse behind the purchase of such a dossier may be as simple as curiosity or as sinister as stalking. As David Brin suggests, "we [cannot] stop folks from constantly sifting, correlating, and drawing conclusions about their neighbors — even things that are 'none of their business.' That is because the underlying

straw finger puzzle: Once you have placed your fingers into either end of the tube the more you struggle to escape the more it tightens its grip.

Id. But see Karas, *supra* note 42 (arguing that the social discourse of consumption allows for a wide range of expressive identities).

97. Knowx.com, available at <http://www.knowx.com/> (last visited July 1, 2002).

98. Metromail is a service that offers for a fee, a complete marketing program, available at <http://www.metromail.co.uk/homepage.html> (last visited July 1, 2002).

99. Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century*, 27 WM. MITCHELL L. REV. 1457, 1473-74 (2001).

100. I am using a nosy neighbor as an example, but a consumer profile may also be purchased by an employer, a colleague, a friend, or an obsessed stalker.

impulse . . . is deeply rooted in human nature."¹⁰¹ So, ironically, at its zenith, the sophistication of database technology will allow us to rifle through someone's garbage without dirtying ourselves physically.

In other words, what is unique about the retailing of consumer profiles is that it harkens back to the world of old surveillance, when power over the individual was exercised in direct, perceptible ways. Whereas the impersonal, automated, diffuse "new surveillance" concerns itself with the mass, traditional surveillance, of which shopping list spying is a form, features a much closer relationship between the watcher and the watched. The only area of overlap here is that surveillance is available to anyone, not just the elites.¹⁰²

The effect of such consumer dossier surveillance is also more perceptible and personally invasive. Daniel Solove explored this distinction, albeit in a different context, when he stated that "[s]ince marketers generally are interested in aggregate data, they do not care about snooping into particular people's private lives This impersonality makes the surveillance less invasive."¹⁰³ Retail sales of consumer profiles, on the other hand, re-introduce the person as the observer. More importantly, they make the object of surveillance not an abstract consumer with a name and an address, but a full-fledged individual who is personally known to the observer.¹⁰⁴

Personal knowledge of the object of surveillance can have considerable negative effects. As Jeffrey Rosen noted, widespread access to personal data carries the risk of mistaking information for knowledge.¹⁰⁵ Unconnected bits of information collected in consumer profile invite interpretation, which may lead to dangerous consequences. For example, if a person's consumer profile lists frequent purchases of alcohol for a part-time catering business, her full-time employer may decide that the person has a secret drinking problem and deny her a promotion. Also, a colleague or neighbor might start a rumor about that person, using the purchased consumer profile as seemingly irrefutable proof. Bare facts lack the texture that make up a personality and when a purchaser of a consumer profile tries to fill in the gaps, the resulting portrait often will have little resemblance to the actual person. The retailing of personal dossiers

101. DAVID BRIN, *THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM?* 244 (1998).

102. *Id.*

103. Solove, *supra* note 1, at 1418.

104. Such personal knowledge is to be assumed; if not, how would the observer choose a person to observe?

105. JEFFREY ROSEN, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA* 223 (2000).

involves a deep plunge into a world of gossip, mistaken assumptions, and public perceptions having little to do with one's personality.¹⁰⁶ To avoid these consequences, people may alter their consumer habits — buying less alcohol, for example. In other words, retail sale of information unnecessarily entangles individuals in a discourse of power that leads to suspicion, alteration of behavior, and consequently, decrease in personal autonomy.

C. Dehumanizing Aspects of Database Marketing

The previous subsection noted that even observers familiar with the subject will inevitably make flawed assumptions. This danger is much greater when the personality of an individual is interpreted by a software program. These misinterpretations dehumanize consumers, alter the range of cultural signals available to them, and, most important, are an exercise of power, since they shape the view of the individual himself as merely a set of data devoid of humanity. Although this dehumanization may be a fundamental feature of modern life,¹⁰⁷ the trauma of personal realization of that fact is likely to have profound effects on the behavior of the person.

Before exploring these effects, however, one should consider how junk mail can affect a person. It is undeniable that the world view of an individual is highly influenced by exposure to cultural stimuli. These stimuli encompass advertising as well as television programs, printed material, and even imperceptible means. While an individual can choose which books to read or which television programs to watch, advertising chooses the individual. Although Americans are exposed to a tremendous volume of advertising, every person's advertising experience is different. As explained in Part II, ads seen on television or received in the mail are tailored to a demographic group with personal inclinations, as determined by psychographics. Importantly, we are moving to an ever more personalized advertising environment. Soon Internet advertisements will be based on browsing behavior and digital cable will allow advertisers to

106. Of course, one can argue that even if there were no mistaken assumptions, it is still no one's business what we purchase.

107. See generally GANDY, *THE PANOPTIC SORT*, *supra* note 60. Dehumanization is of course a cousin of alienation. Alienation, to use one of many definitions, is "the sense of one's own weightlessness and ineffectuality and of the strangeness and impermeability of the social world." William H. Simon, *Ethics, Professionalism, and Meaningful Work*, 26 HOFSTRA L. REV. 445, 447 (1997). "Alienation a central theme of art and literature, has spread from intellectuals to the general population." George W. Dent, Jr., *Secularism and the Supreme Court*, 1999 BYU L. REV. 1, 40. For a recent sociological treatment of the subject, see ROBERT PUTNAM, *BOWLING ALONE: THE COLLAPSE AND REVIVAL OF AMERICAN COMMUNITY* (2001); for a brilliant fictional treatment of the subject, see DANIEL CLOWES, *GHOST WORLD* (ed. 2001).

beam personalized commercials to every set instead of broadcasting them to a wide audience. The cumulative impact of these innumerable tiny cultural stimuli contributes to the world view of an individual. To the extent that consumers accept this imposition, they need to be concerned about whether the stimuli received are misaddressed, thus creating a rather skewed personal world view.¹⁰⁸

When marketers sort and model consumer information in order to arrive at a list of the most promising prospects, they are bound to make mistakes and misaddress advertisements. Database marketers are forced to assume that a person is a compilation of facts, such as income, consumer patterns, and hobbies. However, "the information in databases often fails to capture the texture of our lives. Rather than provide a nuanced portrait of our personalities, they capture the stereotypes and the brute facts of what we do without the reasons."¹⁰⁹ Accordingly, advertisers will often send mistaken personalized solicitations. Returning to the example of the part-time caterer. A programmer may create a database algorithm based on a series of assumptions about individuals that purchase large amounts of alcohol. Once 'someone' or 'a person' is included in this group, she may start receiving mail from Alcoholics Anonymous, swingers clubs, and New Age self-help groups. As mentioned previously, given the trend toward pinpoint, personalized advertising, these kinds of solicitations will also appear on her web browser and her television.

Furthermore, once a profile is formed and sold, there is no way of changing it in accordance to the true personality of the consumer, and it is also incapable of developing along with the consumer. The bits of data sloughed off early in life continue to define the individual. In other words, a database marketing program sees the person and his purchasing habits as fixed, not fluid, as people actually are.¹¹⁰ So, if a person, in her early twenties, exhibited a tendency to splurge on expensive vacations and pricey trinkets, before settling down with a family some years later, her mailbox will continue to bulge with offers from Bulgari and Air France instead of home loan applications in which she might be interested. Eventually, as databases are updated with that person's most recent purchases reflecting her new interests, she might be reclassified into a different target group, but for several years and perhaps forever, the

108. Consider, for instance, black consumers bombarded with all-white advertising or senior citizens deluged with ads catering to the urban youth.

109. Solove, *supra* note 1, at 1425.

110. See Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 25 (1992) (noting that the persona composed of bits of recorded information "achieves more credence than the individual").

market will see her as the person she used to be, not who she is now. Her advertising experience will be addressed to a person that she no longer is or perhaps has never been.

Certainly, these misaddressed advertisements may affect one's worldview. But beneath that predicament, a larger issue emerges: What are the effects of being perceived merely as a set of data? This issue goes beyond database marketing. An unseen insurance clerk, for example, can access the vast field of legally available personal information, sum you up in a glance, and use that instant profile to make a decision. Similarly, your college may vary the tone of the fund-raising letter based on your major or graduation year. This profiling eliminates not only human error, but any distinctive humanity from the process. No information ever disappears or is forgotten and the applicant is judged by isolated bits of data stored on a distant hard drive.

Consumers may be inured to market segmentation in marketing, to personalized ads that market to a psychographic category, and not to the individual. This standardization is inevitable in mass society. Yet, database marketing goes a step further. It allows for marketing to consumers as members of a group to which they do not belong. The marketer's mistakes make the consumer realize that the solicitations sent do not illustrate the advertiser's interest in the consumer's well-being.¹¹¹ Thus, generally, a consumer may be flattered or intrigued by personalized messages from his car dealer, HMO, or alma mater. Misaddressed targeted solicitations, however, make the consumer see himself as a faceless set of data in the database society. As Jeffrey Rosen rightly observed, "In a world of pervasive surveillance, inaccurate rather than accurate profiling could be considered highly offensive to a reasonable person."¹¹² To the extent that individuals respond to others' perception of them, consumers exposed to such misaddressed advertisements are likely to experience an ever-greater sense of alienation.

111. See Eric Jorstad, *The Privacy Paradox*, 27 WM. MITCHELL L. REV. 1503, 1510 (2001) ("When it comes to a small-town hardware store, you feel good getting a call from the owner at home telling you about a new shipment of innovative products helpful to your farm, home, or business. But 'telemarketing' by impersonal behemoths or computer-generated voices is hardly a feel-good enterprise.").

112. Jeffrey Rosen, *Symposium: The Unwanted Gaze*, By Jeffrey Rosen: *The Purposes of Privacy: A Response*, 89 GEO. L.J. 2117, 2122-23 (2001).

D. Panoptic Effects of Consumer Information Gathering

Perhaps the most significant effects of CIG are the least perceptible. Even if individuals will not necessarily act differently if they know or suspect that data is being collected, their thought processes will be altered fundamentally.¹¹³ Foucault argued that diffuse surveillance internalizes the external exercise of power; the individual monitors his behavior as if under constant surveillance until the surveilled self becomes the true self. Surveillance, as Jerry Kang concurred, interferes with free choice because observation “brings one to a new consciousness of oneself, as something seen through another’s eyes,” which leads to self-censorship.¹¹⁴ Not only does surveillance affect the way that one looks within himself, it alters how he perceives the world around him. Accordingly, surveillance, no matter how diffuse, is best viewed as an exercise of power, a threat to selfhood.

The primary panoptic effect of CIG is the transformation of consumption from a private activity to a public one. Essentially, consumption is the taking of an object from a public store shelf into your home, into the ultimate private realm.¹¹⁵ Once that object is in your home, only a limited circle of people know of your ownership of it. Recording of consumer transactions attaches a trail of potential publicness to every purchased object. With CIG, the information about the object’s ownership belongs to the merchant, and in time, owners of countless consumer information databases. The result is that a record of much of what is in your house is available for purchase. Where once the home was one’s castle, now that castle has glass walls. The sense that one’s consumption is being observed and documented leads to panoptic effects.

Importantly, these effects take place whether or not the collected data is ever analyzed. The mere fact that this data is collected at least occasionally and that the individual is unable to shield himself from that process, gives rise to panoptic effects. In fact, it does not even matter if a particular merchant collects data or not, the notion that any merchant may legally do so without informing the consumer is enough to trigger panoptic effects.

113. *Id.* at 2124 (“To be observed out of context in private spaces — on the basis of complete or incomplete information — transforms the self from subject to object; and uncertainty about pervasive surveillance makes the development of the subjective self impossible.”).

114. Kang, *supra* note 83, at 1260-61.

115. There is extensive legal literature on the sanctity of one’s dwelling. *See, e.g.*, Payton v. New York, 445 U.S. 573, 601 (1980) (noting “the overriding respect for the sanctity of the home that has been embedded in our traditions since the origins of the Republic.”).

Admittedly, the increased self-consciousness about consumption may seem to have positive effects. For instance, people may refrain from buying pornography if that purchase will show up on their “permanent record.”¹¹⁶ Still, the use of CIG as a form of social control is deeply problematic. After all, pornography is legal and curtailment of legal rights, even through such subtle methods as self-censorship, impinges on the person’s autonomy.¹¹⁷ More importantly, minor acts of self-censorship may have substantial effects on the social fabric. As Foucault suggested, “surveillance changes the entire landscape in which people act, leading toward an internalization of social norms that soon is not even perceived as repressive.”¹¹⁸ Embracing easy availability of consumer information as a means of curbing undesirable consumption also implies relinquishment of privacy rights in personal information. Once that step is made, the idea that what you buy is nobody’s business, no longer seems so obvious and acceptance of data collection as a social norm makes it immune to ethical and legal challenges.

V. UNPACKING THE PROBLEM, EXPLORING THE OPTIONS

A. *Insufficiency of Privacy Law in Dealing with Aggregation of Personal Information*

The preceding discussion demonstrated that consumer information gathering has social implications that go beyond threats to personal privacy. These broader concerns are often ignored in the privacy-centered

116. Jed Rubenfeld, *The Right of Privacy and the Right to Be Treated as an Object*, 89 GEO. L.J. 2099, 2099 (2001) (“Millions of people, apparently, buy or look at pornography on the Internet every month, but we consider it tremendously embarrassing to admit this sort of thing in public.”).

117. Some scholars have argued that pornography presents a violation of women’s civil rights, and should be prohibited as such. See DRUCILLA CORNELL, *THE IMAGINARY DOMAIN, ABORTION, PORNOGRAPHY AND SEXUAL HARASSMENT* 155, 157 (1995) (observing that such scholars as Catherine MacKinnon view pornography as a form of anti-woman violence); *but see* Am. Booksellers Ass’n v. Hudnut, 771 F.2d 323 (1985) (holding that pornography qualifies as protected speech under the First Amendment to the U.S. Constitution); R.A.V. v. City of St. Paul, Minn., 505 U.S. 377 (1992) (invalidating a municipal ordinance that defined pornography as a civil rights violation because of a lack of evidence of demonstrable harm necessary for the ordinance to justify the overriding of First Amendment guarantees).

118. Solove, *supra* note 1, at 1418. See also Jeffrey Reiman, *Driving to the Panopticon, A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 COMPUTER & HIGH TECH. L.J. 27, 40 n.2 (1995) (“Total visibility infantilizes people. It impoverishes their inner life and makes them more vulnerable to oppression from without.”).

legal discourse. Single-minded reliance on privacy rights is unlikely to affect pervasive data collection and aggregation.

The resort to privacy is only natural. The ingrained American principles of individualism and self-determination lead to a "it's none of your business" rationale for protecting consumer information. If a man's home is his castle, the argument goes, it is no one's concern what products he brings into that castle. Accordingly, access to any information that the individual did not intentionally make public is a gross intrusion, an unwarranted attempt to appropriate that which is private. This approach is seemingly supported by the U.S. Supreme Court, which has defined privacy as "control over information concerning an individual's person."¹¹⁹ Similarly, Arthur Miller, a noted privacy scholar, asserted that "[t]he basic attribute of an effective right to privacy is the individual's ability to control the circulation of information relating to him."¹²⁰ This definition is rather broad, because it grants priority to individual control over information no matter how legitimate the reasons are for obtaining it.¹²¹ Yet, it seems apparent that controlling information about ourselves is integral to any conception of personal privacy.

Still, the individual rights focus in the privacy discourse is much too narrow. Of course, consumers may feel violated if information about certain potentially embarrassing purchases, such as pregnancy kits, adult diapers, or girdles, are disclosed to third parties. But most often CIG sweeps up information that is neither embarrassing nor unseemly.¹²² If you purchase a pair of Dockers, or a gallon of milk, and the retailer discloses transaction information to a third party, you may be disconcerted but probably not truly offended. The third party would know something about you, but that information is so impersonal that you are unlikely to feel that your privacy was invaded any more than if a passerby happened to see you wearing that pair of Dockers or drinking a glass of milk.¹²³

In these situations, the threat to privacy is not in an isolated act of collecting or disclosing information, but rather in the aggregate nature of the practice. Suppose that a person purchases a bottle of scotch and the record of the transaction is sold to a database marketer. Generally

119. U.S. Dep't of Justice v. Reporter's Comm'n, 489 U.S. 749, 763 (1989).

120. ARTHUR MILLER, ASSAULT ON PRIVACY 25 (1971). See also Randall P. Benzanson, *The Right to Privacy Revisited: Privacy, News, and Social Change, 1810-1990*, 80 CALIF. L. REV. 1133, 1135 (1992) ("I will advance a concept of privacy based on the *individual's* control of information.").

121. See Solove, *supra* note 4 (noting that the privacy as control over information theory at most says that we protect as private all information that individuals want to retain control over).

122. Kang, *supra* note 83.

123. See *id.* at 1198-99.

speaking, most privacy theorists would argue that the very fact that a third party may obtain information about your purchase is offensive. It is, the argument would go, nobody's business that you are a drinker of scotch. Yet, the act of purchasing that bottle of scotch is not truly private. After all, the purchase was made in a public place, with both the consumer and the product in plain view.¹²⁴ Indeed, if a newspaper chose to publish a photograph of the act it would not be liable for violation of privacy.

The real importance is in the pooling of these isolated consumer transactions into a comprehensive database. In a consumer records database, that particular purchase may be linked up with a myriad of others, all expressive of your personality.¹²⁵ In other words, with recording of isolated purchases, the threat to privacy is merely a pinprick. But when all of your consumer information is sold, rented, or bartered without your consent, the effect is more of a punch in the stomach.¹²⁶ This is the difference between someone glancing into your window and setting up a 24 hour a day videotaping post across from it. Both acts violate privacy on a basic level, but only the latter is truly invasive.

This distinction illustrates the insufficiency of privacy law to account for such aggregate harm. The difference between the peeping tom example and CIG is that in the former case the victim can identify the violator of her privacy. In the case of CIG because the harm is aggregate, no one defendant can be named. In other words, if your supermarket, pharmacist, and book store collect and sell bits of your personal information no single party is directly responsible for a harm that rises to the level of privacy violation. These dispersed bits of personal data are insignificant and unobjectionable, but their aggregation into a database amounts to a

124. For the sake of the argument, I am ignoring the possibility of buying products privately over the Internet or through an agent.

125. See Litman, *supra* note 72, at 1284 ("Anyone with reason to do so can correlate the information stored on one computer with the information stored on another, and another, and another."). On the issue of consumption being expressive of personality, see Karas, *supra* note 42.

126. See generally SIMON GARFINKEL, DATABASE NATION (O'Reilly Publishers 2000) (describing the feelings of frustration and vulnerability stemming from being immersed in an environment where personal consumer information is used for marketing).

violation and an act of surveillance.¹²⁷ Moreover, suing the database owners is unlikely to succeed because they are merely purchasing bits of information that in themselves are not strictly private.¹²⁸

Other strategies rooted in privacy law are equally likely to fail. First, where data collection is built into the very nature of the transaction or is part of the retailer's privacy policy, the customer is likely to be deemed to have willingly parted with the information.¹²⁹ Thus, disclosure of allegedly private information to a third party invalidates a privacy cause of action. Second, where the consumer's claim is based on a breach of the reasonable expectation of privacy, the court is likely to hold that CIG is so prevalent that such an expectation is unreasonable. Finally, any attempt to limit information gathering will run into First Amendment concerns.¹³⁰

It is also unlikely that the courts will step in with a privacy doctrine sufficiently broad and flexible enough to accommodate CIG. Many legal scholars argue that a Supreme Court endorsed constitutional right to privacy is an improper approach to technology based privacy threats.¹³¹ Perhaps state legislatures will be able to address this problem effectively,¹³² although that assumption has been questioned.¹³³ Even if such a broad information privacy right is established, its application to particular contexts of information collection is problematic, because the

127. That violation may not necessarily have a recourse in law. See George B. Trubow, *Protecting Informational Privacy in the Information Society*, 10 N. ILL. U. L. REV. 521, 537 (1990) (arguing that even a highly detailed profile is unlikely to be considered a "highly offensive" disclosure).

128. Of course, all personal information is private to the extent that one decides not to share it. Yet, pragmatically speaking, a supermarket shopping list is not private in the same way as a diary.

129. See, e.g., *Smith v. Maryland*, 442 U.S. 435 (1976) (parting with information destroys reasonable expectation of privacy). *United States v. Miller*, 425 U.S. 435 (1976) (individuals have no reasonable expectation of privacy in personal financial records maintained by the bank). See also *Dwyer v. Am. Express Co.*, 652 N.E.2d 1351, 1354 (Ill. App. 1995).

130. See Froomkin, *supra* note 23, at 1506-23 (discussing the clash between the First Amendment and privacy concerns); Eugene Volokh, *Freedom of Speech and Information Policy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (1999).

131. See, e.g., FRED H. CATE, *PRIVACY IN THE INFORMATION AGE* 66 (1997); Froomkin, *supra* note 23, at 1540-41. The U.S. Supreme Court has never accepted a constitutional right to informational privacy, but in *Whalen v. Roe*, 429 U.S. 589, 599 (1977) the Court did hold that there is an "individual interest in avoiding disclosure of personal matters." See also Kang, *supra* note 83, at 1230 n.157 (noting that the *Whalen* decision was the closest the Court has come to recognizing such a right).

132. See Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1431 (1992) (predicting that in the coming years the states will have to deal with cutting-edge privacy issues).

133. See CATE, *supra* note 131, at 68.

hundred years of the privacy discourse has not achieved consensus on the definition of "privacy."¹³⁴

Accordingly, one must look beyond privacy to assess fully the social and cultural effects of CIG. As Part IV illustrated, the primary effect of CIG is not offensive disclosure of private facts but rather a persistent and systematized exercise of power over individuals. In other words, the primary effect of data collection is not harm to a particular individual, the prospective plaintiff. Rather, it is the subtle change in the social fabric, in the way that people relate to each other. The feelings of vulnerability, dehumanization, and the self-censorship caused by data collection is the real injury, one that is not easy to translate into the language of an invasion of privacy lawsuit. The injury here is qualitatively different from those addressed by our privacy jurisprudence. Therefore, the terminology of surveillance, rather than privacy law, should become more prominent in the legal discourse on consumer information collection.

This does not mean, however, that legal scholars and practitioners should abandon privacy law in their discussion of CIG. Insights from both fields enhance each other and produce a more comprehensive and realistic approach to data collection. Framing the problem as one of surveillance may also assist the judges in looking beyond rigid doctrines of privacy. The aim here is to situate the problem of CIG in the zone of conceptual overlap between privacy law and Foucauldian sociology.

B. Options For Controlling Data Collection

It is remarkably easy to gaze deeply into one's navel and triumphantly extract therefrom a linty assortment of clever observations about the troubling implications of some social phenomenon. Coming up with solutions is considerably harder.

Much of this Article is concerned with the negative effects of consumer information gathering. Indeed, CIG results in loss of control, vulnerability, dehumanization, and infusion of panoptic power in the daily lives of people. These effects are rather disconcerting and should be subject to greater academic and general discussion.

On the other hand, CIG is a crucial feature of marketing in the United States. As Part II suggested, database marketing allows companies to communicate with consumers more efficiently, targeting them directly instead of relying exclusively on such expensive and scattershot marketing

134. Solove, *supra* note 4 (describing six major definitions of privacy and their variants). See also Gormley, *supra* note 132, at 1339 (arguing the legal right to privacy may not be satisfactorily articulated because "four or five different species of legal rights" have been promulgated under the label of privacy).

methods as television advertising. Indeed, personalization of advertising may be seen as a positive development, since it enables stronger relationships between producers and consumers.¹³⁵ For example, in the wake of the economic downturn related to the events of September 11, some upscale retailers in San Francisco used mailing lists to contact their customers, express their shock over the bombings and encourage them to ward off recession by patronizing their stores. An owner of a clothing store commented, "Many customers have shopped with us for a long time, and it seemed that under the circumstances we needed to communicate with those people."¹³⁶ Without CIG, these kinds of communications would not be possible.

Also, not only would limiting or eliminating CIG make marketing less efficient, but it would stifle a thriving database marketing industry which employs millions of Americans. Moreover, CIG is not only a boon for corporate America, consumers also benefit from the lowered search costs when sent direct solicitations ranging from credit card applications to magazine subscription forms to political fund-raising letters. Furthermore, analyzing consumer information allows companies to modify their products and services to respond to the market's demands.¹³⁷

In other words, we are faced with a conflict: CIG triggers disconcerting psychological and social effects, yet is economically useful. Outright abolition is therefore not a viable option.¹³⁸ The correct approach would preserve the essential features of CIG while minimizing the harms to consumers. Below are several suggestions for accomplishing this goal.

Much may be accomplished by adopting an opt-in model for collection of consumer information. Giving consumers the option to control the flow of personal information would help those who feel helpless to resist ubiquitous data collection. Admittedly, because of transaction costs and incomplete information many, if not most, consumers will sign away their

135. See George Raine, *Retailers Want You*, S.F. CHRON., Nov. 2, 2001, at B1; cf. Jorstad, *supra* note 111, at 1510 ("Customer profiling is the mass market's attempt to simulate the personal attention of a business that is known, liked, and trusted.").

136. Raine, *supra* note 135, at B3.

137. That is especially true of online shopping. For instance, Amazon.com uses past purchases and expressed preferences of customers to suggest other products they may be interested in. This approach pays off if the customer finds a lost gem of a book. The downside is that every purchase contributes to one's profile. A few months ago, I bought a gag gift for a friend. Now, Amazon consistently recommends to me various lewd and provocative films, books, and music.

138. Importantly, prohibition of CIG by Congress cannot eliminate the existing databases. Given the inexpensiveness of database technology and the ease of copying of data, these databases may still be employed after such a prohibition, with the same harmful effect as detailed in Part IV of this Article. See also Froomkin, *supra* note 23, at 1469 ("Once created or collected, data is . . . hard to eradicate; the data genie does not go willingly, if ever, back into the bottle.").

privacy as a matter of course.¹³⁹ Nonetheless, the very presence of an option to refuse information collection has inherent value, and would allow individuals to control the circulation of their personal information. Even if merchants choose to charge more of customers who decline to release their information, these privacy-minded customers will no longer feel as vulnerable.¹⁴⁰ Accordingly, in these cases the exercise of power through surveillance will be greatly diminished.

Another option is taxation of information sales with proceeds to benefit consumer organizations. Currently there are no separate taxes on inter-company sales of consumer information. Taxation of these transactions would produce a fund to sponsor prosecution of consumer fraud or of retailers that violate their own privacy policies. This approach would not affect the social effects of CIG, but it does recognize CIG as a kind of group harm. Under this approach, the affected group, consumers, would get at least indirect benefits from the utilizers of their personal information.¹⁴¹

Finally, a particularly effective method of counteracting surveillance effects of CIG is prohibiting retail sales of personal information. While database marketing is a valuable marketing tool, there are no comparable policy rationales for retail sales of consumer profiles. Given dangers of misinterpretation of information contained in such profiles (especially in the workplace context) this practice should be pre-emptively banned.

Inevitably, these suggestions are subject to objections and qualifications. Giving them full attention is beyond the scope of this Article. The proposals above are tentative ideas, not full-fledged policy agendas. In other words, this section merely presents a framework for thinking about regulating database marketing.

139. See Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 821-28 (2000). See also Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 49 (1997) (observing that most medical patients regularly sign broad releases of disclosures of medical data without truly comprehending the implications of their action).

140. The idea of individuals licensing or selling their personal information, thus receiving a concrete benefit from CIG, has received some prominence. See Jessica Litman, *supra* note 72, at 1287 ("The proposal that has been generating the most buzz, recently, is the idea that privacy can be cast as a property right."); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1132 (2000) ("In recent years, a number of economists and legal commentators have argued that the law ought now to grant individuals property rights in their personal data.").

141. For a discussion of this approach in cases of distributing a damage fund in consumer litigation, see Stan Karas, *The Role of Fluid Recovery in Consumer Protection Litigation*, 90 CALIF. L. REV. 959 (2002).

VI. CONCLUSION

Individuals produce a great volume of data about themselves every single day. Much of this data is collected and stored, largely for marketing purposes. Framing this phenomenon as merely a privacy issue misses its larger social implications. The greatest harm to individuals from data collection is not disclosure of private information, but rather systematic exercise of power over them. The best, although not ideal, way to describe this exercise of power is surveillance. The effects of this surveillance are wide-ranging and complex. Individuals subjected to it, through consumer information collection, are prone to exhibit self-censorship in their consumer habits, to feel dehumanized by the process, and to experience a general loss of control over their personal information. Although the two concepts are related, it is not privacy that is violated, but individual autonomy and dignity. In other words, data collection changes the relationship between individual and society.

As with most complex social problems, the debate over CIG comes down to balancing discrete and contradictory policy interests. On the one hand, CIG has many troubling effects on individuals. On the other hand, database marketing is a revolutionary concept that allows more meaningful relationships between producers and consumers. It is also a large industry, the abolition of which would leave millions of Americans jobless. Even if we perceive CIG as a form of "new surveillance," that does not mean that it should be eradicated. Not all modes of "new surveillance" should be abolished — we do not want to do away with security cameras, or "smart cards," for example.

Yet, a compromise solution reconciling these interests is not impossible. The challenge is to maximize the utility of CIG, while minimizing its deleterious social effects. By modifying the methods of data collection, this goal may be accomplished. No compromise solution is ever ideal and as long as CIG exists it will exercise power over individuals. However, even a slight tilt of the scale in favor of the consumers, should be considered substantial progress.

