The Purloined Personality: Consumer Profiling in Financial Services*

TABLE OF CONTENTS

* J.D. Candidate 2003, University of San Diego School of Law.

The author wishes to thank Professor Robert C. Fellmeth of the University of San Diego School of Law for his wise guidance and direction in the preparation of this Comment; Andrew Kimmel, who was an exemplary comments editor; and Genelle Gertz-Robinson for assistance with some of the literary references. A special thanks to the extraordinarily patient cite checkers of the *San Diego Law Review*. The remaining errors are the author's own. This Comment is dedicated in loving memory of my mother, who proved that there is such a thing as The Reasonable (and wise) Woman.

I. INTRODUCTION

Who steals my purse steals trash; 'tis something, nothing; 'Twas mine, 'tis his, and has been slave to thousands;
But he that filches from me my good name
Robs me of that which not enriches him
And makes me poor indeed.[1]

Financial transaction information[2] is very revealing. By sifting through your credit and debit card transactions, your checks,[3] your ATM archives, your credit application data, your stock portfolios, and your insurance records, financial institutions can discern, among other things, where you live; where you work; whether you own or rent your home; your age; what diseases you have; your height and weight; whether you take prescription medicine; your income to debt ratio; what products or

1. WILLIAM SHAKESPEARE, OTHELLO act 3, sc. 3.

2. No formal definition of the term "transaction data" exists, but as used herein, it refers to any personal information about a consumer that is collected by a commercial enterprise in the conducting of any business transaction with the consumer. In the context of financial services, the transaction data will largely take the form of credit card transactions, check records and credit application data. However, the data can also take the form of data collected in the financial institution's dealings with the consumer (that is, a teller's conversation with the customer at a bank) as well as data that may be purchased by a financial institution from various information databases. For this reason, financial transaction data may include virtually every recorded fact about individual consumers and their behavior.

3. *See* Cal. Banker's Ass'n v. Shultz, 416 U.S. 21, 85 (1974) (Douglas, J. dissenting) ("In a sense a person is defined by the checks he writes. By examining them . . . [one] get[s] to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on *ad infinitum*.").

services you buy; what charities, political causes, or religious organizations you contribute to; your ethnic identity; your marital status; whether you have children; where, with whom, and when you travel; how you spend your leisure time; whether there has been a recent birth or death in your family; whether you have unusual or dangerous hobbies; and even whether you participate in certain felonious activities.[4] Financial institutions collect, process, manipulate, barter, trade, and merge this transaction data with data from other sources, public and private,[5] to produce a robust "profile"[6] representing the economic, demographic, psychographic,[7] and social identity of each customer. This profile provides financial institutions and their affiliates and marketing partners with a detailed information picture of a consumer's personality,[8]

4. For example, automatic teller machine (ATM) records can reveal which bank customers are procuring meretricious services. SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 72 (2000). Garfinkel refers to ATM archives as "hot files." *Id.*

5. For a description of the current scope of this type of activity, see FED. TRADE COMM'N, FEDERAL TRADE COMMISSION PUBLIC WORKSHOP: THE INFORMATION MARKETPLACE: MERGING AND EXCHANGING CONSUMER DATA (2001), *available at* http:www.ftc.gov/bcp/workshops/infomktplace/transcript.htm [hereinafter FTC INFO MARKETPLACE] (remarks of Lynn Wunderman).

6. The term "profile" has no formal definition, although it represents the end result of the processing of data by means of several technologies for data management discussed in Part II of this Comment, including data mining, Knowledge Discovery in Databases (KDD), data modeling, and the use of artificial intelligence to discover unknown patterns and new rules from large databases. One author has defined it as, "the gathering, assembling, and collating of data about individuals in databases which can be used to identify, segregate, categorize and generally make decisions about individuals known to the decisionmaker only through their computerized profile." Karl D. Belgum, *Who Leads at Half-Time? Three Conflicting Visions of Internet Privacy Policy*, 6 RICH. J.L. & TECH. 1, ¶ 8 (1999), *at* http://law.richmond.edu/jolt/v6i1/belgum.html; *see also* PIETER ADRIAANS & DOLF ZANTINGE, DATA MINING v-vii (1996); PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 311–14 (1996). By some accounts, profiles exist on almost every household in the United States. *See* FTC INFO MARKETPLACE, *supra* note 5 (remarks of Lynn Wunderman). The accuracy of the data profile is, in large part, a function of the sheer magnitude of the data collected in financial transactions. *See* STAN RAPP & CHUCK MARTIN, MAX-E-MARKETING IN THE NET FUTURE 17 (2001). One large bank apparently had collected enough personally-identifiable consumer information to create a printout that reached "from the earth to the moon and back." *Id.*

7. *See infra* note 40.

8. Several related terms can be used to define the concept of self. The word "personality" focuses on the multitude of particulars which identify an individual to the world or, "the complex of characteristics that distinguishes an individual . . . or group; [especially] the totality of an individual's behavioral and emotional characteristics." WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY 878 (1989). The word "persona" is a term of art connoting the "symbols or indicia which identify a unique human being . . . includ[ing] the name, likeness, voice, signature, character and other distinctive indicia by

including who that consumer is, what that consumer thinks, and what that consumer is apt to do next.

Profiling is often spoken of with reference to the valuable social and economic benefits it will produce by enabling more efficient marketing and better customer service.[9] Although surveys indicate that consumers are concerned about their transaction privacy,[10] both industry spokespersons[11] and government regulators[12] have stressed that the

---

which a specific person is identified by other persons." JULIUS C.S. PINCKAERS, FROM PRIVACY TOWARD A NEW INTELLECTUAL PROPERTY RIGHT IN PERSONA 265–66 (Info. Law Series No. 5, 1996).

9. Microsoft Corporation founder, Bill Gates, stressed the efficiency of a world where every move of an individual is tracked by authenticating technology and where the resulting personally-identifiable information on all consumers will be readily accessible and tradable by corporate entities. *See* BILL GATES, THE ROAD AHEAD 267–74 (1995). Gates referred to this phenomenon as the "documented life." *Id*. at 268. He described as "backward looking" those who suggest that this technology may degrade the human spirit. *Id*. at 274. Microsoft Corporation markets a product that makes this profiled world possible. *See* Alec Klein, *Planting the Seeds; With Its '.Net' Transition from the Desktop to the Web, Microsoft Could Reap New Dominance—and Scrutiny*, WASH. POST, July 1, 2001, at H1. Michael Saylor, founder and CEO of MicroStrategy, Inc. is a prominent and vocal proponent of the "infinitely more intelligent, efficient and caring society" that useful sliced and diced personal information can provide. *See* Michael Saylor, *The Missing Issue*, WASH. POST, Mar. 14, 2000, at A17; *see also* Jean Schauer, *An Executive Interview: MicroStrategy*, DM REVIEW, Feb. 2001, *at* http://www.dmreview.com/master.cfm. *But see* GARFINKEL, *supra* note 4, at 5:

> Many people today say that in order to enjoy the benefits of modern society, we must necessarily relinquish some degree of privacy. . . .
>
> I think this tradeoff is both unnecessary and wrong. It reminds me of another crisis our society faced back in the 1950s and 1960s—the environmental crisis. . . . Poison was progress: anybody who argued otherwise simply didn't understand the facts.

For remarks highlighting the potential economic benefits of profiling, see DON PEPPERS & MARTHA ROGERS, THE ONE TO ONE FUTURE 5–6 (1993) (indicating that the "1:1 future" will have a tremendous impact on personal privacy, but will also, "create an entrepreneurial froth of opportunities"); *see also* FRED H. CATE, PERSONAL INFORMATION IN FINANCIAL SERVICES 4 (Financial Services Coordinating Council 2000) (quoting Walter F. Kitchenman of the Tower Group when referring to the reporting of personal information about consumers as the "secret ingredient of the U.S. economy's resilience").

10. Ninety-five percent of people questioned would be either not very comfortable or not at all comfortable with the creation of a profile that contained personally-identifiable information such as income and credit data. *Business Week/Harris Poll: A Growing Threat*, BUS. WK., March 20, 2000, at 96. Twenty-three percent of people questioned said that they believed that a bank had at some time violated their financial privacy. Thomson Financial, Inc., *A Crimp in Trust*, FIN. SERVS. MARKETING, July 17, 2001, at 21, 2001 WL 13521307. Statistics show that almost half of consumers would not agree to allow the profiling of their information even if they were told what would be done with the information and were given the choice to opt-out of certain unapproved uses. FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS, June 2000, at 16 (2000), *available at* http://www.ftc.gov./os/2000/06/onlineprofilingreportjune2000.pdf [hereinafter ONLINE PROFILING FTC REPORT].

11. The views of privacy consultant, Alan Westin, are frequently cited by industry. Mr. Westin segments the populace into three categories of consumer: the "Privacy

privacy of transaction data is best dealt with by industry self-regulation. However, there are some indications that industry self-regulation may be failing to protect consumer privacy, and therefore this approach is not without its critics.[13] In fact, a consumer's barter of his or her personality (embodied in personally-identifiable transaction data) to corporate entities may best be described as a Faustian bargain.[14] And

Fundamentalists," the "Privacy Pragmatists," and the "Privacy Unconcerned." He suggests that most consumers fall into the Privacy Pragmatists category, who value the benefits to be obtained from businesses' profiling activities over any potential loss of privacy, and who therefore prefer industry self-regulation to any government legislative action. The Privacy Fundamentalists (described as those who reject all claims of business entitlement to consumer's personal data) are characterized as highly distrustful of government, business, and technology. *See Opinion Surveys: What Consumers Have to Say About Information Privacy, Hearing Before the House Committee on Energy and Commerce*, 107th Cong. (2001) (prepared testimony of Dr. Alan Westin, Professor Emeritus, Columbia University; President, Privacy and American Business). Mr. Westin's funding is largely derived from the substantial consulting fees he receives from multinational corporations that frequently lobby against privacy legislation. Glenn Simpson, *Consumer-Privacy Issue Turns a Retired Professor into a Hot Item*, WALL ST. J., June 25, 2001, at A20.

12. The Federal Trade Commission (FTC) has held several studies on data privacy, most notably in the area of online profiling, but has repeatedly shied away from direct legislative action, stressing the economic benefits of profiling and the need to protect the nascent and economically vulnerable e-commerce industry. The FTC has indicated that the "federal government currently has limited authority over the collection and dissemination of personal data collected on-line" absent a patently deceptive failure to comply with its stated information practices, and it lacks the authority to require a data collector to adopt any information practice policies. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 40–41 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf [hereinafter FTC 1998 REPORT]. The FTC has instead recommended a policy of industry self-regulation. *See* FED. TRADE COMM'N, *supra* note 10, at 20–25. *See generally* Federal Trade Commission, *Privacy Initiatives*, *at* http://www.ftc.gov/privacy/index.html (last visited July 16, 2001).

13. *See, e.g.*, AM. CIVIL LIBERTIES UNION, COMMENTS REGARDING ELEMENTS OF EFFECTIVE SELF-REGULATION FOR THE PROTECTION OF PRIVACY AND QUESTIONS RELATED TO ONLINE PRIVACY, *reprinted in* 2001 PRACTISING L. INST., SECOND ANNUAL INSTITUTE ON PRIVACY LAW 695, 701–09; Peter Henderson, *Privacy Issue Splits Tech Camps: H-P Chief Presses for Web Legislation*, SAN DIEGO UNION TRIB., Aug. 21, 2001, at C2. One privacy activist has indicated that the "notice and choice" self-regulatory approach adopted by the FTC operates more like a disclaimer or a warning label than any real privacy protection. *See Hearing on Privacy in the Commercial World Before the Subcommittee on Commerce, Trade, and Consumer Protection Committee on Energy and Commerce, U.S. House of Representatives* (2001) (Testimony and Statement for the Record of Marc Rotenberg), *reprinted in* SECOND ANNUAL INSTITUTE ON PRIVACY LAW, *supra*, at 305, 311. The FTC has only recently taken up the issue of offline privacy. *See infra* note 35.

14. The tale of Faust's sale of his soul to Mephistopheles has been described as a morality play demonstrating the tensions between advancing technology and proper legal restraints. *See* Manfred Lachs, *Views from the Bench: Thoughts on Science, Technology*

indeed, because a consumer is often oblivious to the fact that such a significant transaction has even taken place (either because the data exchange does not legally require the consumer's consent or because the transfer is deemed permitted merely if the consumer fails to "opt-out"),[15] an individual's transfer of his or her personality to the private sector is perhaps better described as a heist rather than as a bargained-for exchange.

Although almost every sector of the U.S. economy practices consumer profiling,[16] perhaps the most substantive challenge to consumer privacy is found in the activities surrounding the use and disclosure of consumer transaction data by the financial services industry.[17] For that reason, this Comment focuses exclusively on consumer profiling in the context of the financial services sector, defined as banks, credit card issuers, brokerages, and insurance companies.[18]

Necessary to any analysis of the possible impact on privacy posed by

---

and World Law, 86 AM. J. INT'L L. 673, 697 (1992). Marlowe and Goethe penned the most famous accounts of the Faustian legend. *See* CHRISTOPHER MARLOWE, THE COMPLETE PLAYS (J. B. Steane ed., 1969); JOHANN WOLFGANG VON GOETHE, FAUST: A TRAGEDY (Bayard Taylor, trans., 1887). *See generally* PHILIP MASON PALMER & ROBERT PATTISON MORE, THE SOURCES OF THE FAUST TRADITION: FROM SIMON MAGUS TO LESSING (1965). Posner's contractual analysis of the Faust legend concludes that the bargain was void against public policy. RICHARD A. POSNER, LAW AND LITERATURE 110–14 (rev. and enl. ed. 1998). At least Faust negotiated a tangible reward of twenty-four years of worldly pursuits in exchange for his soul. In comparison, U.S. consumers obtain a mere illusory promise that they will receive improved customer service and perhaps fewer unwanted "Nike[™] ads" in exchange for their personality profiles. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 154–55 (1999).

15. "Opt-out" is a term of art, meaning the setting of a default rule whereby a data collector need not obtain express consent prior to using or disclosing a consumer's personal data. *See infra* note 22. Some suggest that there is a "misunderstanding gap" between actual data collection, merger, and exchange practices versus the beliefs of consumers concerning those practices. *See* FTC INFO MARKETPLACE, *supra* note 5 (closing remarks of Joel Winston). A consumer often receives either no notice at all of the sale of her information or her consent is implied by her failure to affirmatively opt-out of data sharing. *See* Beth Givens, Financial Privacy: The Shortcomings of the Federal Financial Services Modernization Act, Presentation before the California Bar Association (Sept. 15, 2000), *at* http://www.privacyrights.org/ar/fin_privacy.htm.

16. *See generally* FTC INFO MARKETPLACE, *supra* note 5.

17. *See* Rachel Zimmerman & Glenn R. Simpson, *Lobbyists Swarm to Stop Tough Privacy Bills in States*, WALL ST. J., April 21, 2000, at A16 ("For all the talk about the Internet's potential to become the ultimate surveillance tool, the most invasive data-collection practices now in use involve credit, banking, housing and health data that consumers have given out for years.").

18. But this category is not as limiting as it may seem at first glance. Consider that General Motors Corporation offers home mortgages; Sears and Nordstrom issue MasterCard and Visa products. *See* Michael Staten, *Customer Relationship Management as a Privacy Enhancer*, *at* http://www.acxiom.com/ DisplayMain/0,1494,USA~en~990~1244~0~0,00.html (May, 2001). This phenomenon is referred to as the "super industry" where telecommunications, computers, financial services, and retailing industries compete for the same customers, with the same products. Rashi Glazer, *Marketing and the Changing Information Environment: Implications for Strategy, Structure, and the Marketing Mix*, *in* USING MARKET KNOWLEDGE 127, 138 (Rohit Deshpandé ed., 2001).

consumer profiling is an understanding of the technology itself. Thus, Part II describes the profiling technology currently utilized by the financial services industry and then discusses the technological advances in profiling technology that are likely to be used by financial services in the near future.

Next, Part III critically reviews some of the social and economic effects that are likely to accompany the widespread use of profiling technology in the financial services sector. As Part III demonstrates, the practice of financial profiling produces important social and economic impacts and has the potential to undermine the existing statutory safeguards regarding the use and disclosure of sensitive personal financial information.

Next, Part IV focuses on the current laws that address financial privacy and illustrates that at present there are no real constitutional or statutory protections in place for consumers who desire to prevent the profiling of their financial information by the private sector. Furthermore, Part IV reviews recently enacted financial privacy legislation and suggests that the Gramm-Leach-Bliley Act (GLBA)[19] not only fails to address the issue of financial profiling but, by its creation of financial holding companies,[20] may even facilitate and encourage the greater use of profiling by financial institutions.

Part V of this Comment therefore urges the courts to recognize a common law right of privacy under which a consumer may control the use and disclosure of his or her data profile. Although rumors of the death of the right of privacy abound,[21] this Comment proposes that such pessimism is unfounded and that the inherently invasive nature of profiling technology may introduce renewed vigor into the application of

19. 15 U.S.C. §§ 6801–6810 (2000).

20. *Id*. A financial holding company is the creation of Title I of the GLBA, and allows banks, securities firms, and insurance companies to align under a holding company structure or as financial subsidiaries. 15 U.S.C. § 6809. *See also* CCH INC., FINANCIAL SERVICES MODERNIZATION: GRAMM-LEACH-BLILEY ACT OF 1999, at 21 (Kenneth R. Benson et al. eds., 1999). Beth Givens, Director of the Privacy Rights Clearinghouse, referred to these financial holding companies as "financial 'supermarkets'" with an "unprecedented ability to compile comprehensive data profiles on their customers." FED. TRADE COMM'N, FEDERAL TRADE COMMISSION PUBLIC WORKSHOP: THE INFORMATION MARKETPLACE: MERGING AND EXCHANGING CONSUMER DATA, (2001) (Comments of Beth Givens, Director, Privacy Rights Clearinghouse), *at* http://www.ftc.gov.bcp/workshops/infomktplace/comments/givens.htm [hereinafter GIVENS FTC COMMENTS].

21. *See, e.g*., Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291 (1983).

both the privacy intrusion on seclusion tort and the appropriation privacy tort to information privacy issues.

Part V further demonstrates that the privacy tort may reformulate the current opt-out paradigm[22] by bringing into question the ability of financial institutions to contract for unreasonably broad rights to use and disclose consumers' private information merely by publishing a privacy policy. Part V then demonstrates that on the basis of a breach of the common law right of privacy, a consumer may then utilize state consumer protection statutes to vindicate this right.

The quiet erosion of privacy by consumer profiling may be an issue that is ignored at our peril. Justice Brandeis wrote: "All law is a dead letter without public opinion behind it. But law and public opinion interact—and they are both capable of being made."[23] This Comment therefore attempts to provide a glimpse of the potential socioeconomic impacts of financial profiling in order to encourage public and judicial opinion toward the recognition and enforcement of a consumer's right to refuse the appropriation of his or her data personality for commercial purposes that exceed the scope of their reasonable expectation of privacy.

II. THE TECHNOLOGY OF PROFILING

"You have zero privacy anyway—get over it."[24]

Consumer profiling is a growing trend in the financial services industry.[25] This business trend was brought about by several converging technological and theoretical changes. First, transaction data is no longer being looked at as simply information, but rather as a commodity in and of itself. Second, the data warehouse is enabling the processing and storage of data in ways never before thought possible. Third, new software technologies now allow data exchange where communication

22. Perhaps the best definition of this paradigm is as follows: '"Opt-out' means that financial institutions can share or sell customer information without their affirmative up-front consent. If customers do not tell the bank to refrain from selling their data, such sale will go on indefinitely. 'Opt-in' means that the default is set [on] 'no sharing.'" Givens, *supra* note 15.

23. Letter from Louis D. Brandeis to Alice Goldmark (Dec. 28, 1890), *in* 1 LETTERS OF LOUIS D. BRANDEIS 97 (Melvin I. Urofsky & David W. Levy eds., 1971).

24. This remark has been attributed to Sun Microsystems Inc.'s chief executive officer, Scott McNealy, apparently spoken to a group of analysts and reporters at a meeting celebrating the introduction of Sun's new data-sharing technology. *See* Andrew Roth, *A New Privacy Flash Point, Courtesy of IBM?*, AM. BANKER, Jan. 3, 2001, at 1.

25. Staten, *supra* note 18 (describing current and potential CRM processes at Wachovia Bank, Fidelity Investments, and Citigroup).

difficulties had previously prevented it. Fourth, a unified market for the exchange and sale of transaction data profiles has emerged.

A. Financial Transaction Data: From Information to Commodity

Until relatively recently, financial institutions merely processed consumer financial information and did not use it for marketing or other revenue generating purposes.[26] The limitations of technology and the relatively high cost of storing and processing massive amounts of data made it economically unfeasible for banks to peer into their customers' personal details.[27] But as this Part later demonstrates, the limitations on transaction surveillance are quickly evaporating with the relentless technological advances and price decreases in data warehousing and data mining technology. An additional impetus to this surveillance is provided by data exchange technology that both encourages the transfer and sale of data and facilitates the increasingly symbiotic relationship that has arisen between financial services companies and marketing organizations.[28] The shift in technology has resulted in a paradigm shift in the meaning and value of information itself.[29] Information no longer fills its traditional role of the "interaction[s] between environmental stimuli and intelligent organisms,"[30] but now fills a role as a marketable product in itself.[31]

---

26. Many banks have apparently been collecting consumer information for some time, but some had absolutely no idea what on earth to do with the data until most recently. *See* FTC INFO MARKETPLACE, *supra* note 5 (remarks of Elisabeth Brown); RAPP & MARTIN, *supra* note 6, at 17.

27. *See* FTC INFO MARKETPLACE, *supra* note 5 (remarks of Elisabeth Brown) (stating that banks have not done much with their sensitive consumer information until very recently because of the lack of large databases and the software capability to property manipulate and update the information). One other gating factor for banks has been the silos in which most information has been kept. *See* GARTNER GROUP, RESEARCH NOTE, BANK DATA WAREHOUSING: ALIVE (THOUGH SOMEWHAT AILING) 2 (2001). Unlinked data marts result in "inconsistent usage, data redundancy and multiple versions of 'the truth.'" *Id.* But see *infra* Part II.D for a discussion of why data silos will soon cease to be a limiting factor.

28. *See, e.g.*, FTC INFO MARKETPLACE, *supra* note 5 (remarks of Lynn Wunderman) (discussing First USA as a key contributor to a data co-op). See *infra* notes 70–71 for a description of data co-ops.

29. *See generally* Glazer, *supra* note 18, at 129 ("A major theme of this generation has been the onset of the 'information age,' a time in which information, or knowledge, replaces matter and energy as the primary resource of society.").

30. *Id*. at 131–32.

31. *Id.* at 149–50. Professor Rashi Glazer of the Haas School of Business, University of California, Berkeley, states that the paradigm shift under which

Technology companies predictably welcome this paradigm shift as an opportunity to gain market share.[32] Bill Gates sees the networked, profiled, information-commodified future.[33] In his book discussing the future of the Internet, he described a world where massive amounts of data would be collected on individuals with the help of numerous authenticating devices operating at ubiquitous data collection points, both inside and outside the home.[34] Although Internet privacy has attracted most of the attention until very recently,[35] as Gates illustrated, the Internet is just one of many collection points for transaction data in the newly evolving "database nation."[36]

And financial data is the gold standard for transaction data. Unlike consumer data gathered from census data, from surveys, or from cookie-enabled[37] websites such as Amazon.com, which is generally anonymous,[38] financial data is, by its nature, personally identifiable unless the account

---

information has become a "marketable asset" is only a very recent phenomenon which is fundamentally redefining the "rules of the game" for commercial transactions. *Id.* at 138, 150.

32. *See, e.g.*, Acxiom Corporation, *Customer Data Integration: Realizing the Promise of Customer Relationship Management*, *at* http://www.acxiom.com/DisplayMain/0,1494,USA~en~374~1737~0~0~,00.html (2001). Acxiom Corporation estimates that a market leader in the customer data integration space would reap up to $5 billion of a total market estimated to reach as much as $15 billion by 2004. *Id.* MicroStrategy Corporation Chairman and CEO, Michael Saylor, looks forward to making "intelligence" a tenth of the economy. *See* Schauer, *supra* note 9, *at* http://www.dmreview.com/master.cfm.

33. *See* GATES, *supra* note 9, at 218–21, 266, 274.

34. *See Id.* However, apparently Gates believes this new privacy-invading interior design is only for the masses. When discussing the design of the living quarters of his own house, Gates said: "[P]rivacy is important." *Id*. at 218.

35. The FTC has only recently taken up the issue of offline consumer privacy issues. *See generally* FTC INFO MARKETPLACE, *supra* note 5. Beth Givens, Director of the Privacy Rights Clearinghouse noted in her comments to the FTC Public Workshop on the Information Marketplace that her organization receives a greater amount of complaints about offline privacy matters than it does about online privacy. *See* GIVENS FTC COMMENTS, *supra* note 20.

36. The term "database nation" was coined by privacy advocate Simson Garfinkel. GARFINKEL, *supra* note 4.

37. A "cookie" is a small text message sent by a Web server, which is stored by the browser in a text file called "cookie.txt." The cookie then enables the Web site to receive information on the Web site visitor's preferences. *See* Leon Stiel, *An Introduction to Privacy Technologies and Techno-Speak*, *reprinted in* SECOND ANNUAL INSTITUTE ON PRIVACY LAW, *supra* note 13, at 33, 48.

38. *See* ONLINE PROFILING FTC REPORT, *supra* note 10, at 4. Several Web sites have recently attempted to integrate anonymous Internet transaction data with databases that convert it into personally identifiable information. The consumer backlash has spawned class action lawsuits. *See, e.g.*, *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001); Supnick v. Amazon.com, No. C00-0221P, 2000 WL 1603820 (W.D. Wash. May 18, 2000) (certifying class action); *In re* RealNetWorks, Inc. Privacy Litig., No. 1329, 2000 U.S. Dist. LEXIS 1458 (J.P.M.L. Feb. 10, 2000). *See generally* Charles L. Kerr, *Online Privacy: Recent Developments*, *reprinted in* SECOND ANNUAL INSTITUTE ON PRIVACY LAW, *supra* note 13, at 51, 66–111.

number, social security number, or other identifying characteristic is either encrypted[39] or deleted. Because financial data includes information on purchasing behavior, it is deemed "psychographic data" and is therefore considered determinate of future behavior.[40] Thus, it is not hard to understand why personally-identifiable financial data and the value of the information therein may easily be termed the new currency of this century.[41] Indeed, the former chairman of Citicorp referred to the information standards for the movement of personal and nonpersonal financial data as the *equivalent of money* in global financial markets.[42] In order to fully understand how that raw data can turn to gold, it is necessary to review the technology behind data warehousing and computer profiling, as well as the mechanisms supporting data exchange.

B. The Data Warehouse

Transaction data normally resides in something called a data warehouse.[43] And the data warehouse makes good business sense for

39. Encrypted information is almost impossible to decipher in a database without the use of the accompanying encryption key. *See* ADRIAANS & ZANTINGE, *supra* note 6, at 81.

40. ONLINE PROFILING FTC REPORT, *supra* note 10, at 5 n.18 ("Psychographic data links objective demographic characteristics like age and gender with more abstract characteristics related to ideas, opinions and interests."). Psychographic information is "incredibly powerful information from a segmentation standpoint" and thus is highly valuable to marketers. *Id.* Psychographic information is found in purchase behavior, and personally identifiable data on purchase patterns is generally very difficult for marketers to obtain on a global level, except where it is obtained voluntarily from consumer survey or warranty card sources. *See* FTC INFO MARKETPLACE, *supra* note 5 (remarks of Lynn Wunderman).

41. *See* Zimmerman & Simpson, *supra* note 17. Financial firms and telemarketers consider personally-identifiable financial transaction data "among their most valuable assets." *Id*.; *cf.* Bob Sullivan, *Bank Crime Data Theft on the Rise*, MSN, June 26, 2002 ("Your concern is no longer a teller walking out the door with cash . . . . Your concern is information walking out the door. That's the new currency. You've got to think: information equals cash." (quoting fraud expert, Rob Douglas)), http://msnbc.com/news/772723.asp?pne=msn&cpl=1 (last visited June 28, 2002).

42. *See* SCHWARTZ & REIDENBERG, *supra* note 6, at 261–62.

43. The data warehouse is not actually a product or a place, but rather is a process or a "staging area" for the collection, integration, storage and delivery of information. *See* INT'L DATA CORP., THE FOUNDATIONS OF WISDOM: A STUDY OF THE FINANCIAL IMPACT OF DATA WAREHOUSING 2 (1996), *available at* http://www.teradatalibrary.com/pdf/idc_010196.pdf (last visited Oct. 27, 2001). Data warehouses are the engines that drive the decision support systems that utilize data mining software to find hidden information in data. *See* ADRIAANS & ZANTINGE, *supra* note 6, at 25–36. See also *infra* note 51 for a discussion of data mining software.

the financial services industry. Not only have hardware, software, and data storage costs declined significantly in the past few years,[44] but empirical evidence shows that companies will rapidly reap a significant return on their investment in such a system.[45] In fact, the economic benefits of the data warehouse are so compelling, that the few banks that do not already possess this technology are now in the process of developing or procuring it.[46] The reduction in costs for a data warehousing system has encouraged the financial services industry to store massive amounts of consumer transaction data spanning over many years.[47] But, price and performance metrics aside, the real driving force for the growth in data warehousing is the increasing sophistication of the software analytical tools that enhance the value of the information stored therein.[48] Stored raw data is of limited value, absent a corporation's ability to manipulate and correlate the data to create consumer profiles. Profiling produces economic value.[49] The equation thus feeds on itself:

---

44. Price declines have been brought about by increased competition among direct access storage device (DASD) manufacturers, as well as by technical advances in storage devices. Industry software and hardware giants like IBM Corporation, Informix, Inc., Oracle Corporation and NCR Corporation compete for a greater share of their corporate customers' information technology budgets by waging a war of terabyte capacity per dollar. *See* Lou Agosta*, Data Warehouse Volume Growth Continues*, IDEABYTE, June 5, 2001, *available at* http://www.teradatalibrary.com/pdf/giga_060501.pdf (last visited Oct. 27, 2001). System manufacturers compete for the top performance in TPC Benchmark tests. According to Giga Information Group, the most recent Transaction Processing Performance Council (TPC) Benchmark indicates that the overall price versus performance metric for a multi-terabyte decision support system shows costs per 3000 GB to be as low as $999. *Id*. A terabyte is defined as "a measure of computer storage capacity and is 2 to the 40th power or approximately a thousand billion bytes." SearchStorage.com, *at* http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci 213118,00.html (last visited March 16, 2002). Aetna Insurance Corporation was recently reported to possess 174.6 terabytes of customer information. *See* Barry Nance, *Managing Tons of Data*, COMPUTERWORLD, April 23, 2001, at 62, *available at* http://www.computerworld.com/hardwaretopics/hardware/server/story/0,10801,59819,0.html.

45. A survey by International Data Corporation indicated that a company will receive an average three-year return on investment of 401% from a data warehouse implementation. INT'L DATA CORP.*, supra* note 43, at 5.

46. *See* META GROUP, DATA WAREHOUSE SCORECARD: COST OF OWNERSHIP AND SUCCESSES IN APPLICATION OF DATA WAREHOUSE TECHNOLOGY 1, *available at* http://www.teradatalibrary.com/pdf. Fully eighty-five percent of all banks utilize either a data warehouse, a data warehouse with data marts, or unlinked data marts to store data. In the interest of pursuing "revenue-producing opportunities" and obtaining one view of the customer, many banks with unlinked data marts are now working to consolidate them. *See* GARTNER GROUP, *supra* note 27.

47. *See* INT'L DATA CORP., *supra* note 43, at 1, 4–5. Royal Bank of Canada, for example, has been collecting customer data since 1978. This data has recently been used by the bank to create profiles on nine million of their personal retail clients. *See* NCR CORPORATION, CUSTOMER SUCCESS STORIES: ROYAL BANK OF CANADA 1, 5 (2000), *available at* http://www.teradatalibrary.com/pdf/eb1323.pdf (last visited Oct. 27, 2001).

48. *See* INT'L DATA CORP., *supra* note 43, at 1.

49. *See, e.g.*, Nance, *supra* note 44 ("Multiple terabytes of the most pampered,

increased storage of data drives the increased use of profiling; the value of profiled data creates a value proposition to justify the increased collection and storage of data.[50]

C. Software Applications

The various software applications that are used to extract hidden information out of data are grouped under the evocative term, "data mining."[51] Companies are spending vast amounts of money to procure data mining software in the hopes of leveraging off of the value inherent in the data piling up in their data warehouses.[52] Customer relationship management (CRM)[53] software, which utilizes statistical modeling techniques[54] on transaction data to analyze a customer's potential future purchase behavior,[55] is estimated to grow at a rate of forty percent per year, and to capture between $10 and $20 billion of the corporate

---

best-maintained data in the world are just a slag heap of bits without accurate, meaningful data definitions and schemas.").

50. *See* INT'L DATA CORP., *supra* note 43, at 1 ("The organizations studied by IDC provided ample evidence that [the goal of leveraging data to make better decisions] is well worth the effort, and cost, of building effective data warehouses.").

51. *See* ADRIAANS & ZANTINGE, *supra* note 6, at 47 (explaining that data mining is an idea and generally describes the process of finding hidden information in data). The various tools that are included under the definition are: query tools, statistical techniques, visualization, online analytical processing (OLAP), case-based learning, decision trees, association rules, neural networks, and genetic algorithms. *Id*. While Data mining only describes the discovery process, knowledge discovery in databases (KDD) is a more general term describing the "whole process of extraction of knowledge from data" and includes machine learning, statistics, database technology, expert systems and data visualization. *Id*. at 5.

52. *See* Acxiom Corporation, *supra* note 32. International Data Corporation (IDC) data indicates that $90 billion was spent by corporations in 1999 for data warehousing, enterprise resource management (ERM) and customer relationship management (CRM) products and that the expected growth rates would double by 2002. *Id.*

53. CRM is a term used to describe the utilization of analytical and decisioning tools on front and back office data to look at an individual's profile to predict their future purchasing patterns. A primary use of the technology is to identify the most profitable customers. *See* Judith Lamont, *Analytical CRM: Capturing Data to Cater to Customers*, KMWORLD, Feb. 2001, at 16, *available at* http://www.kmworld.com/publications/magazine/index.cfm?action=readarticle&article_id=987&publication_id=1.

54. For an example of a CRM model, see MICHEL WEDEL & WAGNER A. KAMAKURA, MARKET SEGMENTATION: CONCEPTUAL AND METHODOLOGICAL FOUNDATIONS 316–20 (2d ed. 2000).

55. CRM software may have fallen short of its technological promise, however. *See* Kevin Fogarty, *Is CRM a Faint Hope?*, COMPUTERWORLD, June 4, 2001, at 50. In Mr. Fogarty's words, CRM was a "boondoggle." *Id*.

information technology expenditures in 2001 alone.[56] But CRM is quickly being eclipsed by a superior technology referred to as "business intelligence."[57] Business intelligence software uses advanced data visualization tools and artificial intelligence, [58] often in the form of neural networks,[59] to find hidden patterns in data that human users might overlook.[60]

The development of CRM and business intelligence software has changed the data warehouse from a tool used to improve process efficiency and collect data into a tool used to construct and analyze individual consumer profiles and to predict individual consumers' future behavior.[61] Companies use this software to process a consumer's transaction data in order to extract an expression of the consumer's very personality, which is then distilled down into a convenient packet of computer code.[62] That simulated personality can then be internally used by a company for its commercial advantage for purposes such as customer relationship management and predictive marketing—or that personality can be sold.

---

56. *Id*.; Lamont, *supra* note 53, at 16.

57. One industry pundit pauses to assure us that this term is not an oxymoron. Dan Miller, *5 Technologies You Need to Know*, INDUSTRY STANDARD, *at* http://www.thestandard.com/article/0,1902,24308,00.html (May 21, 2001).

58. Artificial Intelligence refers to computer systems that self-learn or otherwise model human knowledge. *See* KENNETH C. LAUDON ET AL., INFORMATION TECHNOLOGY AND SOCIETY 491–50 (1994).

59. The most common form of artificial intelligence is found in neural networks. Neural networks attempt to mimic the operation of the human brain by means of thousands of transistors connected in a network. *See* ADRIAANS & ZANTINGE, *supra* note 6, at 2–3, 68–78; LAUDON ET AL., *supra* note 58, at 497. Neural networks have been criticized as "black boxes" that produce a decisioning system that is impossible to audit for discriminatory criteria. *See generally* Marcia Stepanek, *Weblining*, BUS. WK., April 3, 2000, at EB26, EB33 (stating that the value assumptions used by the black box software cannot be determined with precision even by the system's developers).

60. *See* ADRIAANS & ZANTINGE, *supra* note 6, at 68–78. One industry analyst discussed business intelligence as a further generation of the technology provided in knowledge management and data mining. Miller, *supra* note 57. Business intelligence uses artificial intelligence to discover unexpected patterns in data. *Id.* The market for business intelligence software is expected to grow to $8.8 billion in 2004, and the corporate players include giants such as IBM Corporation, Oracle Corporation, SAP, Computer Associates and Microsoft Corporation. *Id.* According to Michael Saylor, CEO of MicroStrategy Corporation, business intelligence can come in several forms: analytics (optimal merchandizing, inventory, fraud detection), narrowcasting (predictive analytics, arbitrage, and demand activation) and "embedded intelligence" (for example, a "bank account that moves its own cash around"). *See* Schauer, *supra* note 9, *at* http://www.dmreview.com/master.cfm.

61. *See* INT'L DATA CORP., *supra* note 43, at 4, 12.

62. Customer behavior as recorded in transaction data has been referred to in *Business Week* magazine as a "silicon simulacrum." Jonathan Berry et al., *A Potent New Tool for Selling: Database Marketing*, BUS. WK., Sept. 5, 1994, at 56, 58.

D. Profile Exchange Mechanisms

As a major financial industry publication recently pointed out, the current inability of different file formats to "speak the same language" has up to now been a major enforcer of consumer privacy.[63] But the commercial rewards to be gained have spawned an entire industry focused on developing universal data exchange mechanisms to overcome this barrier. The XML, or extensible markup language[64] platform, has been termed the "lingua franca of cyberspace"[65] and has the potential to enable the widespread sharing of data over the Internet.[66] Another such mechanism for information sharing in development, the Customer Profile Exchange Network, is based on the XML format and is backed by a consortium of technology companies and several financial services industry partners.[67] Data from disparate sources that does not utilize one of these universal communication languages can otherwise be unified by universal data exchange software applications.[68] The

63. *See* Roth, *supra* note 24.

64. *See* Klein, *supra* note 9. Microsoft Corporation is developing its Hailstorm technology on the XML platform. Hailstorm is part of Microsoft's .Net initiative and may prove to be particularly invasive because it is being designed to work only in conjunction with an authentication and identification device. *Id.* American Express entered discussions with Microsoft to partner in the .Net initiative to offer its cardholders instant notification of potential fraud on their account. *Id.*

65. *See* FTC INFO MARKETPLACE, *supra* note 5 (remarks of Richard Smith).

66. *Id.*

67. Backers of the consortium include International Business Machines Corporation, Hewlett-Packard Company, Intuit, Lucent Technology, First Union National Bank, HSBC-USA, Bank of Nova Scotia, and Charles Schwab Corporation. *See* Roth, *supra* note 24. First Union Corporation released a statement indicating that they valued their customers' privacy and that they joined the consortium "to stay informed of new technologies and how those technologies will benefit our customers." *Id*. For more information on the consortium, see Customer Profile Exchange Network, *at* http://www.cpexchange.org. As of March 2001, the consortium had over ninety corporate members. *See* FTC INFO MARKETPLACE, *supra* note 5 (remarks of Dana Rosenfeld).

68. Acxiom Corporation recently introduced a product called AbiliTec[sm], enabling one view of the customer to be built out of disparate data sources. *See* ABERDEENGROUP, ANNOUNCEMENT PROFILE, ACXIOM'S ABILITEC: KEY TO CREATING A TOTAL CUSTOMER VIEW (1999), *available at* http://acxiom.com/interactive/dpdwebdev/productsandservices /brochure/pdfs/aberdeen.pdf (last visited Mar. 18, 2002). Hummingbird Communications highlights the significant cost reductions and increased efficiency their universal data exchange product can provide to a company dealing with information from disparate systems or databases. *See* HUMMINGBIRD COMMUNICATIONS LTD., UNIVERSAL DATA EXCHANGE: AN ENTERPRISE-WIDE SOLUTION (2000), *available at* http://www. hummingbird.com/collateral/universaldataexchange_whitepaper_EN.pdf (last visited May 25, 2002).

resulting ease of data transfer and data matching has encouraged the formation of "data intermediaries"[69] and "co-op database[s],"[70] where information and profiles containing the life traces of individuals are offered and purchased like any other commodity.[71] Data exchange is also increased by the fact that data sharing is increasingly *de rigueur* between alliance partners under today's marketing alliance agreement.[72] To quell consumers' concerns over the loss of their privacy, many of the companies selling information exchange technology argue that their technologies enforce customer privacy preferences while still allowing the free flow of data.[73] But some are skeptical that these technologies will be utilized in a way that will give consumers any real privacy protections.[74]

---

69. A "data compiler" is defined as a "third party organization[ ] that collect[s], slice[s], and dice[s] and then resell[s] consumer data." *See* FTC INFO MARKETPLACE, *supra* note 5 (remarks of Professor Culnan). A data compiler will not usually have a direct relationship with the data subject. *Id*. One data compiler refers to itself as an "infomediary." *Id.* (remarks of Johnny Anderson). The data compilers apparently operate on an informal consortium basis amongst themselves. Allison Brown, an attorney for the FTC's Bureau of Consumer Protection remarked at the FTC Public Workshop on the Information Marketplace that "[o]ne thing that becomes clear pretty quickly is how integrated the aggregators are with the sources and how the data sort of rotate in and out of the different databases." *Id.* (remarks of Allison Brown). According to the statement of one participant at this FTC workshop, even data on pharmaceutical purchases and doctor's visits may end up in the hands of the data compilers. *Id.* (remarks of Michael Pashby).

70. The term "co-op database" refers to an arrangement where members of the co-op pool their customer transaction data and profiles in order to gain the opportunity to receive the data contributed by other members. *Id.* (remarks of Lynn Wunderman).

71. This information marketplace is a phenomenon distinct to the U.S. One theory of why U.S. mortgage rates are up to two percent lower than those in Europe is that the standardized consumer credit information in the U.S. makes wider securitization possible. *See* CATE, *supra* note 9, at 4. One European participant at the FTC Public Workshop on the Information Marketplace expressed his disbelief and outrage at the U.S. information marketplace as follows: "[W]here will it end? At which point do I say, [t]his data is sacrosanct, you cannot have access to it . . . will it just be taken for granted that this is just another piece of information that can be used to market to me?" *See* FTC INFO MARKETPLACE, *supra* note 5 (remarks of Mark Le Maitre).

72. *See* RAPP & MARTIN, *supra* note 6, at 137 (indicating that information sharing is *expected* by most businesses entering into any form of alliance agreement).

73. *See, e.g.*, Cristina Lourosa-Ricardo, *What's Ahead for Privacy: Technology Has Taken away Privacy. Now It Promises To Give It Back*, WALL ST. J., June 25, 2001, at R-17. An analyst at Forrester Research indicated that the Customer Profile Exchange will manage data at such a granular level that consumer privacy preferences will be able to follow information as it is passed along. *See* Roth, *supra* note 24. An Acxiom Corporation spokesperson made the argument that their data matching software and the increased profiling that it will enable will foster an increasingly personalized customer experience which will build trust in the merchant and thus alleviate a consumer's privacy concerns. *See* Staten, *supra* note 18.

74. *See e.g.*, FTC INFO MARKETPLACE, *supra* note 5 (remarks of Richard Smith) (expressing skepticism that the privacy controls in the Consumer Profile Exchange would be implemented); Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 751–55 (2000) (referring to the "blinking twelve" problem; that is, privacy system

The silo walls are falling down. This is a revolution, albeit a silent one.[75] It thus behooves us to stop to consider the socioeconomic effects of this information revolution.

III. PROFILING: THE SOCIAL AND ECONOMIC EFFECTS

> "*Where is the wisdom we have lost in knowledge? Where is the knowledge we have lost in information?*" [76]

A. Social Effects

Proponents of the information revolution often depict the social benefits of profiling as a return to the good old days where shopkeepers knew their customers by name, knew their special preferences, and thus interjected a personal element into the commercial experience.[77] One proponent even referred to data profiling and the resulting customer relationship management techniques as the "old fashioned" way of doing business.[78] But others are less sanguine about the social effects of a commercial ecosystem built on profiling[79] and have sought to distinguish profiling from traditional marketing practices. One important difference is rooted in the permanent record that transaction data leaves behind. As Lawrence Lessig states:

> Gossipy neighbors might have watched, but their watching produced nothing as lasting or as reliable as . . . a credit card system's endless collection of data about your purchases, or the telephone system's records of who you called when and for how long. . . . Then the technology noticed only what was different; now it notices any transaction.[80]

---

defaults will be set to allow data transfer and consumers will respond in the same manner as they do to their VCRs, which they have absolutely no clue how to reprogram). This author's own example of this phenomenon is that because every new version of Microsoft Explorer seems to make the "disable cookies" function more inconvenient for her to locate than it was before, she tends not to bother.

75. *See* Glazer, *supra* note 18, at 127, 129. Lawrence Lessig compared the information revolution to the breakup of the Soviet Union in regard to its far-reaching consequences. *See* LESSIG, *supra* note 14, at 234.

76. T.S. Eliot, THE ROCK pt. I (1934).

77. *See, e.g.*, PEPPERS & ROGERS, *supra* note 9, at 21; *Siebel Corporation Advertisement* (CBS Television Network, June 24, 2001) (viewed by author).

78. *See* PEPPERS & ROGERS, *supra* note 9, at 21.

79. *See, e.g.*, LESSIG, *supra*, note 14, at 154–56; Schwartz, *supra* note 74, at 746–49. *See generally* Stepanek, *supra* note 59.

80. LESSIG, *supra* note 14, at 151. In fact, if any analogy can be drawn to an

Furthermore, traditional interchanges of information always left consumers with a choice of which information was to be shared with the merchant and which information they chose to keep secret. Computer profiling takes away the consumer's choice of providing *selective* information to others. Although this *full disclosure* could produce a positive result by providing businesses with a practical means of preventing consumer fraud, it could also provide businesses with a new means of manipulating their customers.[81] This manipulation could take the form of a discriminatory regime of customer ranking based on existing prejudices, which some have suggested will ossify society and chill free association and behavioral autonomy.[82]

The customer ranking that accompanies profiling is already well entrenched in the financial services sector.[83] Sanwa Bank gives *A*s to its best customers, but those whose profile indicates that they will produce less profit for the bank earn *C*s.[84] Predictably, the bank tends to charge those earning *C*s more fees and puts them on hold more often and for longer periods of time.[85] Statistics show that eighty percent of a bank's profit is gained from only twenty percent of their customers.[86] It is therefore no surprise that evidence indicates that banks utilize profiling software not only to provide superior customer service, but also to

---

existing marketing practice, the closest parallel is the A.C. Neilsen Company's practice of collecting data on consumers' television viewing habits. Such tracking only takes place by invitation. *See* Nielsen Media Research, *What if Nielsen TV Ratings Contacts Me?*, *at* http://www.nielsenmedia.com (2002).

81. Posner suggested that the law does not always require the "shrewd bargainer" to disclose to the other party to the transaction the facts of the bargainer's true opinion of the value of the transaction. He suggested that this shrewdness does at one point cross the line into fraud. The line is crossed, according to Posner, when the information that a party seeks to conceal is not a product of significant investment. Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 397–98 (1978).

82. *See, e.g.*, Schwartz, *supra* note 74, at 755–62. Paul Schwartz saw a risk to democratization of opportunity by a restriction of economic and information opportunity by means of profiling in its reinforcement of existing prejudices and mistaken beliefs. *Id*. at 757. Schwartz also predicted a substantial restriction of autonomous decisionmaking as a result of the oppressive force of constant surveillance. *Id*. at 758–59 ("The threat to autonomy is through a coercive influence that takes over, or subtly and persistently colonizes, a person's thinking process.").

83. *See* Stepanek, *supra* note 59, at EB 26–27.

84. *Id.* First Union National Bank uses a similar ranking system called "Einstein." It uses colors instead of letter grades. Marginal customers are accorded a red ranking. *Id.*

85. *Id.*

86. Lamont, *supra* note 53. This theory is commonly known as the "Pareto Principle," so named after Vilfredo Pareto, the Italian economist and sociologist who postulated the theory. *See* Don Bauder, *Blame That Troublesome 20% for 80% of the Problems*, SAN DIEGO UNION TRIB., Sept. 9, 2001, at H2. Pareto was branded a fascist for supporting a theory of the superiority of the elite by virtue of his statement that twenty percent of the people will always control eighty percent of the wealth. *Id*.

identify their most profitable customers and to "fire" their unprofitable, or even less profitable, customers.[87] Furthermore, it is not beyond the imagination to expect that a customer who has been fired might also have that fact reflected in (or otherwise inferable from) their profile that is sold to the data co-op market.[88] The net effect is likely to be less access and less financial choice for the economically disadvantaged who either earn a marginal profile by virtue of their socioeconomic status or who do not produce high profit margins for a financial institution.[89]

These exclusionary decisions may be made on the basis of inaccurate assumptions. Far from being scientific,[90] the decisions generated by profiling technology may actually be discriminatory.[91] In fact, in the context of profiling by financial services, profiling may simply be a new and insidious legal form of discrimination that merely automates old-fashioned redlining practices.[92] Because the criteria used for profiling decisions are often hidden inside the "black box" of a neural network or other computer self-learning algorithm,[93] the Equal Credit Opportunity Act (ECOA),[94] which strictly prohibits discriminatory lending practices,

87. In the words of one banking software developer, "Not all customers are created equal." Stepanek, *supra* note 59, at EB 28.

88. This is the flip side of what is now occurring with regard to high-value customers who are being "bought and sold like derivative securities." *Id*. at EB 29.

89. *See* Balvinder S. Sangha, *Online Lending Brings with It Issues of Equal Credit Access*, AM. BANKER, March 16, 2001, at 17.

90. The assumptions made by computer profiling technology can be inscrutable. *See, e.g.*, Sandra Martin, *Is Little Brother Watching You?*, THE GLOBE AND MAIL REP. ON BUS. MAG., Aug. 25, 2000, at 70 (observing that Amazon.com decided author Simson Garfinkel was interested in erotic lesbian films based on his prior purchase of online women's literature and his browsing of books on computer networking), *available at* http://www.robmagazine.com/servlet/ GIS.Servlets.HTMLTemplate?tf=robm.

91. *See* Sangha, *supra* note 89. Whereas banks have historically offered equal rates for financing to all customers who met acceptable credit standards, the "risk based" pricing that transaction profiling brings will mean unaffordable financial products for some high risk consumers. Higher risk scores will be given to certain demographic groups, which may cause systematic pricing differentials that are racially defined. *Id*. Neural networks are known for making generalizations that are not contextually defined and thus could produce inapposite conclusions that exceed the most egregious form of traditional discrimination. *See* LAUDON ET AL., *supra* note 58, at 493 ("[I]t thinks everything in the shape of a car is a car, even if the shape is a paper cutout!").

92. *See* ONLINE PROFILING FTC REPORT, *supra* note 10, at 13.

93. Professor Joel Reidenberg of Fordham University remarked about the microprofiles created by value assumptions generated by self-learning neural networks: "Some of this really crosses the line into offensiveness." Stepanek, *supra* note 59, at EB 33.

94. 15 U.S.C. § 1691 (2000) (prohibiting the use of information relating to sex, race, color, religion, national origin, age, or marital status for purposes of making discriminatory credit decisions).

may be effectively skirted with probable impunity.[95] This is due to the fact that under the new one-to-one marketing regime in use by financial institutions, a consumer unfortunate enough to possess a profile that produces a substandard score from the predictive black box would be discriminated against not in the context of a credit denial per se, but rather by virtue of a marketing decision by the financial institution to either withhold the offer entirely from the consumer or to price the offer unfavorably, thus providing a disincentive to a consumer's acceptance of the financial product offering.[96] Because the decisions based on profiles are inscrutable even to the developers of the profiling software,[97] it would be difficult if not nearly impossible for the wronged consumer to prove that the criteria utilized in a decision generated by a black box was in fact discriminatory under the ECOA.[98]

These social effects are all the more disturbing when one considers that the data used to profile consumers may simply be wrong or outdated.[99] If the error rate in data utilized by the credit reporting agencies is any guideline, the error rate may be as high as forty-three percent.[100] Consumers have little opportunity to discover or correct these errors. Unlike the right of review and correction for consumer credit reports, which is codified under the Fair Credit Reporting Act (FCRA),[101] consumers currently have no notice of adverse decisions made on the basis of their transaction profiles, no mechanism to see their profiles to audit for errors, and no right of correction for erroneous

95. According to Dierdre Mulligan, staff counsel at the Center for Democracy & Technology, it is extremely hard to prove discrimination resulting from the use of personal information. Edward C. Baig et al., *Privacy: The Internet Wants Your Personal Info. What's in it for You?*, BUS. WK., April 5, 1999, at 84.

96. For example, consider a profile showing an individual who lives in a zip code classified as low income and predominantly minority, subscribes to a women's magazine, does not have a joint checking account, and regularly contributes to the local African Methodist Episcopal church. If this person is accordingly assigned a high risk score by a predictive computer model that determines that these data points are undesirable, and she is thus offered credit at prohibitively high rates or not advised of the availability of a suitable financial product at all, that (possibly legal) decision would likely have the substantially similar net effect as would an illegal denial of credit resulting from discriminatory redlining that was based specifically and demonstratively on the fact that she was a single, black female.

97. *See* Stepanek, *supra* note 59, at EB 30 (stating that scientists cannot vouch for the accuracy of conclusions nor can they determine how the technology reached any particular conclusion).

98. Some have remarked about the dearth of legislative and regulatory guidance on the subject of when risk based pricing and other decisions taken on the basis of profiling constitute an ECOA violation. *See* Sangha, *supra* note 89.

99. *See* SCHWARTZ & REIDENBERG, *supra* note 6, at 299.

100. *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 212 (1992).

101. 15 U.S.C. § 1681 (2000). For a discussion of the FCRA, see *infra* notes 197–211 and accompanying text.

data.[102] And by some accounts, banks may be relying less on consumer credit reports from the credit reporting agencies to support their consumer lending decisions, relying instead on their available transaction profiles.[103]

Although it is reasonable to price financial products differentially according to objective risk based on a consumer's credit report, payment history, or other factors with a direct and substantial link to credit risk, that is distinguishable from the practice of pricing financial products by means of predictive assumptions made by computer models based on attenuated generalizations deduced from randomly aggregated transaction patterns. The information revolution is likely to produce a structure where the disadvantaged receive less service, less choice, and less attractive terms for financial products due to discriminatory practices hidden in the guise of low profile scores.[104] The economic impacts of profiling are likely to further aggravate this situation.

B. Economic Effects: Pareto Optimal Efficiency or Market Failure?

Increased profiling and data sharing practices will modify the balance of power within the financial services industry. Financial industry spokespersons have argued that information sharing in financial services is critically necessary to allow small financial institutions to obtain a greater cache of data from marketing partners to enable them to better compete with the larger financial holding companies.[105] However, the

102. The FCRA explicitly excludes "experience information" and any information disclosed among affiliated entities from the definition of a consumer credit report. Thus this type of data is not subject to provisions in the FCRA concerning transparency, notice, and restrictions on use of consumer credit reports. *See* 15 U.S.C. § 1681a(d)(2)(A) (2000).

103. *See* H. JEFF SMITH, MANAGING PRIVACY 25–27 (1994). This practice does not make the bank a consumer reporting agency subject to regulation under the FCRA. *See infra* note 199.

104. As one letter writer to *Business Week* magazine stated the issue: "[P]ersonal information will be used to discriminate against the less successful, less healthy, or otherwise less commercially desirable among us. . . . How many companies won't be financed on the founder's credit cards because the cards weren't issued in the first place?" *Readers Report, "Weblining" Could Sideline Would-Be Entrepreneurs*, BUS. WK., April 24, 2000, at 14 (letter of David Raab).

105. The GLBA's purpose was to facilitate the affiliation of banks, insurance companies, and other financial services companies. *See* H.R. REP NO. 106-434, at 145 (1999), *reprinted in* 1999 U.S.C.C.A.N. 246. The GLBA's adherents indicated that the legislation would enable smaller financial institutions to compete with larger entities

increased information sharing and resultant profiling that is now allowed under the GLBA[106] is just as likely to create extreme competitive imbalances between the small financial institutions and the large financial holding companies. Smaller institutions rely on their ability to serve niche markets to achieve profitability.[107] However, the increased customer segmentation that will be possible with profiling may allow the larger financial holding companies to cut into those traditional niche markets that smaller institutions have traditionally served.[108] Thus, instead of helping the smaller institutions to compete with the much larger financial holding companies, the information sharing practices allowed under the GLBA may actually serve to cripple the smaller financial institutions. And small community banks and thrifts generally serve the less affluent or more rural portions of society.[109]

In addition to changing the competitive structure of the financial services industry, profiling alters the economic balance between the individual consumer and the financial institution.[110] By profiling consumers, financial institutions can predict an individual's demand and price point sensitivity[111] and thus can alter the balance of power in their price and value negotiations with that individual. Statistics indicate that the power shift facilitated by predictive profiling has proven highly

---

with affiliates, perhaps because of the power granted them to share data with unaffiliated third parties. *See* 145 CONG. REC. E2237 (daily ed. Nov. 1, 1999) (statement of Hon. James Leach) ("The power under the act will provide community banks a credible basis to compete with financial institutions of any size or any specialty and in addition to offer, in similar ways, services that new entrants into financial markets, such as Internet or computer software companies, may originate.").

106. For a description of the information sharing provisions of the GLBA, see *infra* notes 212–31 and accompanying text.

107. Robert W. Dixon, Note, *The Gramm-Leach-Bliley Financial Modernization Act: Why Reform in the Financial Services Industry Was Necessary and the Act's Projected Effects on Community Banking*, 49 DRAKE L. REV. 671, 672–75 (2001).

108. The move to Internet banking and other Web-based customer interfaces will further aggravate this trend. Forrester Research says that twenty-three percent of companies are already using the Net to "micro-segment" their customers. *See* Stepanek, *supra* note 59, at EB 29.

109. *See, e.g.*, 154 CONG. REC. S13876 (daily ed. Nov. 4, 1999) (statement of Sen. Hagel); Dixon, *supra* note 107, at 674–75.

110. Companies are able to keep what amounts to a dynamic profit and loss statement on their customers. *See* Stepanek, *supra* note 59, at EB 28. Forrester Research suggests that customers will be bought and sold "like derivative securities." *Id.* Some comments submitted to the FTC expressed the view that the targeting of consumers by profiling is manipulative. *See* ONLINE PROFILING FTC REPORT, *supra* note 10, at 14.

111. RAPP & MARTIN, *supra* note 6, at 43 (referring to this as "the great value shift," which will affect pricing as well as the value of what is sold). Some have suggested that this information imbalance could constitute a deceptive trade practice under consumer protection laws. *See* Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305, 1306 (2001).

profitable for the financial services industry.[112] However, there is little evidence that indicates that any of these profits or cost savings are being passed on to consumers. For this reason, and because most consumers have no practical ability to negotiate price terms for the exchange of their data, many characterize the commercial exploitation of consumer transaction data as a classic example of a market failure.[113]

Some have suggested correcting this market failure by creating a consumer's property right in their transaction data, thereby creating the basis for a market where data can be traded for value like any other commodity.[114] Proponents of this solution cite the resultant market efficiency benefits of an economy blessed by the ideal of classic economic theory: perfect efficiency based on perfect knowledge.[115] However, others suggest that due to valuation difficulties and the unequal bargaining positions between consumers and corporations, a property rights approach to personal information would create a market failure of even greater dimensions than what currently exists.[116] In

112. *See* Stepanek, *supra* note 59, at EB 32. Profiling enabled Sanwa Bank to realize productivity increases amounting to fourteen percent in one year, First Union saw an eighteen percent increase in one year. Visa International saves millions of dollars annually from its risk analysis technology. *Id*. at EB 28. The financial industry has the highest return of investment on a data warehouse, at close to twenty-five percent. INT'L. DATA CORP., *supra* note 43, at 9 fig.1.

113. *See, e.g.*, Pamela Samuelson, *Cyberspace and Privacy: A New Legal Paradigm? Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1127 (2000) ("[T]he company internalizes the gains from using the information but can externalize some of the losses and so has a systematic incentive to overuse it.") (quoting PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8 (1998)); Paul M. Schwartz, *supra* note 74, at 763 (a bilateral monopoly). *But see* RAPP & MARTIN, *supra* note 6, at 42 (suggesting that profiling is simply a self-defense response by business to the ever increasing competitive pressures that have resulted from the growing ability of consumers to access instant data about a product's features, price, and value).

114. *See, e.g.*, LESSIG, *supra* note 14, at 160–63.

115. *See id.* For the classic discussion of economic theory as it relates to liability rules, see Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972). Under Pareto-optimal market theory, "[i]t is the capacity of the market to induce disclosure of individual preferences which makes it theoretically possible for the market to bring about exchanges leading to Pareto optimality." *Id*. at 1095 n.13.

116. *See* Schwartz, *supra* note 74, at 763–76 (arguing against the use of a market solution based in property rights in data to provide consumers with control over their data). Schwartz feared that the commodification of personal data will result in a bilateral monopoly producing contracts of adhesion of a new dimension and a resultant market failure of monumental proportions. *Id*. at 763. *See generally* Samuelson, *supra* note 113 (arguing that a licensing approach rooted in trade secrecy law is superior to a property

addition, any scheme based on property rights necessarily encourages alienability,[117] and thus rather than discouraging the commercial exploitation of a person's identity, establishment of property rights in transaction data would likely have the effect of encouraging this exploitation by establishing the financial institution's ownership to any and all data that a consumer provided to it for purposes of a commercial transaction. In short, a property rights regime would set in motion a significant transfer of economic and market power to the data collectors.

Indeed, a theory creating a market for data seems improbable when one considers that the propertization and commodification of information actually turns classic economic theory on its head.[118] Information, unlike tangible assets, resists any real codification under an economic theory of value, because it defies measurement, it is not easily divisible or appropriable,[119] it typically is not subject to scarcity, it is not a thing that is owned by one party to the exclusion of another, it does not decrease in value with use, and it probably will not exhibit decreasing returns of marginal utility to scale.[120] In addition, information is difficult to value because it often exhibits wide divergence between its value of use and its exchange value due to the fact that it does not respond to the rules of supply and demand.[121] Market inefficiency results because a consumer is likely to part with his or her information for a much lower price than the actual value of the information to the data collector.[122]

---

rights regime). For an analysis of why a property rights theory would be unlikely to improve information privacy, see generally Jessica Litman, *Cyberspace and Privacy: A New Legal Paradigm? Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000).

117. Calabresi & Melamed, *supra* note 115, at 1092.

118. *See* Glazer, *supra* note 18, at 135.

119. One author suggests that commodifying digital information would make it an act of theft to exchange recipe ideas with a friend or neighbor, invalidating the theories of the progress of the arts and sciences that lie at the foundation of Enlightenment philosophy. Rosemary J. Coombe, *Left Out on the Information Highway*, 75 OR. L. REV. 237, 239 (1996).

120. Glazer, *supra* note 18, at 135–36.

121. *See id.*; *see also* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1502–03 (2000) (discussing how consumers underestimate the actual marginal value of their data because they are often unaware of the aggregate value of their profile); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 830–34 (2000).

> The standard definition by economists of price discrimination is that under it a seller sets 'different prices to different purchasers depending not on the costs of selling to them, . . . but on the elasticity of their demands for his product.' In contrast, privacy price discrimination involves a differentiation by data processing companies among individuals with varying preferences about the use of their personal data.

Id. (quoting R. Posner).

122. Because consumers have little ability to either reduce the supply of their data or to increase the price, a "subsidy is given to those data processing companies that

And the data collector, if not forced to internalize the costs of a consumer's privacy preferences, is likely to engage in wasteful behavior, such as increased marketing to consumers who do not desire to receive such offers.[123]

Judge Posner analyzed privacy in economic terms and concluded that the high transaction costs associated with assigning property rights to individuals in their data suggest that information secrets should become the property of those to whom they are disclosed.[124] However, Posner also suggested that this analysis is only valid where information privacy fills the role of an "intermediate good" and not the final good itself.[125] Posner suggested that where privacy becomes a final good, the economic analysis comes "to a grinding halt" because "tastes are unanalyzable from an economic standpoint."[126] But, the privacy interest in aggregated and profiled personal information cannot be looked at as merely an intermediate good, because the profile is no longer information per se, but instead is a marketable commodity.[127] And not just any commodity, but a derivative work of personal information that contains the essence of self.

---

exploit personal data." Schwartz, *supra* note 121, at 833.

123. *Id*.

124. *See* Posner, *supra* note 81, at 398. Courts considering whether a person has ownership of his biological information have arrived at a similar conclusion. *See* Moore v. Regents of the Univ. of Cal., 793 P.2d 479 (Cal. 1990) (holding that a patient did not have a conversion cause of action against his physician for use of his spleen cells to patent a cell line). The few courts that have accorded property rights in biological information to the donor have only done so where a contract between the donor and recipient established a legal obligation toward a tangible thing of value similar to a bailment. *See* Southeastern Fertility Ctr. v. Aetna Cas. & Sur. Co., No. 99-1736, 2000 WL 223339 (4th Cir. Feb. 28, 2000) (finding that sperm was personal property, and therefore, its destruction was excluded from coverage under the insurance policy exclusion for coverage of damage to the personal property of others in the care, custody, and control of the insured).

125. Posner, *supra* note 81, at 394 ("Under [the intermediate good] approach, people are assumed not to desire or value privacy or prying in themselves . . . .").

126. *Id*.

127. *See, e.g.*, GARFINKEL, *supra* note 4, at 243–53. The concept of a derivative product of transaction information that encompasses and emulates the personality is not farfetched science fiction. Technology increasingly enables the simulation of the persona, particularly the predictive agent technology that utilizes unstructured text in natural language. Such technology enables a computer to read a large set of text messages to extract pertinent information into a machine-readable form. "The profile could know every document you've ever read, every person you've ever known, every place you've ever been, and every word you've ever said that has been recorded. Your identity would no longer exist just inside of you, but in the model." *Id.* at 252. As an example of this, a computer program was developed at Yale University that emulated the personality of Cyrus Vance, responded to questions as if from his memory, and "thought of itself as Vance." *Id.*

Concerns over the potential ramifications of corporate ownership of these derivatives of personality and the potentially disturbing socioeconomic effects of profiling have driven many legal scholars to search for a legal solution to regulate or otherwise control the practice.[128] But the search for a legal oasis of privacy protection in U.S. common law and statutory authority has unfortunately led most to a destination resembling a waterless desert.[129]

IV. THE LEGAL FOUNDATIONS OF PRIVACY IN THE U.S.

"*[T]hese are the business records of the banks.*"[130]

Privacy is an ancient concept. The inviolate right of a person to a protected zone of privacy that cannot be invaded by the outside world is traceable in the earliest codification of the laws of western civilization. The Code of Hammurabi provided the death penalty for any "breach into a house."[131] The Mosaic Law provides that no man may enter into his neighbor's house to collect a pledge for a debt, but rather requires that the creditor must wait outside for the debtor to collect the pledge from inside the house and bring it out to his creditor.[132] Under Roman law the

128. *See, e.g.*, *id.* at 253 (suggesting that it may be necessary to utilize the doctrine of compilation copyright to protect against the "extraction of self"); Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U.S.F. L. REV. 633, 704 (2000) (suggesting property rights in data combined with reverse click wrap agreements); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423–28 (2000) (arguing for a fundamental right of information privacy grounded in autonomy); Susan M. Giles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy*, 43 BUFF. L. REV. 1, 52–84 (1995) (analyzing the use of the breach of confidence tort for protecting privacy, and concluding it would be unconstitutional); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1313 (2000) (concluding that a legislative solution is the best answer, but that any legislation will be watered down by special interest groups); Reidenberg, *supra* note 100, at 236–43 (arguing for the implementation of some coherent and consistent privacy rights in the U.S., but warning that any general U.S. scheme to protect privacy will need to incorporate a more flexible administrative mechanism to avoid the implementation problems seen in Europe); Francis S. Chalpowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 158–59 (1991) (arguing for a constitutional right rooted in Lockean property rights).

129. *See, e.g.*, Froomkin, *supra* note 121, at 1543 ("There is no magic bullet, no panacea. If the privacy pessimists are to be proved wrong, the great diversity of new privacy-destroying technologies will have to be met with a legal and social response that is at least as subtle and multifaceted as the technological challenge.").

130. United States v. Miller, 425 U.S. 435, 440 (1976).

131. *See* 1 ALBERT KOCOUREK & JOHN H. WIGMORE, EVOLUTION OF LAW 395 (1915).

132. *See Deuteronomy* 24:10–11. This principle is retained in the common law under which even a bailiff of the court is enjoined from entering a house to regain another's property. NELSON LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH

hearth and home was accorded the status of a sanctuary from any invader and any person entering the home of another—even to serve a summons—was guilty of invasion of privacy.[133] The concept of Roman *Injuria* also reached beyond the protections of hearth and home to include the protection of the personality and reputation. Thus, the *Injuria* of Roman law criminalized the action of shouting until a crowd gathered around an individual as well as the act of following an honest woman or young boy or girl.[134]

The expression "a man's home is his castle" predates English jurisprudence,[135] but certainly in feudal Britain, identity, self-worth and legal protection were directly linked to the land and the baronial estate.[136] As such, feudal society came to link the concept of protection from the invasions of the outside world as well as the concept of identity with the concept of real property.[137]

Perhaps upon a feudal basis linking identity with the notion of real property estates, Locke, Hume, Bentham, and others developed the Enlightenment theories of law based on proprietary rights and those rights' relationship to freedom and the inviolate self, which were the

---

AMENDMENT TO THE UNITED STATES CONSTITUTION 13–15 (1970), *reprinted in* RICHARD C. TURKINGTON & ANITA L. ALLEN, PRIVACY LAW: CASES AND MATERIALS 7 (1999).

133. *See* PRIVACY LAW: CASES AND METHODS, *supra* note 132, at 7–8; *see also* Pavesich v. New England Life Insurance Co., 50 S.E. 68, 71 (Ga. 1905) (discussing the history of the right to privacy).

134. *Pavesich*, 50 S.E. at 71; s*ee also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 n.1 (1890) ("Injuria, in the narrower sense, is every intentional and illegal violation of honour, i.e., the whole personality of another." (quoting SALKOWSKI, ROMAN LAW 668–69 n.2 (n.d.)).

135. 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 223 (1877) ("[T]he law of England has so particular and tender a regard to the immunity of a man's house, that it stiles it his castle, and will never suffer it to be violated with impunity: agreeing herein with the sentiments of ancient Rome.").

136. *See* Semayne's Case, 77 Eng. Rep. 194, 195 (K.B. 1603) ("[T]he house of every one is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose.") (citation omitted).

137. The close identification of real property rights with identity can be seen in the incidence of sumptuary laws in Renaissance Britain. The disintegration of the feudal system and the dislocation from the land and resulting problems with loss of identity among the feudal classes may have been at least partly to blame for the incidence of these laws which were instituted in Renaissance Britain in an attempt to prevent the common classes from impersonating the nobility. *See* Malla Pollack, *Your Image Is My Image: When Advertising Dedicates Trademarks to the Public Domain—with an Example From the Trademark Counterfeiting Act of 1984*, 14 CARDOZO L. REV. 1392, 1423 n.139 (1993). Pollack analogizes historical sumptuary laws to today's protection of proprietary rights under trademark law. *Id.* at 1422–28.

primary sources of the United States constitutional tradition.[138]

A. The Constitutional Basis for Financial Privacy

The right in one's own person or persona could be said to be the very foundation of the political system of the United States.[139] John Locke expressed his concept of the inviolate self: "Though the earth, and all inferior creatures be common to all men, yet every man has a property in his own person. This nobody has any right to but himself."[140] This right most often is categorized as a right of privacy in the United States legal tradition.[141] However, the term "privacy" may be an unfortunate nomenclature due to its common linkage with secrecy or facts that should be kept hidden. The right of privacy in personal information actually has very little to do with hiding things, but is instead about a foundational right of inviolate personality and about the autonomy and integrity that stems from that right.[142] Laurence Tribe expressed this concept as the "preservation of 'those attributes of an individual which are irreducible in his selfhood.'"[143] The protection of the privacy right finds its source in a constitutive right rooted in autonomy and the protection of a zone of privacy that cannot be invaded by the outside world without an individual's express consent.[144]

The most obvious articulation of the protection of the zone of privacy accorded to hearth and home is in the Fourth Amendment's guarantee of protection from unlawful search and seizure.[145] A critical test of the

138. *See, e.g.*, GERALD J. POSTEMA, BENTHAM AND THE COMMON LAW TRADITION 101–05, 183–87 (1986); LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 1310 & n.16 (1988); *cf.* Lynch v. Household Finance Corp., 405 U.S. 538, 552 (1972) ("[A] fundamental interdependence exists between the personal right to liberty and the personal right in property. Neither could have meaning without the other.").

139. *See* ALAN BRIAN CARTER, THE PHILOSOPHICAL FOUNDATIONS OF PROPERTY RIGHTS 13 (1989).

140. JOHN LOCKE, TWO TREATISES OF GOVERNMENT 128 (Mark Goldie ed., J.M. Dent 1993) (1690). Locke's self-evident natural rights were not expressly incorporated into the Constitution by its framers, but some have indicated that this omission was merely because the founding fathers deemed these rights so obvious that they did not consider them necessary to include. *See* TRIBE, *supra* note 138, at 1309–10. Early drafts of the Bill of Rights did expressly incorporate natural rights into the Constitution. *Id.* at 1310 n.14.

141. *See* TRIBE, *supra* note 138, at 1302–08.

142. *See, e.g.*, GARFINKEL, *supra* note 4, at 4.

143. TRIBE, *supra* note 138, at 1304 (quoting Paul A. Freund, Address at the American Law Institute 52nd Annual Meeting (May 23, 1975)).

144. Perhaps the best expression of this concept is crystallized in Justice Louis Brandeis's statement that privacy is simply "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men." Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

145. U.S. CONST. amend IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be

scope of the Fourth Amendment came to pass with the Supreme Court's consideration of the case of *Olmstead v. United States.*[146] *Olmstead* revealed the Court's struggle with information privacy issues inherent in the impact on society of new telecommunication technologies as well as with how the constitutional protections of human rights related to these new technologies. *Olmstead* specifically concerned the issue of wiretapping and whether the government's interception of a telephone conversation constituted an unlawful search and seizure. Unfortunately, instead of adapting the spirit of the law to the challenges of new applications, the Court retreated into formalism.[147] Thus, the majority of the Court held that because no physical entry of the house was necessary to accomplish interception of a phone conversation, and because the information was obtained by the sense of hearing and not by any actual physical entry, wiretapping did not constitute any violation of the Fourth Amendment guarantee against unlawful search and seizure.[148] Justice Brandeis wrote a seminal dissent,[149] carrying with him Justices Holmes, Stone and Butler. Brandeis expressed the importance of adapting the constitutional guarantees to changing technology[150] in prescient terms:

> In the application of a constitution, therefore our contemplation cannot be only of what has been but of what may be. . . .
>
> . . . Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. . . . Can it be that the Constitution affords no protection against such invasions of individual security?[151]

Justice Brandeis went on to assert that the framers of the Constitution, in recognition of man's spiritual nature, feelings, and intellect, conferred upon the citizens of the United States "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[152] Although formalism carried the day, the dissent carried history

violated.").

146. 277 U.S. 438 (1928).

147. ALAN F. WESTIN, PRIVACY AND FREEDOM 338–39 (1967) (concluding that the law did not catch up with the technological advances of the early twentieth century until the late 1950s).

148. *See Olmstead*, 277 U.S. at 466, *overruled by* Katz v. United States, 389 U.S. 347 (1967).

149. *Id.* at 471–85.

150. *Id*. at 473–79.

151. *Id*. at 474 (Brandeis, J., dissenting) (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

152. *Id*. at 478.

as well as the future of Fourth Amendment jurisprudence. Later, in *Katz v. United States*,[153] the Warren Court overruled *Olmstead* and required that government wiretaps meet the procedural requirements of the Fourth Amendment, including the requirement for prior judicial approval.[154]

However, since the Court's general recognition in *Katz* of the Constitution's protection of a basic zone of privacy under the Fourth Amendment,[155] information privacy rights have undergone gradual erosion. A major decision weakening the protection for information privacy was *United States v. Miller*.[156] In *Miller*, the Court held that an individual has no legitimate "expectation of privacy" in the checks and deposit slips that are disclosed to a bank in the course of the business relationship. The Court further stated that these transaction records were accorded no protection from search and seizure because they were voluntarily disclosed, were negotiable instruments and thus not confidential communications, and furthermore were deemed "the business records of the bank."[157] The Court indicated, however, that the requirement for disclosure to governmental authorities did not abrogate the pre-existing duty of the bank to ensure that the customer's financial information will "be used only for a limited purpose and the confidence placed in the [bank] will not be betrayed."[158]

A further dilution of the constitutional protection of information privacy occurred with the Court's decision in *Smith v. Maryland*.[159] In *Smith*, the Court concluded that the police may utilize a pen register in

153. 389 U.S. 347 (1967).
154. *Id*. at 358–59.
155. *Id.* at 351 ("[T]he Fourth Amendment protects people, not places.").
156. 425 U.S. 435 (1976).
157. *Id*. at 440–43. Because *Miller* permitted unlimited government access to financial records, Congress reacted by enacting the Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422 (2000), to set limits on government's free access. However, the scope of the Act is limited to controlling the disclosure of a consumer's financial information to the federal government and does not establish any limits on disclosure to private entities. *See* SCHWARTZ & REIDENBERG, *supra* note 6, at 262. The states are therefore left with the responsibility to regulate any disclosures of financial information to the private sector as well as to state and local governments. *See* L. RICHARD FISCHER, THE LAW OF FINANCIAL PRIVACY 5-2 (1983). However, a recent Supreme Court decision indicates that Congress is vested with the primary responsibility to regulate data privacy under the Commerce Clause. *See* Reno v. Condon, 528 U.S. 141, 148 (2000) (reasoning that data is a thing in interstate commerce). Because most state constitutions roughly parallel the Fourth Amendment of the U.S. Constitution with reference to search and seizure jurisprudence, state constitutions generally protect only against disclosure of personal information to governmental entities and do not concern themselves with disclosure of personal financial information to the private sector. FISCHER, *supra*, at 5-3 to 5-7.
158. *Miller*, 425 U.S. at 443. *See also infra* note 258.
159. 442 U.S. 735 (1979).

recording calls made by an individual without invoking the Fourth Amendment guarantees against search and seizure.[160] The Court reasoned that unlike the telephone conversation itself, which is accorded Fourth Amendment protection, because the telephone numbers are voluntarily disclosed to and recorded by the phone company for billing purposes, a person has no reasonable expectation of privacy in the numbers dialed.[161] The Court further stated that the caller assumes the risk that the telephone company will disclose this information to the police.[162] This decision effectively stands for the proposition that consumers have no expectation of privacy from government intrusion into their transaction data that is voluntarily disclosed in a commercial transaction. Legal scholars have criticized the Court's approach to data privacy as not appreciating the potentially invasive uses to which transaction data could be put.[163] Whether the Court will modify its position regarding a consumer's reasonable expectation of privacy in his or her transaction data in light of the increasingly invasive potential of new technologies remains to be seen.[164] But, under the current Fourth

160. *Id.* at 742.

161. *Id.* at 742–44.

162. *Id*. The Court's conception of "assumption of risk" is based on the theory that the consumer chooses to disclose information, and by this choice, forfeits any expectation of privacy that may have existed in this information. Laurence Tribe called this the "assumption of broadcast" notion and expressed the opinion that it is impossible to say that one has "assumed" a risk of surveillance where one has no other choice but to do so, based on the fact that it is not feasible to live without a telephone or a bank account. TRIBE, *supra* note 138, at 1391–92.

163. *See, e.g.*, TRIBE, *supra* note 138, at 1390–92. Tribe stated: "The Court's counter-intuitive understanding of 'assumed risks' generates a terribly crabbed sense of the contemporary possibilities for privacy." *Id*. at 1391.

164. A recent Supreme Court decision may indicate the Court's willingness to expand the reasonable expectation of privacy principle to cover information obtained by new forms of invasive technology. In *Kyllo v. United States*, Justice Scalia expanded the Fourth Amendment's protections against unreasonable searches and seizures to apply to surveillance by means of infrared heat detection sensors. Overruling the lower court decision that held that the defendant had not revealed any intimate details of the plaintiffs home, the Court held that all details in the home are deemed intimate details. Kyllo v. United States, 533 U.S. 27, 37 (2001). Moreover, the Court concluded that the "homeowner [should not be left] at the mercy of advancing technology." *Id*. at 35–36. Although the real impact of *Kyllo* is still unclear, some have suggested that the decision may bode well for such an expansion of the protection of information privacy against invasions, public and private. *See, e.g.*, William Safire, *Privacy Still Under Attack*, N. COUNTY TIMES (San Diego), June 22, 2001, at A-14 (commenting on *Kyllo*: "The Supreme Court's reaffirmation of the individual's right to privacy is heartening news to citizens who want to maintain personal control of their medical, financial and academic records, their buying habits, their genetic makeup and other intimate details of their lives.").

Amendment jurisprudence, the protection of information privacy against government invasions remains somewhat anemic.

However, the true constitutional protections of information privacy as it relates to computer profiling by governmental entities may arise not out of the Fourth Amendment, but rather out of the Fourteenth Amendment and its guarantee of due process. The Court's approach to the issue of computer profiling may be discerned from the opinion rendered in *California Bankers Ass'n v. Shultz*.[165] In *California Bankers Ass'n*, the plaintiffs challenged the constitutionality of the Bank Secrecy Act of 1970 that required banks to maintain certain records on their customers' transactions, as well as to report any transactions in currency that exceeded $10,000.[166] The Court upheld the Act without reaching any First, Fourth or Fifth Amendment claims.[167] However, the Court expressed in dicta that more difficult constitutional questions would be raised in any information-gathering program that expanded the scope of transaction data to include information that would "reveal much about a person's activities, associations, and beliefs."[168] The Court has given other indications that future technological encroachments on privacy may be met with a more forcible constitutional challenge, including questions of violations of due process rights. Justice Brennan expressed this view in his dissent in *Whalen v. Roe*,[169] where he stated: "The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology."[170]

The Fourteenth Amendment liberty interest may also guarantee a right of associational privacy and the inviolate right to "shape the 'self' that one presents to the world, and on the basis of which the world in turn shapes one's existence."[171] This constitutive right was articulated by the Court in

---

165. 416 U.S. 21 (1974).
166. *Id.* at 78.
167. *Id*. at 46–47.
168. *Id*. at 78–79 (Powell, J., concurring).
169. 429 U.S. 589 (1977).
170. *Id*. at 607 (Brennan, J., concurring). Laurence Tribe has also expressed the potential of the Fourteenth Amendment to provide protection against invasive profiling technologies as follows:

> In an information-dense technological era, when living inevitably entails leaving not just information footprints but parts of one's self in myriad directories, files, records and computers, to hold that the fourteenth amendment does not reserve to individuals some power to say when and how and by whom that information and those confidences are to be used would be to denigrate the central role that information autonomy must play in any developed concept of the self.

TRIBE, *supra* note 138, at 1400.

171. TRIBE, *supra* note 138, at 1389–90; *see also* David H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 CASE W. RES. L. REV. 831,

Whalen v. Roe[172] as the basic human right to withhold information that one does not wish to share with others.[173] The court expanded upon this aspect of the liberty interest in *Roberts v. United States Jaycees*.[174] In *Roberts*, the Court indicated that the attributes surrounding intimate associations—marriage, family, childbirth, and the raising and education of children—are protected from intrusion as an element of personal liberty.[175] The Fourteenth Amendment may therefore afford some protection against profiling activities that are found to implicate these subjects.[176]

Although it is axiomatic that the Constitution applies solely with respect to invasions to personhood by the government and not by the private sector,[177] the right of inviolate personality is still entitled to recognition as a basic tenet of our constitutional system by virtue of the states' enforcement of individual rights under the Ninth and Tenth Amendments.[178] This implied constitutive right of privacy is evidenced by the Court's protection of harm to reputation under state law in the face of a First Amendment challenge.[179] Case law has further developed this concept of linkage between the common law right of privacy and

839–41 (1991).

172. 429 U.S. 589 (1970).

173. *Id*. at 599–600. Laurence Tribe characterized this concept as one aspect of the aspiration to be the "master of the identity one creates in the world." TRIBE, *supra* note 138, at 1304.

174. 468 U.S. 609 (1984).

175. *Id*. at 619–20; *see also* United States v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989) (finding an expectation of privacy in detailed computerized records and stating that: "[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person").

176. *See* Commonwealth v. Blood, 507 N.E.2d 1029, 1034 (Mass. 1987):

> [I]t is not just the right to a silent, solitary autonomy which is threatened by electronic surveillance: It is the right to bring thoughts and emotions forth from the self in company with others doing likewise, the right to be known to others and to know them, and thus to be whole as a free member of a free society.

177. *See, e.g.*, TRIBE, *supra* note 138, at 1306 (stating that governmental coercion is accorded express constitutional limitations because it is viewed differently than the "passive, incremental coercion that shapes all of life and for which no one bears precise responsibility").

178. Katz v. United States, 389 U.S. 347, 350–51 (1967) ("[T]he protection of a person's *general* right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States.") (citations omitted); *see also* Rosenblatt v. Baer, 383 U.S. 75, 92 (1966) ("The protection of private personality, like the protection of life itself, is left primarily to the individual States under the Ninth and Tenth Amendments.").

179. TRIBE, *supra* note 138, at 1396 n.42 (collecting cases).

constitutional guarantees by grafting the Fourth Amendment "expectation of privacy" principle onto the privacy intrusion torts.[180] Because the rights enforced by the states under the Ninth and Tenth Amendments are rooted in the basic constitutional protections, any strengthening or expansion of a constitutional right in information privacy by the Court is likely to produce an equivalent level of protection of information privacy by the states with reference to private sector actions. Conversely, any reticence by the Court to extend constitutional protection to information privacy is likely to be reflected in the lower courts' unwillingness to extend similar protections in their interpretations of the common law and in legislatures' unwillingness to expand the statutory protection of information privacy.[181]

B. The Legislative Basis for Financial Privacy

The United States was the birthplace of the Code of Fair Information Practices[182] that were later the basis for Organization for Economic

180. *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977) ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."); *see also* Nader v. Gen. Motors Corp., 255 N.E.2d 765, 773 (N.Y. 1970) (comparing the protections of the Fourth Amendment to common law privacy torts); State v. Brooks, 601 A.2d 963, 969 (Vt. 1991) (comparing tort law privacy intrusion concepts to a search and seizure case). *See generally* PRIVACY LAW: CASES AND METHODS, *supra* note 132, at 80–81 (1999) (discussing the linkages between tort and constitutional protection for information privacy).

181. Fred Cate, Director of the Information Law and Commerce Institute at the Indiana University School of Law, insists that the Supreme Court is unlikely to support the constitutionality of legislation requiring opt-in consent from consumers prior to use of their personal transaction data because of "significant" First Amendment issues. *Senate Chairman Charts Legislation to Provide Privacy Opt-In*, Fed. Banking L. Rep. (CCH) No. 1921, at 1–2 (July 20, 2001). This viewpoint necessarily assumes a premise that consumers have no underlying tort action based on a reasonable expectation of privacy against the disclosure of that data to the private sector. Recognition of such an underlying cause of action would possibly change the analysis. *See* U.S. West v. Fed. Communications Comm'n, 182 F.3d 1224, 1245 (10th Cir. 1999) ("When the fundamental right to privacy clashes with the right of free expression, *the interest in privacy does not play second fiddle when the speech is merely intended to propose a commercial transaction*." (Briscoe, J., dissenting) (emphasis added) (quoting Curtis v. Thompson, 840 F.2d 1291, 1300 (7th Cir. 1988)); *see also infra* note 305.

182. The Code of Fair Information Practices is based on the following five principles:

(1) There must be no personal data-record-keeping systems whose very existence is secret.
(2) There must be a way for an individual to find out what information about him is in a record and how it is used.
(3) There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

Cooperation and Development guidelines[183] that have since been codified in the European Commission Directive on Data Protection.[184] However, in contrast to the welcome adoption of the Fair Information Practices in Europe,[185] the general U.S. legislative scheme for data privacy rights does not conform uniformly to these guidelines.[186] Instead of being unified under one data protection statute, information privacy is protected in the U.S. by sectoral-specific statutes containing inconsistent criteria for notice, choice, transparency, access, and security.[187] Examples of this are the Children's Online Privacy Protection Act of 1998 (COPPA),[188] the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[189] the Electronic Communications Privacy Act,[190] the Computer Fraud and Abuse Act,[191] the Video Privacy Protection Act

---

(4) There must be away for an individual to correct or amend a record of identifiable information about him.
(5) Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS xx-xxi (1973).

183. *See Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, O.E.C.D. Doc. No C(80)58 (final), 1981 I.L.M. 422 (Sept. 23, 1980).

184. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, T.S. No. 108, 1981 I.L.M. 317.

185. Simson Garfinkel theorizes that the reason the Health, Education and Welfare report was adopted so readily in Europe during the 1970s was because of Europe's desire not to repeat their relatively recent experiences with Nazi Germany. *See* GARFINKEL, *supra* note 4, at 7. Hitler's *schutzstaffel* used data sourced from both the public and private sectors to round up suspects for incarceration. *Id*.

186. For an analysis of the divergences between the U.S. protection of information privacy and that codified under the European Directive, see generally SCHWARTZ & REIDENBERG, *supra* note 6.

187. *See, e.g.*, Reidenberg, *supra* note 100, at 201 ("In the United States, however, no single source of privacy rights covers each data processing activity. Informational privacy rights emerge from a complex web of federal and state laws that have responded to narrowly identified problems.").

188. 15 U.S.C. §§ 6501–6506 (2000).

189. On December 28, 2000, the Department of Health and Human Services set forth its final rule for standards for privacy of individually identifiable health information, implementing certain provisions of Title II of the Health Insurance Portability and Accountability Act of 1996. The regulations are codified at 45 C.F.R. §§ 160, 164 (2001).

190. 18 U.S.C. §§ 2510–2522, 2701–2711, 3121–3127 (2000).

191. 18 U.S.C § 1030 (2000).

of 1980 (the "Bork Bill")[192] and the GLBA. There are many difficulties with a sectoral approach. Although placing different rules for protection of substantially similar data depending upon the industry sector of the data collector probably would survive an equal protection challenge, this approach may soon become unworkable and outmoded with the increasing convergence of the telecommunications sector, both internally and in combination with the financial services sector.[193]

But apart from mere inconsistency, the U.S. statutory framework addressing information privacy lacks comprehensive force by focusing primarily on the issue of disclosure to third parties instead of focusing on the permissible *uses* of data.[194] This differs fundamentally from the information privacy laws in Europe that set defined use restrictions on personal data and require the consumer's express consent for any processing activities outside of the purpose for which the data was disclosed.[195] As was suggested in Part II, intrusive invasions to privacy

192. 47 U.S.C. § 551 (West, WESTLAW through P.L. 107-209, approved Aug. 6, 2002). Under the Bork Bill, a consumer's video viewing habits may not be disclosed without his or her express consent. *Id.*; *see also* SCHWARTZ & REIDENBERG, *supra* note 6, at 314–15. The bill obtained its nickname from the circumstances surrounding the unsuccessful nomination to the Supreme Court of Judge Robert Bork. In an attempt to overturn Bork's nomination, a Washington, D.C., newspaper journalist visited a local video store Bork frequented hoping to find "dirt." Instead of pornographic films, what turned up were 146 videos consisting mostly of Disney movies and Hitchcock films. *See* GARFINKEL, *supra* note 4, at 72. But perhaps other members of Congress had more to hide, as evidenced by their enthusiastic support of the opt-in provisions for information sharing or disclosure under this bill.

193. The problems that are likely to arise with the convergence of the industry are illustrated by the court's interpretation of the Cable Act. 47 U.S.C. §§ 521–559 (West, WESTLAW through P.L. 107-209, approved Aug. 6, 2002). *See, e.g.*, Parker v. Time Warner Entm't Co., No. 98 CV 4265 (ERK), 1999 WL 1132463 (E.D.N.Y. Nov. 8, 1999). Citing the legislative history of the Cable Act, the *Parker* court held that if a customer has not opted out of information disclosures, a cable operator is permitted to disclose only "that an individual subscribes to services." Id. at *9. The cable operator is not permitted to "reveal the details of a particular transaction conducted over the cable system (such as bank-at-home or shop-at-home transaction)" even if the customer has not opted out. *Id*. However, under the GLBA, financial institutions are permitted to disclose customer experience information to third parties if they have notified their customers of this disclosure and the customer has not opted out of this disclosure. Although this inconsistency between the Cable Act and the GLBA would not be likely to invoke any equal protection issues (because these inconsistent regulations are arguably at least minimally rational), this structure is likely to set up a possible legal quagmire in determining which standard should apply if a financial holding company should ever merge with a cable company. And, because the financial services industry is becoming more and more reliant on telecommunications to compete in the information economy, such a merger may not be unlikely.

194. For a review of data protection in the United States see generally, SCHWARTZ & REIDENBERG, *supra* note 6.

195. *See* SCHWARTZ & REIDENBERG, *supra* note 6, at 12–14. The major difference between the European Union Convention and the United States' data protection scheme is that the European Union focuses on the permitted uses of data as well as disclosure,

arising from computer profiling can take place without any actual disclosure of data to third parties, and harm to a consumer may result where a commercial entity internally uses a consumer's profile to its own benefit and to the consumer's detriment. Thus, for legislation to be truly protective of information privacy, it must not only address disclosure, but must also set use restrictions precluding processing activities that exceed the scope of the initial purpose for which the data was disclosed or the scope of the consumer's reasonable expectation of privacy.[196]

Financial privacy in the United States is dealt with under two major statutes:[197] the Fair Credit Reporting Act of 1970 (FCRA),[198] which governs the reporting of consumer credit information, and the GLBA, which sets forth the rules for information sharing between financial holding companies and their affiliates and other third parties.

The purpose of the FCRA is to set forth guidelines and procedures for consumer reporting agencies with regard to their preparation and dissemination of consumer credit reports bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, if that credit report is used or collected to serve as a factor in determining the consumer's eligibility

---

whereas the United States' legislative scheme focuses solely on the disclosure of data. For example, the UK Data Protection Act 1998 provides, in part, that an individual is entitled to notify a data processor at any time to cease or not to begin processing any personal data of the data subject if that processing is "likely to cause substantial damage or substantial distress to him or to another, and . . . that damage or distress is or would be unwarranted." Data Protection Act, 1998, c. 29 § 10 (Eng.), *available at* http://www.hmso.gov.uk/acts/acts1998/19980029—b.htm.

196. For a discussion of the ambit of the consumer's reasonable expectation of privacy, see *infra* notes 158–164, 256–70 and accompanying text.

197. Three other statutes impact financial privacy. The Electronic Funds Transfer Act of 1978 establishes the guidelines for dealings between consumers and financial institutions in connection with electronic fund transactions. 15 U.S.C. §§ 1693–1693r (2000). Although the Act sets forth the requirements for collection of transaction data and requires disclosures and the provision of account statements to consumers, it does not restrict the uses of that data nor does it restrict the disclosure of that data to third parties. *See also* Reidenberg, *supra* note 100, at 214. The Equal Credit Opportunity Act also regulates financial privacy, to the extent that it regulates the use of data by prohibiting any use of information relating to sex, race, color, religion, national origin, age, or marital status for purposes of making discriminatory credit decisions. 15 U.S.C. §§ 1692b(2), 1692c(b) (2000). The Fair Debt Collection Practices Act regulates disclosures of debtors' financial information for debt collection purposes. 15 U.S.C. § 1691(a)(1) (2000). These statutes only tangentially relate to the practice of profiling and thus are not discussed in detail herein.

198. 15 U.S.C § 1681 (2000).

for household credit, insurance, or employment. The FCRA only relates to disclosures of information by consumer reporting agencies and not to disclosures of financial information by banks, insurance companies, credit card companies, and the like.[199] Unlike the other statutes addressing financial privacy, the FCRA sets defined restrictions on permissible uses of personal information. Under the FCRA, a consumer credit report may be furnished by a consumer reporting agency to a third party only for limited purposes.[200] Any subsequent use by a recipient of a consumer credit report is subject to strict guidelines for the use of that information which must be in accordance with a permissible purpose defined under the Act.[201] But the standard of care that is required of the consumer reporting agencies is to put in place "reasonable procedures"[202] so that consumer credit information is not disclosed for other than a permissible purpose. The standard of care requires consumer reporting agencies to do "what a reasonably prudent person would do under the circumstances."[203] Under the FCRA, consumers are neither provided with notice of the collection and use of the data, nor are they provided with the opportunity to opt-out of the consumer reporting agencies' collection and use.[204]

199. A "consumer reporting agency" means "any person which . . . regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f) (2000). The term "consumer reporting agency" has been narrowly construed by the courts and as such does not include banks, credit card companies, or other financial entities that collect and disseminate information based solely on their own experiences with a consumer. *See, e.g.*, Lema v. Citibank (S.D.), N.A., 935 F. Supp. 695, 697 (D. Md. 1996); Freeman v. S. Nat'l Bank, 531 F. Supp. 94, 95–96 (S.D. Tex. 1982); Nikou v. INB Nat'l Bank, 638 N.E.2d 448, 453 (Ind. Ct. App. 1994).

200. These purposes are: (1) in response to a court order, (2) in accordance with the consumer's written instructions, or (3) to a person which it has reason to believe intends to use it: (i) in a credit transaction involving the consumer, (ii) for employment purposes, (iii) for the underwriting of insurance, (iv) for determination of eligibility for a license or other benefit of a governmental instrumentality, (v) as a potential investor or servicer, or current insurer or risk assessment of an existing credit obligation, or (vi) otherwise has a legitimate business need for the information. 15 U.S.C. § 1681b(a) (2000). However, the credit reporting agency is not subject to strict liability for failure to limit the furnishing of consumer reports to the permissible purposes. Spence v. TRW, Inc., 92 F.3d 380, 383 (6th Cir. 1996). The courts balance the potential harm of inaccuracy against the burden on the agency of safeguarding against such inaccuracy. Houston v. TRW Info. Servs, Inc., 707 F. Supp. 689, 693 (S.D.N.Y. 1989).

201. 15 U.S.C. § 1681e(e) (2000).

202. *Id*. § 1681e(a). These reasonable procedures consist of requiring that users of the information identify themselves, certify the purposes for which the information is sought and to certify that it will be used for no other purpose. *Id*.

203. Dobson v. Holloway, 828 F. Supp. 975, 977 (M.D. Ga. 1993).

204. A consumer is, however, able to opt-out of the so-called prescreening practices of the consumer reporting agencies. The Act provides that a consumer reporting agency may furnish a consumer report to a third party that is not initiated by the consumer if the

Moreover, the FCRA does not provide for strict liability for errors contained in a consumer credit report, but merely imposes a duty of reasonable care.[205] The FCRA does, however, provide the consumer with the opportunity to review his or her credit report and to correct any inaccurate information.[206] The FCRA generally preempts any common law claims sounding in defamation, invasion of privacy or negligence, and provides qualified immunity for the consumer reporting agencies except where the agency furnishes false information with malice or willful intent to injure the consumer.[207]

Thus, the FCRA gives consumers very limited rights pertaining to limiting profiling activities of their transaction information. First, although the FCRA requires a consumer credit reporting agency to disclose the contents of a credit report to a consumer, the FCRA does not require disclosure to the consumer of the score that is generated by the agency's computer model or of the criteria that the agency uses to arrive at that score.[208] Second, the broadly-stated language of the FCRA establishing a permissible use for any "legitimate business need" has permitted the consumer reporting agencies, as well as recipients of the

---

transaction consists of a "firm offer of credit or insurance." 15 U.S.C. § 1681b(c)(1)(B)(i) (2000). A consumer may, however, opt-out of these disclosures by notifying the credit reporting agency that they do not consent to such disclosures to third parties. *Id*. § 1681b(e). Recently, the major consumer reporting agencies have established a central toll-free number that consumers may call to opt-out of these disclosures: 1.888.5OPTOUT. *See* BANK OF AM. CORP., BANK OF AMERICA PRIVACY POLICY FOR CONSUMERS: HOW WE PROTECT AND USE INFORMATION (2001).

205. *See Spence*, 92 F.3d 380 at 383.

206. 15 U.S.C. § 1681g (2001).

207. 15 U.S.C § 1681h (2001). The FTC is given the power to enforce the FCRA under the Federal Trade Commission Act (FTC Act), *id*. § 41, and any violation of the FCRA will be deemed an unfair and deceptive act under the FTC Act. *Id*. § 1681s. A private individual does not have the right to act as a private attorney general in enforcing the FCRA. *See* Kekich v. Travelers Indem. Co., 64 F.R.D. 660, 668 (W.D. Pa. 1974).

208. The score is most often generated by a modeling technology licensed from Fair, Isaac and Company (FICO). FICO has guarded the score as its proprietary information and only recently has provided customers the opportunity to obtain a copy of their score. *See* Fair, Isaac and Company, Inc., *myFICO—Your Source For Credit Scoring*, *at* http://www.myfico.com (last visited May 24, 2002). FICO will provide a copy of your score for a fee, currently $12.95. *Id.* FICO's scoring methodology itself is not publicly available, but FTC materials indicate that some factors included in the score are age, income, residential status (own or rent), income, and debt ratio. *See* Fair, Isaac and Company, *Credit Scoring 101, Presentation to the Federal Trade Commission available at* http://www.ftc.gov/bcp/creditscoring/present/sld001.htm, at slide 7 (July 22, 1999).

report, broad latitude in their use of personal financial information.[209]

In fact, the FCRA sets forth as one of its core purposes the maintenance and protection of the "elaborate mechanism [that] has been developed for investigating and evaluating the credit worthiness, credit standing, credit capacity, character, and general reputation of consumers."[210] In essence, the FCRA legitimizes and regulates profiling activities with reference to the consumer reporting industry. But because of its limited applicability to credit reporting agencies, it has no effect on and does not regulate the elaborate mechanisms for scoring consumer risk and behavior that have now spread to the balance of the financial services industry.[211]

The Federal Financial Modernization Act, commonly known as the Gramm-Leach-Bliley Act (GLBA) was passed by Congress and signed into law by the President in November 1999. The purpose of the GLBA was "to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance companies, and other financial service providers."[212] At the same time, Congress recognized the increased vulnerability of consumers to the dissemination of their personal financial information that such a structure would permit.[213] Thus, Congress enacted Title V of the Act for purpose of ensuring that "each financial institution ha[ve] an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic

209. However, the D.C. Circuit has recently upheld the FTC's interpretation that a targeted marketing list generated by a consumer reporting agency is included in the ambit of a "consumer report" under the FCRA and that targeted marketing was not a permissible purpose under the Act. Trans Union Corp. v. F.T.C., 245 F.3d 809, 812, 819 (D.C. Cir. 2001), *cert denied*, 122 S. Ct. 2386 (2002).

210. 15 U.S.C. § 1681(a)(2) (2000). This elaborate mechanism was found by Congress to be critical to the continued health of the banking system. *Id*. § 1681(a)(1).

211. In fact, a recent decision limiting the ability of the credit reporting agencies to disclose personally identifiable financial information to direct marketers may forge a new alliance between the financial services industry (which is not generally subject to the FCRA strictures) and the direct marketing association for purposes of the profiling of consumer transaction information. *See* Individual Reference Servs. Group v. F.T.C., 145 F. Supp. 2d 6 (D.D.C. 2001), *aff'd*, Trans Union LLC v. F.T.C., 295 F.3d 42 (2002). In *Individual Reference Services Group*, the district court upheld an FTC regulation that prevented the credit reporting agencies from distributing credit header, tradeline, or aggregate data obtained from financial institutions. The appeals court upheld the district court decision, but refused to rule on the permissible uses of data aggregated by the CRAs, stating that the issue was "not yet ripe" because the FTC had "not determined whether or to what extent aggregation should be considered 'use'" under the applicable FTC regulation. *Trans Union LLC*, 296 F.3d at 51. This decision effectively places the FTC in the crucial role of defining (or perhaps of declining to define) the parameters for data aggregation and profiling of financial information permitted under the GLBA.

212. H.R. CONF. REP. NO. 106-434, at 245–46 (1999).

213. *See* H.R. REP. NO. 106-74, pt. 3, at 98 (1999).

personal information."[214] Under the Act, the regulators are given discretion to establish standards for financial institutions in the protection of the security and confidentiality of customer records and information.[215] These include (1) to insure the security and confidentiality of customer records and information, (2) to protect against any anticipated threats or hazards to the security or integrity of such records, and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[216] The GLBA extends its authority over "financial institutions," which are defined broadly as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of title 12."[217]

Although the GLBA sets forth as one of its core purposes the prevention of the unauthorized use of personal financial information which could result in substantial harm or inconvenience to any customer,[218] the Act fails to set any express use restrictions on information and instead codifies a mechanism for permissible disclosures to third parties. The GLBA prohibits financial institutions from disclosing to nonaffiliated third parties any nonpublic personal information, unless that consumer has first been provided with a notice that permits the consumer to opt-out of those disclosures.[219] A financial institution must "clearly and conspicuous[ly]"[220] disclose to a consumer its practices with regard to (1) disclosure of nonpublic personal information to affiliates and nonaffiliated third parties, (2) disclosure of nonpublic personal information of persons who have ceased to be its customers, and (3) its measures to protect a consumer's nonpublic personal

214. 15 U.S.C. § 6801(a) (2000).
215. *Id*. § 6802.
216. *Id*.
217. *Id*. § 6809(3)(A).
218. *See, e.g*., Joan P. Warrington, *Synopsis of S. 900 Gramm-Leach-Bliley Act, Title V—Privacy*, *in* ALI-ABA COURSE OF STUDY MATERIALS: FINANCIAL SERVICES MODERNIZATION (2000), *available at* LEXIS SEA1 ALI-ABA 213, 215 ("This broad language could be construed by regulators to allow issuance of regulations much broader than the statutory language. Certainly, the concept of customer 'inconvenience' is a troublesome standard, one that could be exploited by class action lawyers. For example, telemarketing and spam could be considered inconveniences.").
219. 15 U.S.C. § 6802 (2000).
220. Some have suggested that the notices sent by financial institutions were far from clear or conspicuous. *See Confusing Privacy Notices Leave Consumers Exposed*, USA TODAY, July 9, 2001, at 13A. An ABA survey indicated that forty-one percent of respondents could not recall receiving the prescribed privacy notices. *Id*. Perhaps as a result, less than one percent of consumers have opted-out of information sharing. *Id*.

information.[221] However, under the GLBA a consumer is not empowered to prevent a financial institution's disclosure of his or her nonpublic personal information to its affiliates.[222] Nor may a consumer prohibit a financial institution from sharing such information with "a nonaffiliated third party . . . perform[ing] services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions,"[223] provided that the financial institution "fully discloses" this type of activity to the consumer.[224]

Thus, the GLBA does not provide a consumer with any substantive protection against the profiling of his or her financial information. First, although the GLBA does permit a consumer to prevent the sharing of his or her personal financial information with nonaffiliated third parties, the Act provides no protection whatsoever against the sharing of a consumer's financial information with the financial institution's affiliates or by the financial institution's marketing partners.[225] In addition, the exception for disclosure to affiliates provides a very broad carve out to the Act's limits on disclosure to third parties. And, the permitted disclosures to financial institutions under joint marketing agreements have been described by some as including "everything but the kitchen sink" because of the expansive definition of the term "financial institution" under the Act.[226]

---

221. 15 U.S.C. § 6803(a) (2000).

222. *Id*. § 6802(b)(2) (2000).

223. The exception for marketing partners was a last-minute addition to the legislation, without a full conference committee debate, at the behest of industry lobbyists such as GE Capital Services, Inc. *See* Michael Schroeder, *Late Requests for Favors and Fixes Precede Votes on Landmark Overhaul*, WALL ST. J., Nov. 5, 1999, at A2. Some have suggested that this exception, as well as the exception for affiliates, negates any real privacy protection under the bill. William Raspberry, *Privacy: The Horse Has Left the Barn*, WASH. POST, June 25, 2001, at A15, *available at* http://www.washingtonpost.com/wp-dyn/opinion/A41200-2001Jun24.html.

224. 15 U.S.C. § 6802(b)(2). The method, frequency and standard for "fully discloses" is not defined in the Act.

225. The potential scope of disclosures to affiliates is illustrated by several of the recent mergers that have resulted from the liberalization of the banking industry: the creation of Citigroup by the merger of Citicorp and Travelers; Royal Bank of Canada's acquisition of the life insurance subsidiaries of Liberty Corporation, Dexia's acquisition of Financial Security Assurance and MetLife, Inc.'s, acquisition of Grand Bank N.A. of Kingston, N.J. *See* Wolcott B. Dunham, Jr. et al., *Financial Services Reform: The New Business of Banking and Insurance Under Gramm-Leach-Bliley*, 2001 PRACTISING L. INST., GRAMM-LEACH-BLILEY UPDATE 121, 123–24.

226. Neal R. Pandozzi, *Beware of Banks Bearing Gifts: Gramm-Leach-Bliley and the Constitutionality of Federal Financial Privacy Legislation*, 55 U. MIAMI L. REV. 163, 193 (2001) (explaining that a financial institution includes "any institution that engages in activities that are financial in nature, incidental to such financial activity or complementary to a financial activity").

Second, the Act gives consumers no knowledge or control over the uses of their nonpublic personal information by the financial institution, by the financial institution's affiliates, by the financial institution's marketing partners, or (if they failed to opt-out) by nonaffiliated third parties. In addition, the annual notices that a financial institution is required to send to a consumer must only describe the financial institution's practices concerning the disclosure and security procedures in regard to the nonpublic personal information, not the uses to which this information may be put. In fact, at least one bank that formerly did provide its customers with notice of its profiling practices has now deleted that information from its privacy policy with the enactment of the GLBA.[227]

Third, the likely effect of the GLBA will be to increase the incidence of profiling. Your bank now may become a financial holding company, and may act as banker, insurance provider, realtor, and stock broker. The resulting scope and breadth of the data aggregations that are thus created may open the floodgates to data sharing and data profiling. Under the GLBA, consumers who fail to opt-out may be assumed to have waived any express or implied restrictions on disclosure of their financial information to third parties.[228] The wealth of personal financial data thus available for marketing purposes, combined with the effect of recent case law decisions limiting such uses by the credit reporting agencies,[229] may have the effect of forging a stronger alliance between

---

227. *See* FTC INFO MARKETPLACE, *supra* note 5 (remarks of Ms. Culnan). Mary Culnan, Slade Professor of Management and Information Technology at Bentley College in Waltham, Massachusetts, conducts research on information privacy. She made the following remarks at the FTC's Public Workshop on the Information Marketplace:

> [T]here was one excellent financial services notice about enhancement that basically said, ["]We do profiling, we do data mining, we acquire third-party data, non credit report data, to understand how you use our card and we use this to serve you better,["] and they had an opt-out form right with the notice, and you could mail that back or call the 800 number. *Unfortunately, with the Gramm[-]Leach[-]Bliley requirement, that doesn't cause companies to have to specify how they're going to use information, just what they collect and who they disclose it to. That very nice statement disappeared from the Gramm[-]Leach[-]Bliley notice that this company has sent out, which is now their de facto privacy notice*.

Id. (emphasis added).

228. *But see infra* Part V.C.

229. *See generally* Individual Reference Servs. Group v. F.T.C., 145 F. Supp. 2d 6, 32 (D.D.C. 2001), *aff'd*, Trans Union LLC v. F.T.C., 295 F.3d 42 (2002) (holding that consumer reporting agencies are precluded from disclosing their "credit header" information on consumers to third parties without abiding by the notice provisions of the

financial institutions and the direct marketing industry.

The GLBA allows the states to craft greater protection for nonpublic personal information under state legislation, except to the extent of any inconsistency with the GLBA. The Act expressly explains that a state law is not deemed inconsistent with the GLBA if the law provides protection greater than that provided under the Act.[230] Bills have been introduced into Congress to modify the GLBA to eliminate the exception for information sharing among affiliates and to require opt-in prior to any information sharing. However, intense industry lobbying activities at the state and federal level indicate that it will be extraordinarily difficult to establish legislation providing any greater protection for nonpublic financial information than that which currently exists under the GLBA.[231]

V. WHERE DO WE GO FROM HERE: A COMMON LAW SOLUTION

"*Law never is, but is always about to be.*"[232]

In light of the paucity of constitutional and legislative protections against invasions of information privacy by the private sector, is there a common law right that will afford a solution? Prior to his tenure on the Supreme Court, Justice Louis Brandeis wrote a law review article in conjunction with his friend from Harvard Law School, Samuel Warren, entitled, "*The Right to Privacy*."[233] This law review article was destined

---

GLBA). Thus, financial institutions are likely to become the data vendor of choice for the Direct Marketing Association. Because the consumer reporting agencies do not have direct relationships with individual consumers, the ruling effectively precludes the agencies' sale of this data to marketers. And obtaining consumer financial data from financial holding companies rather than credit reporting agencies obviates the necessity of abiding by the fair information practices that restrict the permitted uses of credit data under the FCRA. *See supra* note 211 and accompanying text.

230. 15 U.S.C. § 6807 (2000).

231. Rachel Zimmerman & Glenn R. Simpson, *Lobbyists Swarm to Stop Tough Privacy Bills in States*, WALL ST. J., April 21, 2000, at A16; Robert Salladay, *Davis May Weaken Privacy Measure*, N. COUNTY TIMES (San Diego), Aug. 3, 2001, at A-3; Editorial, *Davis Stands Privacy Bill on Its Head*, N. COUNTY TIMES (San Diego), Aug. 31, 2001, at A-18.

232. BENJAMIN N. CARDOZO, The Method of Sociology, The Judge as Legislator, Address Before the Law School of Yale University (1921), *in* THE NATURE OF THE JUDICIAL PROCESS 98, 126 (1921).

233. Warren & Brandeis, *supra* note 134, at 193 (articulating some of the same concepts that were later repeated in Brandeis' *Olmstead* dissent). The similarities between the language of the law review article, which concerned itself with the civil protections of the right to privacy, and the *Olmstead* dissent, which related to the constitutional right to privacy, would indicate that Brandeis saw a theoretical link between the common law right to privacy and the constitutional protection of the liberties of man against government oppression. "The common law has always

to become known as the "outstanding example of the influence of legal periodicals upon the American law."[234] *The Right to Privacy* leads off with the assertion that the "recognition of man's spiritual nature, of his feelings and his intellect" have broadened the natural rights of man to include the "right to be let alone."[235] The article went on to trace the development of the civil protection of this right through the tort actions of battery, assault, nuisance, slander and libel, the protection of intellectual property, and finally to the fullest and highest expression of this liberty right which is found in the law's protection of the right to privacy.[236] Some have characterized the Warren and Brandeis law review article as a response to the yellow journalism and "kodakers" found in Boston of the late 1800s.[237] However, a reading of the close parallels of the law review article to Brandeis' *Olmstead* dissent may indicate that the article was not a statement about the overreaching of the press,[238] but rather it was an expression of Brandeis' prescient concern over the invasive potential of technology and the importance of the growth of the law to "defin[e] anew the exact nature and extent of [full protection of the individual in person and in property] in light of that invasiveness."[239]

---

recognized a man's house as his castle . . . [s]hall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?" *Id*. at 220.

234. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 383 (1960).

235. Warren & Brandeis, supra note 134, at 193.

236. *Id*. at 193–95.

237. *See*, *e.g.*, ALAN WESTIN, PRIVACY AND FREEDOM 338 (1967) (referring to use of the "instantaneous photography" perfected by Kodak in the late 1880s). Following this line of reasoning, Dean William Prosser wrote that the article was penned as a response to Samuel Warren's annoyance at the invasive behavior of the press at the wedding of Warren's daughter. Prosser, *supra* note 234, at 383. Prosser surmises that "she must have been a very beautiful girl. . . . This was the face that launched a thousand lawsuits." *Id*. at 423. Although great prose, Prosser's tale may be apocryphal. Warren married in 1883 and Warren's daughter was only six years old in 1890 when the article was published. *See* LEWIS J. PAPER, BRANDEIS 35 (1983). In addition, modern researchers have found scant evidence of an abusive form of journalism in Boston in the 1890s. *Id*.

238. In fact, the article goes to great lengths to set forth the applicable limits to the right of privacy that protect the First Amendment rights of the press for matters of public or general interest, establish privileged communications, and set forth protection for oral publications. Warren & Brandeis, *supra* note 134, at 214–17.

239. *Id*. The article expressly mentioned concern over the protection of the "right to be let alone," in view of "recent inventions and business methods," "mechanical devices," and "instantaneous photographs," along with the "intensity and complexity of life" brought on by "modern enterprise and invention." *Id*. at 195–96. These concerns

The New York Court of Appeals was one of the first courts to deal with the privacy gauntlet that Warren and Brandeis had thrown down in *The Right to Privacy*. And the court's swift response was to reject the right of privacy in its entirety.[240] The court explained its reasoning to the effect that the introduction of such a right would usher in vast amounts of litigation and it would be impossible to demarcate the line between a plaintiff's right of privacy and the rights of others.[241] The response of the legal community to this decision was generally that of regret.[242] Three years later, in *Pavesich v. New England Life Insurance Co.*,[243] the Georgia Supreme Court criticized the New York decision in a

about modern technology are echoed in Brandeis's *Olmstead* dissent. Olmstead v. United States, 277 U.S. 438, 473–78 (1927). Indeed, one biographer of Louis Brandeis reports that the fervor of Brandeis's dissent may have been driven at least in part by his concern over General Electric Corporation's RCA subsidiary's development of television and its potential for government surveillance uses. An early draft of Brandeis's dissent read that: "Through television, radium and photography, ways may soon be developed by which the Government can, without removing papers from secret drawers, reproduce them in court." PAPER, *supra* note 237, at 312. The Warren Court later vindicated many of the views Brandeis set forth in the *Olmstead* dissent. *See supra* notes 152–153 and accompanying text. However, the Supreme Court, by its failure to give express protection against the invasiveness of modern profiling technologies, has not yet given full vindication to Brandeis's views that the Fourth and Fifth Amendments should protect against "[a]dvances in the psychic and related sciences [that] may bring means of exploring unexpressed beliefs, thoughts and emotions." *Olmstead*, 277 U.S. at 474.

240. Roberson v. Rochester Folding Box Co., 64 N.E. 442, 447–48 (N.Y. 1902). In *Roberson*, a woman sued to recover for damages caused by humiliation and sickness on account of a flour milling company's reproduction of her image, without her consent, on its boxes of flour next to the advertising slogan, "the flour of the family." *Id*. at 442. The trial court had held that the woman had a right of property in her own self, and thus denied the defendant's demurrer. *Id*. at 442. The defendant appealed and the New York Court of Appeals, in a four-to-three decision, reversed, holding that there was no right of privacy as a matter of law. *Id*. at 447–48.

241. *Id*. at 443. Some have traced New York Supreme Court Chief Justice Parker's reticence to accord protection to the right of privacy to the fact that he subscribed to the theory of legal positivism that "views 'law' as consisting solely of an objectively determined body of enactments, principles, doctrines and rules which are fixed in advance of litigation." PRIVACY LAW: CASES AND METHODS, *supra* note 132, at 54–55.

242. *See* Pavesich v. New England Life Ins. Co, 50 S.E. 68, 79 (Ga. 1905) (listing critical law review articles). An editorial in the *American Law Review* offered the opinion that the decision "shocks and wounds the ordinary sense of justice of mankind." *Right to Privacy: Injunction Denied a Young Woman to Restrain the Publication of Her Portrait on Commercial Packages for the Purpose of Advertising*, 36 ALR 614, 636 (1905). The New York legislature quickly responded to the decision by enacting Sections 50 and 51 of the New York Civil Rights Act which provided a statutory cause of action for invasion of privacy. N.Y. CIV. RIGHTS LAW §§ 50–51 (McKinney 2001). Section 50 reads as follows: "A person, firm or corporation that uses for advertising purposes, or for the purposes of trade, the name, portrait or picture of any living person without having first obtained the written consent of such person . . . is guilty of a misdemeanor." *Id*. § 50.

243. 50 S.E. at 68. In *Pavesich*, an insurance company had used plaintiff's photograph in an advertisement for insurance containing a false statement of plaintiff's

similar fact situation in which a photograph of the plaintiff was used to market a life insurance product. The court penned an elaborate opinion tracing the history of privacy from early civilization as justification for the rationale that privacy was a natural right of man. Justice Cobb depicted the right of privacy as rooted in the liberty interest to be free from commercial exploitation as follows:

> The knowledge that one's features and form are being used for such a purpose . . . brings . . . the person . . . to a realization that his liberty has been taken away from him . . . he is no longer free, and . . . he is, in reality a slave without hope of freedom, held to service by a merciless master.[244]

The *Pavesich* decision gave common law legitimacy to the right of privacy introduced by Warren and Brandeis, and other courts generally followed the decision.[245]

More than fifty years later, Dean Prosser took a look at the legal landscape of privacy and compared it to "a haystack in a hurricane"[246] due to the utter disarray and confusion in the law. So Prosser set forth to codify the right of privacy into four causes of action which, although dissimilar in the scope of circumstances they covered, had as their unifying principle that "each represents an interference with the right of the plaintiff . . . 'to be let alone.'"[247] Prosser delineated these four torts as follows:

(1) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;
(2) Public disclosure of embarrassing private facts about the plaintiff;
(3) Publicity which places the plaintiff in a false light in the public eye; and

---

endorsement of defendant's life insurance products that was published in the *Atlanta Constitution*. *Id*. at 68. The plaintiff sued on the right of privacy, alleging that the statement attributed to him was offensive. *Id*. at 69. While the dissent in *Roberson* unsuccessfully relied on Lockean property rights to justify a right of privacy, *Roberson*, 64 N.E. at 448–51, Justice Cobb in *Pavesich*, while relying in part on Judge Grey's *Roberson* dissent, instead relied on a natural rights theory. *Pavesich*, 50 S.E. at 73–74.

244. *Pavesich*, 50 S.E. at 80.

245. For the historical listing of cases and statutes recognizing the right of privacy after the *Pavesich* decision, see Prosser, *supra* note 234, at 386–88 nn.17–58.

246. Prosser, *supra* note 234, at 407 (quoting Biggs, J., in Ettore v. Philco Television Broad. Co., 229 F.2d 481, 485 (3d Cir. 1956)).

247. Prosser, *supra* note 234, at 389 (quoting THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS 29 (2d ed. 1888)).

(4) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness[248]

Prosser's theory of the four-fold manifestation of the tort received some initial disagreement.[249] But eventually Prosser's analysis prevailed as the general standard, receiving codification in the *Restatement (Second) of Torts*[250] and, as such, serves as the basis for most states' common law privacy doctrines. Of these categories, the intrusion on seclusion and the appropriation torts may provide protection against profiling.

A. Intrusion on Seclusion

The tort of intrusion on seclusion occurs when "[o]ne . . . intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person."[251] This form of invasion of privacy focuses on the manner in which the information is obtained and implicates the "use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs."[252] The tort therefore does not require any actual disclosure of the information to a third party to be actionable.[253] Public information is not protected under the tort, and the intrusion must therefore invade the zone of "private seclusion that the plaintiff has thrown about his person or affairs."[254] The crux of the tort is that the intrusion must be highly offensive to a reasonable person. And the standard for "highly offensive" turns on whether the plaintiff has a reasonable expectation of privacy against that intrusion.[255]

Because the intrusion must abrogate the plaintiff's reasonable expectation of privacy, is the applicability of the intrusion tort to disclosures of financial information to the private sector therefore

248. *Id.*

249. *See, e.g.*, Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964); Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34 (1967); *see also infra* notes 278–281 and accompanying text.

250. RESTATEMENT (SECOND) OF TORTS § 652 (1977).

251. *Id.* § 652B.

252. *Id*. at cmt. b. The *Restatement (Second) of Torts* gives the following as examples of actionable behavior: opening a person's mail, searching a person's wallet, and *viewing his private bank account*. *Id*. (emphasis added).

253. *See Id*. at cmt. a.

254. *Id*. at cmt. c.

255. *See* White v. White, 781 A.2d 85, 91–92 (N.J. 2001) (reasoning that the definition of what is highly offensive to a reasonable person turns on one's reasonable expectation of privacy, which is measured objectively).

hampered by the Supreme Court's decision in *Miller*? Because the Court in *Miller* held that a bank customer has "no expectation of privacy" against disclosure of his financial information to governmental authorities,[256] some have generalized this principle and have concluded that a consumer also has no reasonable expectation of privacy against disclosure of his or her financial information to a private sector actor.[257] But, in fact, the Court in *Miller* was careful to distinguish the Fourth Amendment expectation of privacy (that is, where financial records are provided to the government under a subpoena duces tecum) from a situation where a consumer's financial records are disclosed to the private sector.[258]

Some have also taken the holding in *Miller* to stand for the principle that an individual has no legitimate expectation of privacy in business records that have been voluntarily conveyed to the bank and have thus become the bank's property.[259] According to this line of reasoning, the

256. United States v. Miller, 425 U.S. 435, 442–45 (1976).

257. *See* FISCHER, *supra* note 157, at 5-8 (suggesting that the lack of a reasonable expectation of privacy in financial data precludes any liability under the intrusion tort unless the financial institution acts in an unreasonable or outrageous manner). A senior bank official at a large credit card company stated that information sharing by banks with third parties has "long been a standard industry practice" and is given endorsement by federal regulators as being "a reasonable part of commerce." *See* Lisa Fickenscher, *Chase Pact in N.Y. Shows How States Could Set Privacy Rules*, AM. BANKER, Jan. 27, 2000, at 1.

258. United States v. Miller, 425 U.S. 435, 443 (1976) (holding that the plaintiff did not have a *constitutionally* protected zone of privacy in financial records). The Court's holding was quite narrow and limited any disclosure to the context of a narrowly-focused subpoena duces tecum, which was therefore subject to the accordant legal restraints. The Court distinguished its holding from a fact pattern implicating a "wide-ranging inquiry that 'unnecessarily touches upon intimate areas of an individual's personal affairs.'" *Id*. at 444–45 n.6 (quoting Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 78–79 (1974)). Notwithstanding the absence of a constitutionally protected zone of privacy in financial information, the Court acknowledged the duty that is incumbent upon a financial institution to protect this information from disclosure to the private sector:

> This court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to *Government* authorities, even if the information is revealed on the assumption that *it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed*.

Id. at 443 (emphasis added).

259. *See, e.g*., CATE, *supra* note 9, at 15 (citing *Miller* for the proposition that it is "fundamentally unfair [to prohibit] financial institutions from using . . . information that they have spent millions of dollars collecting and in which they have a legally recognized property interest"). A. Michael Froomkin called this phenomenon the "joint and several ownership of the facts of a transaction." Froomkin, *supra* note 121, at 1502.

bank is free to do whatever it wants with any personal financial information in its possession. The Indiana Court of Appeals recently was asked to review the *reductio ad absurdum* of this syllogism—in a slightly different context—and rejected it in its entirety with the following statement:

> It does not follow that one gives up all expectations of privacy and therefore, waives all [privacy] claims . . . when voluntarily revealing one's affairs to a third party. . . . [T]o the extent that our [prior holding] . . . may be read to align fourth amendment expectation of privacy analysis with the tort of invasion of privacy in general, we disaffirm such a reading.[260]

The existence of a reasonable expectation of privacy against disclosure to the private sector is also substantiated by holdings in actions arising out of the Freedom of Information Act (FOIA).[261] In the context of the government's disclosure of an individual's personal information to the private sector, the federal courts have found a reasonable expectation of privacy in names and addresses,[262] in information concerning private activities, and in activities taking place in the home.[263] Furthermore, in this context, at least one court has found a significant privacy interest in financial information that is combined with names and addresses.[264]

The reasonable expectation of privacy in financial information is further demonstrated by the protection accorded to financial information under the breach of confidence tort.[265] The duty of confidentiality is based on precedent found in English common law.[266] Many state courts have adopted the English precedent and accord a duty of confidentiality towards any information learned "in the character of a banker."[267] Such

260. Pohle v. Cheatham, 724 N.E.2d 655, 660 (Ind. Ct. App. 2000). In *Pohle*, Cheatham had taken compromising pictures of his ex-wife with her permission. *Id.* at 657. The pictures were deemed Cheatham's property by virtue of the divorce decree. *Id.* Cheatham then proceeded to post these pictures in conspicuous places around town. *Id.* at 657. Pohle sued, premised on a public disclosure of private facts cause of action. *Id.* at 657–58. Cheatham raised the defense of waiver, relying on Fourth Amendment jurisprudence, arguing that because the plaintiff had voluntarily "taken the risk in revealing [her] affairs to third parties that the information will be conveyed by that person to law enforcement officials" she therefore had no reasonable expectation of privacy in the photographs. *Id*. at 660. The court held for the plaintiff. *Id*. at 661.

261. 5 U.S.C § 552 (2000).

262. HMG Mktg. Assoc. v. Freeman, 523 F. Supp. 11, 14 (S.D.N.Y. 1980).

263. Wine Hobby USA, Inc. v. United States, 502 F.2d 133, 137 (3d Cir. 1974).

264. Aronson v. U.S. Dep't of Hous. and Urban Dev., 822 F.2d 182, 186 (1st Cir. 1987).

265. For a discussion of the breach of confidence tort see, Susan M. Gilles, *Promises Betrayed: Breach of Confidence As a Remedy for Invasions of Privacy*, 43 BUFF. L. REV. 1, 57 n.250 (collecting cases).

266. Tournier v. Nat'l Provincial & Union Bank of Eng., 1 K.B. 461 (Eng. C.A. 1924).

267. *See* McGuire v. Shubert, 722 A.2d 1087, 1091 (Pa. 1998). For states adopting

information must not be disclosed to third parties, except under compulsion of law, for prevention of crime or fraud against the bank or a third party, or with the implied or express consent of the customer.[268] Judicial precedents are not in accord as to the source of the duty of confidentiality, but some trace its basis in the right of privacy.[269] One court expressed the parallel between the duty of confidentiality and the reasonable expectation of privacy as: "A bank customer's *reasonable expectation* is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes."[270]

Furthermore, the second branch of the tort is satisfied by the fact that intrusion into personal financial affairs by a third party is highly offensive to a reasonable person.[271] Profiling is especially intrusive, and can reveal intimate details of a person's activities, associations, and beliefs. Profiling therefore could easily be found to intrude into the zone of seclusion that a person throws about his affairs.[272] Because the reasonable expectation of privacy is often defined with reference to general social norms,[273] the high incidence of consumer discomfort with financial profiling[274] further demonstrates the strength of the reasonable

---

the *Tournier* doctrine, see FISCHER, *supra* note 157, at 5-10 to 5-16.

268. *See generally* FISCHER, *supra* note 157, at 5-10 to 5-16. Fischer observes that the Tournier doctrine is basically identical to the scope of consumer privacy outlined by the Right to Financial Privacy Act of 1978, 12 U.S.C. § 3403(c)–(d) (2000). FISCHER, *supra* note 157, at 5-11.

269. *See, e.g.*, *McGuire*, 722 A.2d at 1091 ("It is an implied term of the contract between the banker and his customer that the banker will not divulge to third persons, without the consent of the customer, express or implied, either the state of the customer's account or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his account." (quoting Peterson v. Idaho First Nat'l Bank, 367 P.2d 284, 290 (Idaho 1961)); *see also* DAVID A. ELDER, THE LAW OF PRIVACY 370 (1991 & Supp. May 2001) (implied contract). FISCHER, *supra* note 157, at 5-15 (implied contract). But there is considerable legal confusion over the source of this duty and whether it actually arises in tort. *See* Giles, *supra* note 128, at 18 n.86 & 55 nn. 245–51 (collecting cases).

270. Burrows v. Superior Court, 529 P.2d 590, 593 (Cal. 1974) (emphasis added).

271. *McGuire*, 722 A.2d at 1092.

272. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977). This may be analogized to the Supreme Court's protection of a zone of privacy in intimate associations from state intrusion under the Fourteenth Amendment. *See supra* notes 165–76 and accompanying text.

273. *See, e.g.*, State v. Hempele, 576 A.2d 793, 802–03 (N.J. 1990).

274. Statistics reveal that at least ninety-five percent of people questioned would be either not very comfortable or not at all comfortable with the creation of a profile that contained their financial data. *See supra* note 10 and accompanying text.

expectation of privacy in financial information.

Therefore, the intrusion on seclusion tort is likely to provide a basis of relief against intrusive computer profiling activities in the financial services industry. However, in alignment with the parameters of the duty of confidentiality, the tort would not be implicated where the financial institution used the consumer's information for internal banking purposes incident to the normal course of a business transaction. Liability under the tort would probably be limited to situations where information is collected in an unreasonably intrusive manner or when the consumer's profile is used to facilitate offensive marketing or discriminatory scoring activities.

B. The Appropriation Privacy Tort

The appropriation privacy tort may also provide a basis to prevent profiling activities by effectively setting restrictions on the permissible uses of personal financial information. As the appropriation tort is set out in the *Restatement (Second) of Torts*, the cause of action presents the following deceptively simple formulation: "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."[275] In order to determine if the appropriation privacy tort can afford a remedy against computer profiling, the following four questions must be answered: (1) what is the nature of the interest protected, (2) what are the aspects of identity, (3) how is the interest invaded, and (4) what constitutes an "appropriation" for purposes of the tort?

1. The Nature of the Interest Protected: A Right Just for Blondes, "Kings," and Legends, or a Right for the Rest of Us?

As expressed in Part III of this Comment, information privacy is unlikely to be accorded any real protection by virtue of consumers being assigned property rights in their transaction data. For this reason, many who have looked at the possible applicability of the appropriation privacy tort for solving issues of information privacy have concluded that it was unsuitable for this application by virtue of the fact that it was inherently a property right.[276] This Part seeks to demonstrate that the appropriation privacy tort is in fact not a property right that capitalizes

275. RESTATEMENT (SECOND) OF TORTS § 652C (1977).

276. *See, e.g.*, Schwartz, *supra* note 74, at 778–79 ("The misappropriation tort safeguards the monetary value of the kind of self-revelation that our culture associates with celebrity status. . . . But the misappropriation tort will not establish constitutive privacy's domains of access and non-access to information.").

on a person's ability to recover from the "user's failure to pay" for the use of his or her likeness, but rather is a personal right rooted in the injury to sensibilities that occurs with the shock of confronting the commercialization of one's own self.[277]

The early disagreement over Prosser's codification of the right to privacy arose out of some legal scholars' concern with Prosser's implication of a "proprietary" interest[278] as the rationale for the appropriation tort, as

---

277. *See* James M. Treece, *Commercial Exploitation of Names, Likenesses, and Personal Histories*, 51 TEX. L. REV. 637, 641 (1973). It should probably be noted at this point that Thomas J. McCarthy cautions against the use of the labels of "personal rights" and "property rights" to describe the appropriation privacy and right of publicity torts, respectively, because these attributions flow from and do not create the difference between the right of privacy and the right of publicity. McCarthy stresses that the crucial difference between the rights is the nature of the right invaded. In Mr. McCarthy's words, the right of publicity protects the pocketbook, and the right of privacy protects the psyche. Once this distinction is understood, Mr. McCarthy advises that the labels of property versus personal rights may follow without the danger of having us march "lock-step into any preconceived result." 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 5:65, at 5-121 (2d ed. 2001).

278. *See* PROSSER & KEETON ON THE LAW OF TORTS 854 (W. Page Keeton gen. ed., student ed. 1984 & Supp. 1988) ("[T]he effect of the appropriation decisions is to recognize or create an exclusive right in the individual plaintiff to a species of trade name, his own, and a kind of trade mark in his likeness. . . . [I]t is at least clearly proprietary in its nature."). In accord with Prosser's depiction of the appropriation right of privacy as proprietary in nature, the *Restatement (Second) of Torts* defines the interest protected as follows:

> The interest protected . . . is the interest of the individual in the exclusive use of his own identity, in so far as it is represented by his name or likeness, and in so far as the use may be of benefit to him or to others. Although the protection of his personal feelings against mental distress is an important factor . . . the right created by it is in the nature of a property right, for the exercise of which an exclusive license may be given to a third person.

RESTATEMENT (SECOND) OF TORTS § 652C cmt. a (1977).

However, it is probable that Prosser viewed the creation of a proprietary interest as based in the tort's protection against mental anguish. Prosser later clarified his position on the basis for the proprietary nature of the interest protected in a little-known German law review article published in 1956. In this article Prosser explained that his intent was to create a right similar to the German right of personality. The German right of personality protects both mental and commercial rights but is a personality right and not an assignable property right. *See* PINCKAERS, *supra* note 8, at 94 & n.156 (citing William Prosser, *Das Recht auf die Privatsphäre in Amerika,* 21 ZEITSCHRIFT FÜR AUSLÄNDISCHES UND INTERNATIONALES PRIVATRECHT 401, 404 (1956)). The rush to proclaim the appropriation privacy a property right from Prosser's statement that it protected a proprietary interest may have been premature, in the light of the analysis of Calabresi and Melamed that a liability rule can have the effect of producing a licensable entitlement, and not a property right per se, particularly where social or economic factors mitigate against allowing alienability of the entitlement. *See* Calabresi & Melamed, *supra* note 115, at 1111–15. Prosser clearly stated that the four torts covered under right

distinguished from the intrusion, false light, and disclosure of private facts torts, which otherwise protect a right of inviolate personality and the right to be let alone. These scholars rested their arguments on Warren and Brandeis's clear delineation of the right of privacy as not as implicating any right of private property, but as a form of *injuria*, a cause of action similar to battery—that of the right to one's "inviolate personality."[279] Legal scholars thus countered Prosser's codification by reasoning that the right of privacy should remain as a unified tort based solely in the protection of human rights.[280] Prosser's somewhat equivocal approach to the issue was to admonish that disputes over whether the appropriation privacy tort constituted a property right were "pointless."[281]

Thus, despite its humble beginnings rooted in the protection of the common man against commercial appropriation of his name or photograph, the appropriation privacy tort was promptly and expeditiously high-jacked by a parade of celebrity litigants who perhaps saw in the tort a means of licensing their celebrity images without being hampered by the statutory limitations normally imposed on intellectual property rights.[282] This rather striking development initially gave many

---

of privacy were not alienable rights. Prosser, *supra* note 234, at 408 ("[T]he plaintiff's right is a personal one . . . . The right is not assignable."). For a further review of the German right of personality, see 2 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 6:154, at 6-300 to 6-302 (2d ed. 2001); *see generally* Susanne Bergmann, *Publicity Rights in the United States and in Germany: A Comparative Analysis,* 19 LOY. L.A. ENT. REV. 479 (1999).

279. Warren & Brandeis, *supra* note 134, at 205, 207, 231. *But see id*. at 205 n.1 (indicating proprietary nature of unpublished manuscripts which, although not property, may be an incorporeal right or "substantial right of legal interest").

280. *See* Bloustein, *supra* note 249, at 962.

281. Prosser, *supra* note 234, at 406 ("It seems quite pointless to dispute over whether such a right is to be classified as 'property.' If it is not, it is at least, once it its protected by the law, a right of value upon which the plaintiff can capitalize by selling licenses." (citations omitted)).

282. This parade has included the likes of Elvis Presley (as represented by the heirs, licensees and executors), Vanna White, Johnny Carson, Bette Midler, Michael Jordan, and numerous other celebrities, authors, musicians, sports legends, scientists, and other world-famous luminosities. *See, e.g.*, Hoffman v. Capital Cities/ABC, Inc., 255 F.3d 1180, 1183 (9th Cir. 2001) (Dustin in a designer dress); Groden v. Random House, Inc., 61 F.3d. 1045, 1048 (2d Cir. 1995) (suit over defendant's aspersions of Groden's Kennedy assassination theory); Cher v. Forum Int'l, Ltd., 692 F.2d 634, 636–37 (9th Cir. 1982) (Cher sues *Forum Magazine* over publication of an exclusive interview with *US Magazine*); Ruffin-Steinback v. dePasse, 82 F. Supp. 2d 723, 726 (E.D. Mich. 2000) (publication of life story of former member of the Temptations), *aff'd*, 267 F.3d 457 (6th Cir. 2001); MJ & Partners Rest. v. Zadikoff, 10 F. Supp. 2d 922, 930 (N.D. Ill. 1998) (licensees sue over exclusive use of Michael Jordan's name in connection with Chicago area restaurants); Sagan v. Apple Computer, Inc., 874 F. Supp. 1072, 1074 (C.D. Cal. 1994) (Carl Sagan sues for his name being used as a code name for a new computer, which code was later changed to "Butt-Head Astronomer"); Estate of Elvis Presley v. Russen, 513 F. Supp. 1339, 1348, 1359 (D.N.J. 1981) (suit over Elvis impersonation,

courts pause with reference to the internal conflicts inherent in applying a privacy tort to a celebrity whose very fame required widespread recognition and public use of their identity in a commercial context.[283] This concern set in motion the establishment of a separate cause of action for celebrity publicity rights, the right of publicity.[284] Thomas P. McCarthy, in his treatise on privacy and publicity, expressed the differences between the appropriation right of privacy and the right of publicity as follows:

> The right of publicity is now a separate and distinct legal concept which recognizes the proprietary and commercial value of a person's identity and persona. Simply put, an infringement of the right of publicity focuses upon injury to the pocketbook, while an invasion of "appropriation privacy" focuses upon injury to the psyche.[285]

Nevertheless, the question of the correct classification of the appropriation privacy tort, and whether it protects a human right or a property interest, continues to be debated to this day.[286] And, because of

The Big El Show); Stern v. Delphi Internet Servs. Corp. 626 N.Y.S.2d 694, 695 (Sup. Ct. 1995) (internet service provider's publication of Mr. Stern's posterior).

283. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 46 cmt. b (1995) (commenting on some courts' refusal to apply the privacy tort action to celebrities).

284. The New York Court of Appeals attempted to solve this problem by establishing the right of publicity as a separate tort from the appropriation right of privacy in Haelan Labs. Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866, 868 (2d Cir. 1953). Later, an influential legal scholar defined the need for the right of publicity in a law review article. Melville Nimmer, *The Right of Publicity*, 19 LAW & CONTEMP. PROBS. 203 (1954). Nimmer distinguished the right of publicity, a property right, from the appropriation privacy tort, a personal right. *Id.* at 203. Nimmer is described by Thomas P. McCarthy as the "first builder of the right of publicity." MCCARTHY, *supra* note 277 § 5:64, at 5-119. The Supreme Court, influenced by the views of Nimmer, followed with its own legitimization of the publicity tort, classifying it as a separate cause of action from the right to privacy in the celebrated "human cannonball" case, Zacchini v. Scripps-Howard Broad. Co. 433 U.S. 562, 572–73 (1977). Later, the American Law Institute gave the right of publicity its own separate codification as a right protecting the value inherent in a celebrity's name, apart from the right of privacy. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 46 cmt. a (1995).

285. MCCARTHY *supra* note 277 § 5:61, at 5-110; a*ccord* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 49 cmt. b (1995) ("The history of the publicity tort . . . ha[s] created confusion regarding the appropriate measure of damages. The right of publicity protects the commercial value of a person's identity . . . . [P]rotection is available under the right of privacy for the personal interest in controlling the use and exploitation of one's own identity.").

286. MCCARTHY, *supra* note 277 §§ 5:59 to 5:65, at 5-107 to 5-122; *compare id.* at 5-115 ("Modern decisions clearly distinguish between the various types of privacy and the right of publicity."), *with* ELDER, *supra* note 269, at 375 ("[M]ost more modern decisions have emphasized that the tort protects a 'valuable right of property in the

the lack of clarity on this point, and regardless of Prosser's careful four-tort classification schema, the law concerning the appropriation privacy tort is repeatedly compared to a "haystack in a hurricane",[287] particularly with respect to the question of the proprietary nature of the tort.

But, a review of the case law carefully distinguishing between cases that are pleaded and decided under the appropriation privacy tort versus those pleaded and decided under the right to publicity, reveals a consistent trend of the courts to treat the appropriation right of privacy as a personal right, distinct from the right to publicity.[288] Furthermore, the gravamen of the appropriation privacy tort lies not in protecting a valuable *thing* against any loss of income from licensing revenues,[289] but rather in the right to define a zone of inviolate personality into which commercial interests cannot intrude. Another way of stating this distinction is that the right of publicity is analogous to an intellectual property right,[290] whereas the appropriation privacy right is analogous to

---

broadest sense of that term.'" (quoting McQueen v. Wilson, 161 S.E.2d 63 (Ga. 1968), *rev'd on other grounds,* Wilson v. McQueen, 162 S.E.2d 313 (Ga. 1968))). Mr. Elder distinguishes between the right of publicity and the right of privacy only as it relates to the issue of damages and bases the gravamen of the tort on property rights and the prevention of unjust enrichment. *Id*. at 375–79.

287. *See, e.g.*, Uhlaender v. Henricksen, 316 F. Supp. 1277, 1279 (D. Minn. 1970) (Neville, J., despairing of the continuing lack of consistency in the state of the law).

288. *See e.g.*, Prima v. Darden Rests., Inc., 78 F. Supp. 2d 337, 346 (D.N.J. 2000) (acknowledging that majority trend is that privacy and publicity fall under separate and distinct torts); Sagan v. Apple Computer, Inc., 874 F. Supp. 1072, 1079 (C.D. Cal. 1994); KNB Enters. v. Matthews, 92 Cal. Rptr. 2d 713, 717 (Ct. App. 2000); Martin Luther King, Jr. Ctr. for Soc. Change, Inc. v. Am. Heritage Prods., Inc., 296 S.E.2d 697, 703 (Ga. 1982) (the fundamental distinction is the measure of damages); Bear Foot, Inc. v. Chandler, 965 S.W.2d 386, 389 (Mo. Ct. App. 1998) (collecting cases). *But see* Allison v. Vintage Sports Plaques, 136 F.3d 1443, 1447 (11th Cir. 1998) (distinction largely semantic); Uhlaender v. Henricksen, 316 F. Supp. 1277, 1279–80 (D. Minn. 1970) (misappropriation involves pecuniary loss). Most recent decisions are fairly consistent in their holdings that the appropriation right to privacy is a personal right, unlike the right of publicity, which protects against commercial harm and otherwise provides for a property right in the *persona. See, e.g.*, Dora v. Frontline Video, Inc., 18 Cal. Rptr. 2d 790, 792 (Ct. App. 1993); Hudson v. Montcalm Publ'g Corp., 379 S.E.2d 572, 576–77 (Ga. Ct. App. 1989); Jones v. Hudgins, 295 S.E.2d 119, 121–22 (Ga. Ct. App. 1982); Hetter v. State, 874 P.2d 762, 764–65 (Nev. 1994); Faber v. Condecor, Inc., 477 A.2d 1289, 1294–95 (N.J. Super. Ct. App. Div. 1984). Staruski v. Cont'l Tel. Co., 581 A.2d 266, 268 (Vt. 1990). *But see* Matthews v. Wozencraft, 15 F.3d 432, 437–38 (5th Cir. 1994) (equating misappropriation with the expropriation of goodwill); MJ & Partners Rest. v. Zadikoff, 10 F. Supp. 2d 922, 930 (N.D. Ill. 1998) (reasoning that the appropriation privacy tort protected property rights, but eventually recognizing the existence in Illinois a common law right to publicity instead).

289. The term "property" refers to legal relations between people with respect to things and is used to describe a bundle of rights in the thing. The property bundle of rights is as follows: "1) the right of possession, use and fruits or profits of the thing; 2) the right to exclude others; [and] 3) the right to dispose of (e.g., to alienate) the thing." PINCKAERS, *supra* note 8, at 263.

290. And indeed, many courts have utilized concepts from intellectual property law

the right to be free from defamation or battery.[291] However, as opposed to most torts protecting personal rights, the appropriation tort is complete without proof of emotional distress or economic damage to the plaintiff. The focus of the tort is the defendant's intentional use of the plaintiff's identity for the defendant's benefit. Thus, damages under the tort may stem either from the harm suffered by the plaintiff or may be calculated with reference to the economic benefit accruing to the defendant.[292]

2. What are the Aspects of Identity and the Characteristics of Its Indicia?

A second aspect of the nature of the privacy interest has to do with what constitutes a "name" or "likeness" under the tort. The appropriation tort includes under its protective ambit any appropriation of a name or likeness for one's use or benefit.[293] If a computer profile is a likeness, it could come under the protection of the tort. Although limited under some privacy statutes,[294] the majority of courts give a broad definition to the indicia of identity.[295] In essence, the tort has the capacity to protect any tangible expression of identity that can be identified by others as a

in their analysis of the right of publicity. *See, e.g.*, Allison v. Vintage Sports Plaques, 136 F.3d 1443, 1448 (11th Cir. 1998) (applying the first-sale doctrine). For an analysis of the right of publicity as an intellectual property right see PINCKAERS, *supra* note 8, at 263–80; *cf.* Alice Haemmerli, *Whose Who? The Case for a Kantian Right of Publicity*, 49 DUKE L.J. 383 (1999) (applying copyright doctrines to publicity while also theorizing that a Kantian foundation more accurately reflects the value of the human being behind the *persona* at issue).

291. Laurence Tribe has suggested a parallel between the "psychic mayhem" caused by violence to one's personal identity and the physical injury caused by a battery. TRIBE, *supra* note 138, at 887–88.

292. *See, e.g.*, Harbin v. Jennings, 734 So. 2d 269, 273 (Miss. Ct. App. 1999) (Invasion of privacy in this type of action is an intentional tort and thus actual injury is not essential to establish a case of liability, and nominal damages would apply).

293. RESTATEMENT (SECOND) OF TORTS § 652C (1977).

294. Some courts have drawn very narrow interpretations of these terms and have thus delimited the concept to include only name or photographic likeness, although most often this form of interpretive analysis arises in the context of statutory, and not common law, privacy causes of action. Wilkinson v. Methodist, Richard Young Hosp., 612 N.W.2d 213, 216 (Neb. 2000) (concluding that under Nebraska's privacy statute that computer records could not constitute a form of "name or likeness," because the statute only mentioned photographs or other similar likenesses).

295. The author of the major treatise on privacy and publicity, Thomas McCarthy, describes the cause of action as covering use of any "aspect of the plaintiff's identity or persona in such a way that plaintiff is identifiable from defendant's use." MCCARTHY, *supra* note 277 § 5:60, at 5-109.

symbol of the personality.[296] The Ninth Circuit in *White v. Samsung*[297] moreover indicated a preference for maintaining open, expansive definitions of the contours of what might constitute identity. In *White*, the court indicated it was not disposed to any set delineation of what factors can constitute the identity under the right of publicity, because of its concern that such a formulation would present an invitation to sharp practices and abuse of the law.[298]

When the concept of identity is applied to a transaction profile, a computer profile should be found to be an expression of the personality in the same way that a signature, a voice, or a computer-altered photograph has been found to be an expression of the personality. Precedent indicates that courts are willing to admit identification of the persona through extrinsic indicia, even where resemblances to the plaintiff are completely and obviously artificial.[299] These extrinsic indicia do not have to be visual, but refer to any capture of identity.[300]

---

296. Very broad judicial interpretations to the dimensions of the aspect of identity revealed in the persona have been found under the right of publicity. *See, e.g*., Hoffman v. Capital Cities/ABC, Inc., 255 F.3d 1180, 1183 (9th Cir. 2001) (computer-altered image); Midler v. Ford Motor Co., 849 F.2d 460, 463 (9th Cir. 1988) (voice); Carson v. Here's Johnny Portable Toilets, Inc., 698 F.2d 831, 833, 835 (6th Cir. 1983) (nickname associated with phrase implicating play on words, "The World's Foremost Commodian"); Motschenbacher v. R.J. Reynolds Tobacco Co., 498 F.2d 821, 822, 827 (9th Cir. 1974) (picture of a car identifiable with racecar driver Lothar Motschenbacher); Michaels v. Internet Entm't Group, Inc., 5 F. Supp. 2d 823, 828 (C.D. Cal. 1998) (videotape); Uhlaender v. Henricksen, 316 F. Supp. 1277, 1282 (D. Minn. 1970) (statistics); Comedy III Prods., Inc. v. Gary Saderup, Inc., 21 P.3d 797, 799 (Cal. 2001) (lithographic reproduction), *cert. denied*, 122 S. Ct. 806 (2002); Palmer v. Schonhorn Enters., Inc., 232 A.2d 458, 459, 462 (N.J. 1967) (statistical profile). The right of publicity is analogous to the right of privacy when assessing the definition of identity. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 46 cmt. a (1995) ("Although not directly applicable, the rules stated here may be useful by analogy in evaluating claims under the right of privacy arising from an unauthorized commercial exploitation of a person's identity."). The Ninth Circuit even accorded the distinction of the persona of Vanna White on a robot in a blonde wig. White v. Samsung Elecs. Am. Inc., 971 F.2d 1395, 1396–97 (9th Cir. 1992); *accord*, Wendt v. Host Int'l, Inc., 125 F.3d 806, 810–11 (9th Cir. 1997) (allowing plaintiffs to proceed with proof that the robots bore sufficient resemblance to the plaintiffs); *see also* Landham v. Lewis Galoob Toys, Inc., 227 F.3d 619, 624–25 (6th Cir. 2000) (noting that the right of publicity will "cover anything that suggests the plaintiff's personal identity" (collecting cases)); Mark D. Robins, *Publicity Rights in the Digital Media, Part I*, THE COMPUTER & INTERNET LAW., Nov. 2000, at 7–8.

297. *White*, 971 F.2d at 1395.

298. *Id*. at 1398 ("A rule which says that the right of publicity can be infringed only through the use of nine different methods of appropriating identity merely challenges the clever advertising strategist to come up with the tenth.").

299. *See* Robins, *supra* note 296, at 7 (citing the *White* and *Wendt* decisions as examples of identification through extrinsic indicia).

300. This is not to say that a profile could not eventually take the form of a visual representation of an individual. *See* MCCARTHY, *supra* note 278 § 8:122, at 8-200 to 8-202 (discussing how recent technology permits the scanning of an individual's image to create a digital reproduction that can be manipulated in a computer. This technology

And, indeed, at least one court has indicated that computerized records contained in a database represent an identity for purposes of the tort.[301]

Second, aggregated financial data is also particularly likely to evoke identity because of its essentially biographical nature. Financial data has been called a "virtual current biography" of an individual.[302] Biographical information of any type, when used for a defendant's commercial benefit, has traditionally brought liability under the tort.[303] The rule is generally stated that, absent some redeeming social value or newsworthiness exception, any use of biographical information for commercial purposes without the subject's express consent is actionable under the tort.[304] To carry this analysis forward and apply it to the practice

permits the so-called "rotoscoping" of an image so that it is now possible to superimpose an image of a deceased actor into a live scene interacting with live actors); *see also* PINCKAERS, *supra* note 8, at 419–20 (stating that technology may soon provide Hollywood with the option of using reanimated actors rather than hiring the real one). The potential for the combination of profiling and rotoscoping and the possible uses to which these combined technologies might be put is quite intriguing.

301. Weld v. CVS Pharmacy, Inc., No. 98-0897F, 1999 WL 494114, at *6–7 (Mass. Super. June 29, 1999) (holding that records in a computer database are a name or likeness under both the common law and the Massachusetts privacy statute) [hereinafter Weld I]; c*f.* Crump v. Forbes, 52 Va. Cir. 52, 55 (Cir. Ct. 2000) (holding that an Internet domain name is a name under Virginia's statutory right of action).

302. United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting).

303. Palmer v. Schonhorn Enters., Inc., 232 A.2d 458, 462 (N.J. 1967) (holding that the use of statistical or biographical data for the purpose of capitalizing upon the name of the individual by using it in connection with a commercial project other than the dissemination of news or articles or biographies provided liability under the appropriation privacy tort); *accord* Uhlaender v. Henricksen, 316 F. Supp. 1277, 1283 (D. Minn. 1970). The tort is invoked by virtue of the unconsented *use* of the information for some benefit of the defendant. *See* Tellado v. Time-Life Books, Inc., 643 F. Supp. 904, 909–10 (D.N.J. 1986) (holding that the infringing use must be mainly for purposes of trade, without a redeeming public interest, news or historical value); *Palmer*, 232 A.2d at 462 ("[A]lthough the publication of biographical data of a well-known figure does not per se constitute an invasion of privacy, the use of that same data for the purpose of capitalizing upon the name by using it in connection with a commercial project other than the dissemination of news or articles or biographies does."); Flores v. Mosler Safe Co., 164 N.E.2d 853, 857 (N.Y. 1959) (distinguishing use of photo in item of general public interest and information versus "a use in, or as part of, an advertisement or solicitation for patronage"); Rall v. Hellman, 726 N.Y.S.2d 629, 632 (App. Div. 2001) (stating in dicta that a fabricated e-mail discussion may have been actionable under the appropriation tort if it had attracted customers to defendant's Web site); Stern v. Delphi Internet Servs. Corp. 626 N.Y.S.2d 694, 697 (Sup. Ct. 1995) (commenting that if the ads at issue used plaintiff's name and likeness to advertise products unrelated to news dissemination, plaintiff would have stated a claim for relief).

304. *See* RESTATEMENT (SECOND) OF TORTS § 652C cmt. c (1977). Because the cornerstone of the tort is appropriation for purposes of taking advantage of some value associated with an individual, biographical information that is published for a

of profiling, a financial institution's use of a customer's transaction data for marketing purposes in no way provides newsworthy information to the public. Nor does it fill a socially useful purpose or substantially add to cultural values. Rather, the sole purpose behind profiling and the sale of profiled information by financial institutions is to enable the financial institutions to increase their profitability and market dominance. Therefore the use of a consumer's transaction data for marketing purposes is not likely to be subject to the newsworthiness exception.[305]

A third approach to demonstrating that a computer profile is a form of identity under the appropriation tort is to recognize that the data profile may be a type of photograph. Photography can no longer be defined as a chemical process.[306] Because photographs and other visual images are now often created, stored, and transferred in a digital form, a photograph is now most accurately defined as data that, when combined in aggregate form, creates an image that invokes an associational linkage to a distinct and recognizable individual.[307] Thus, a photograph is just another form of information. And aggregated information, when profiled, creates the

---

newsworthy, parody or entertainment purpose is not actionable. *Id*. at cmt d.

305. One very attractive feature of the appropriation tort may be its ability to sustain most First Amendment challenges. Although the issue has not yet been passed upon by the Supreme Court, the appropriation branch of the right of privacy, being a personal right with proprietary overtones, is likely to trump the somewhat limited First Amendment protections that are accorded to commercial speech under the *Central Hudson* balancing test. Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 566 (1980). "The Constitution . . . accords a lesser protection to commercial speech than to other constitutionally guaranteed expression." *Id.* at 562 (citation omitted). *But see* U.S. West Inc. v. F.C.C., 182 F.3d 1224, 1237–38 (10th Cir. 1999) (striking down an FCC order restricting the use, disclosure and access to a telecommunications customer's proprietary network information without the customer's prior express opt-in to the disclosure, because the regulation did not directly and materially advance the government's interest in privacy). But if profiling activities are deemed to be more deceptive than informational in character, the activity would probably receive no First Amendment protection. *Central Hudson,* 447 U.S. at 563 ("The First Amendment's concern for commercial speech is based on the *informational* function of advertising. Consequently, there can be no constitutional objection to the suppression of commercial messages that do not accurately inform the public about lawful activity. *The government may ban forms of communication more likely to deceive the public than to inform it*." (emphasis added) (citations omitted)). However, the regulation of computer profiling activities may escape First Amendment scrutiny altogether. The Supreme Court has also indicated that computer processing is a "thing in interstate commerce," and thus the First Amendment protections of commercial speech may be completely inapposite to data profiling and, possibly, to data exchange. *See* Reno v. Condon, 528 U.S. 141, 148 (2000).

306. *See* WEBSTER'S NEW WORLD DICTIONARY 1102 (college ed. 1964) (defining photography as a process "producing images of objects upon a photo sensitive surface by the chemical action of light or other radiant energy").

307. *See* LAUDON ET AL., *supra* note 58, at 26. In the words of Bill Gates, "The world is totally going digital." *Id.* This digitization means that information of all types, television, movies, telecommunications, books, home shopping and bill paying, and all other forms of audio and video images will soon take the uniform form of digital bits. *See id.*

same associative capture of identity as does a photograph. In fact, some technical literature describing the technology of profiling uses the illustrative example of a phased-resolution digital photograph to depict how the increased aggregation of information will eventually produce a "clear enough image of your customer that you can create and market a product to her that will fit her like a glove."[308] Personally identifiable transaction data, when profiled, can thus be described as a personality "portrait"[309] or behavioral photograph of an individual, and it should reasonably receive the same level of protection under the appropriation tort as does its photographic counterpart.

An analysis of the interrelation of the appropriation and publicity torts with copyright law further shows that the exact tangible expression of the identity is somewhat irrelevant and that the material issue is whether the subject's persona is identifiable by the tangible expression. The law is settled that the persona is not copyrightable.[310] Although it is not settled to what extent and in what circumstances copyright pre-emption does or does not apply to the persona,[311] cases dealing with copyright pre-emption generally demonstrate that the persona is distinct and separate from the tangible expression of the persona that may be subject to copyright law.[312] There is some quality of a person's being that,

308. *Id*. at 442.

309. ONLINE PROFILING FTC REPORT, *supra* note 10, at 16 ("[T]he [ac]cumulation over time of vast numbers of seemingly minor details about an individual produces a portrait that is quite comprehensive and, to many inherently intrusive.").

310. *See* 1 MELVILLE NIMMER, NIMMER ON COPYRIGHT § 1.01[B][1][c], at 1-24 (2001) ("A *persona* can hardly be said to constitute a 'writing' of an 'author' within the meaning of the Copyright Clause of the Constitution. *A fortiori*, it is not a 'work of authorship' under the Act." (citations omitted)).

311. *See, e.g.*, Mark D. Robins, *Publicity Rights in the Digital Media, Part II*, THE COMPUTER & INTERNET LAW., Dec. 2000, at 29, 32 ("[I]t is far from clear that the aspects of the actor's identity can be separated from the copyrightable dramatic performance and given protection without eviscerating the [copy]right to prepare derivative works.").

312. *See, e.g.*, Brown v. Ames, 201 F.3d 654, 658–59 (5th Cir. 2000) (holding that the tort of misappropriation protects a person's persona, which is not copyrightable because it does not consist of a writing of an author; placement in or on a tangible medium does not change this analysis); Midler v. Ford Motor Co., 849 F.2d 460, 462 (2d Cir. 1981) ("A voice is not copyrightable. . . . What is put forward as protectible here is more personal than any work of authorship."); Prima v. Darden Rests., Inc., 78 F. Supp. 2d 337, 352–53 (D.N.J. 2000) (finding that a voice is not copyrightable, as distinguished from the copyrightable recording of a voice); Michaels v. Internet Entm't Group, Inc., 5 F. Supp. 2d 823, 836–37 (C.D. Cal. 1998); KNB Enters. v. Matthews, 92 Cal. Rptr. 2d 713, 722–23 (Ct. App. 2000) (holding that because a persona is not copyrightable, the unauthorized publication is not the equivalent of a copyright infringement claim and is not preempted). The legislative history also indicates congressional intent to not apply

although captured by a tangible medium, is distinct from the tangible medium. Thus, what constitutes an indicia of the persona relates simply to whether the tangible expression is evocative of and identifiable to an individual, and not to the material form or substance of the tangible medium. Profiled financial data is distinctly identifiable by virtue of an account number or social security number that relates the profile to a particular person. A profile is furthermore evocative of the data subject in that it derives its market value by virtue of its ability to create an identification with, and by its ability to predict the behavior of a particular person. Thus, a computer profile should unquestionably be found to constitute an indicia of identity.

3. How Is the Interest Invaded?

The appropriation privacy tort is typically invaded by the defendant's advertising use of the plaintiff's identity.[313] Although some courts have sought to limit the tort's coverage to *only* apply to advertising use,[314] the law does not restrict the tort in this way.[315] But in general, advertising use is broadly construed by the courts,[316] and includes any form of use that might be an advertisement in disguise.[317] Furthermore, no actual endorsement of a product by the plaintiff is necessary to establish an advertising use.[318] Profiling could easily be found to constitute advertising use because profiling facilitates marketing activities targeted individually at the consumer for purposes of inducing the consumer to purchase particular products or services. Thus, even though technology provides the capacity to advertise to a micro-segmented audience of only one individual, it is still advertising toward that one individual. And because the tort does not require any actual endorsement of a product by the plaintiff, the fact that the advertising is directed back at the data subject himself, rather than at third parties, should not make any difference for

---

copyright pre-emption to the persona. *See* H.R. REP. NO. 1476, at 132 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5748 ("The evolving common law rights of 'privacy,' 'publicity' and trade secrets . . . would remain unaffected as long as the causes of action contain elements, such as an invasion of personal rights or a breach of trust or confidentiality, that are different in kind from copyright infringement.").

313. 62A AM. JUR. 2D *Privacy* § 77 cmt. (1990).

314. *See, e.g.*, Matthews v. Wozencraft, 15 F.3d 432, 439 (5th Cir. 1994); Shibley v. Time, Inc., 341 N.E.2d 337, 339 (Ohio Ct. App. 1975).

315. RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (1977) ("[The tort] applies . . . when the defendant makes use of the plaintiff's name and likeness for his own purposes and benefit, even though the use is not a commercial one, and even though the benefit sought to be obtained is not a pecuniary one.").

316. 62A AM. JUR. 2D *Privacy* § 77 (1990) (defining advertising use as "the use of a person's name or picture for all types of promotional endeavors").

317. *See* Matthews v. Wozencraft, 15 F.3d 432, 440 (5th Cir. 1994).

318. Flores v. Mosler Safe Co., 164 N.E.2d 853, 857 (N.Y. 1959).

purposes of defining profiling as advertising under the tort.

But, the tort also includes within its parameters any other use of the plaintiff's persona that accrues to the defendant's benefit.[319] The concept of benefit has been broadly defined and, unless otherwise limited by statute, does not require that the benefit be economic.[320]

Profiling handsomely benefits a financial institution. And it is immaterial for purposes of the appropriation tort whether that benefit comes in the form of the economic benefits of increased sales generated by targeted marketing or through the increased profits from risk-based credit pricing, or in the somewhat less tangible goodwill that accrues to the financial institution through increased customer satisfaction or efficiency.

4. What Constitutes an Appropriation?

Assuming that profiling provides a benefit to financial institutions by means of the use of consumers' identities, it is then necessary to continue the analysis to determine whether profiling also implicates an appropriation. Appropriation under the tort occurs only where the defendant "appropriate[s] to his own use or benefit the reputation, prestige, social or commercial standing, public interest or other values of the plaintiff's name or likeness."

---

319. For instance, liability under the tort has been found where a defendant derived some benefit from the impersonation or mimicry of an individual. *See e.g.*, Wendt v. Host Intern., Inc. 125 F.3d 806, 809 (9th Cir. 1997) (robot look alike); Waits v. Frito-Lay Inc., 978 F.2d 1093, 1096 (9th Cir. 1992) (sound alike); White v. Samsung Elecs. Am., Inc., 971 F.2d 1395, 1396 (9th Cir. 1992) (robot look alike); Midler v. Ford Motor Co., 849 F.2d 460, 463–64 (9th Cir. 1988) (sound alike); Prima v. Darden Rests., Inc., 78 F. Supp. 2d 337, 339–41 (D.N.J. 2000) (sound alike); Onassis v. Christian-Dior N.Y., Inc., 472 N.Y.S.2d 254, 256, 263 (App. Div. 1984) (look alike). Of course, any discussion of the right of publicity would not be complete without an Elvis case. *See, e.g.*, Estate of Elvis Presley v. Russen, 513 F. Supp. 1339, 1361 (D.N.J. 1981) (Elvis impersonator). The benefit found in each of these cases is analogous to that derived from profiling, where the benefit a commercial entity receives is by virtue of the computer profile's ability to simulate or *mimic* a consumer's future behavior.

320. Thus, benefit has been found where a scientist's name was used as an internal code name for a new product in development, Sagan v. Apple Computer, Inc., 874 F. Supp. 1072, 1074 (C.D. Cal. 1994), where defendant used plaintiff's name to provide a father for an illegitimate child on a birth certificate, Vanderbilt v. Mitchell, 67 A. 97, 97, 101 (N.J. 1907), where defendant used a plaintiff's name on a petition without consent, Schwartz v. Edrington, 62 So. 660, 662–63 (La. 1913), and where defendant forged plaintiff's signature on an income-tax return, Schlessman v. Schlessman, 361 N.E.2d 1347, 1348 (Ohio Ct. App. 1975). Statutory privacy actions often limit the parameters of the tort to uses of the plaintiff's identity for commercial benefit. For a review of state statutes, see ELDER, *supra* note 269, at 449–72.

Perhaps because the concept of benefit is so amorphous and because the scope of appropriation is so potentially far reaching under the tort, courts limit the scope of appropriation in several ways. First, appropriation does not include uses of a plaintiff's identity that are of general public interest or that otherwise accrue to society's general benefit.[321] Second, courts have consistently declined to find tort liability where the information does not have a meaning-making or value-creating aspect for the appropriator.[322] Third, when applying the tort to information privacy, courts have required some use or disclosure of the information that infringes the plaintiff's reasonable expectation of privacy.[323] Therefore, when applying the tort to information privacy, an appropriation occurs only where the following three factors are present: (1) the use of the information is outside the scope of a socially beneficial function, such as fraud detection, crime prevention or national security; (2) the personal information is collected, aggregated and processed in such a manner as to create value for the data collector; and (3) where the use of the information is inherently intrusive or is used for purposes that otherwise infringe the consumer's reasonable expectation of privacy.

And indeed, one court recently applied this analysis to the profiling of medical information and found the appropriation tort actionable. The trio of cases in the *Weld v. CVS* action[324] may change the paradigms of tort law relating to information privacy. The *Weld* case arose from CVS Pharmacy's entry into an alliance agreement with several drug company partners, whereby it agreed to sell its customers' private transaction information to these drug companies for marketing purposes.[325] The

321. *See supra* notes 303–05 and accompanying text.

322. *But see* Bartow, *supra* note 128, at 695–96 (suggesting that where data is compiled it can have broad meaning or can serve as the basis for broad meaning-making to the same extent that a celebrity's image has meaning-making power); *cf.* Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995) (holding that the plaintiff failed the test of appropriation because: "[A] single, random cardholder's name has little or no intrinsic value to defendants . . . . Furthermore, defendants' practices do not deprive any of the cardholders of any value their individual names may possess."). Three accordant decisions discuss the sale of a customer's name to a third party for marketing purposes without the customer's consent. *See generally Dwyer*, 652 N.E.2d 1351; Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio Ct. App. 1975); U.S. News & World Report, Inc. v. Avrahami, No. 95-1318, 1996 WL 1065557 (Va. Cir. Ct. June 13, 1996). These cases have generally stood for the principle that the sale of names to a third party in a subscription list is not deemed an appropriation for purposes of the tort.

323. *Dwyer*, 652 N.E.2d at 1355; *Shibley*, 341 N.E.2d at 339–40.

324. *See* Weld I, *supra* note 301; Weld v. CVS Pharmacy Inc., No. CIV. A. 98-0897, 1999 WL 1565175 (Mass. Super. Nov. 19, 1999), *aff'd*, Weld v Glaxo Wellcome, Inc., 746 N.E.2d 522 (Mass. 2001).

325. CVS began the program in 1998, using profiles extracted from its database of transaction information to identify those customers that might be potential targets for marketing offers from its drug company partners. CVS first profiled its customers to determine to whom to send the mailings. It then provided a third party with a disk

consumer outrage over CVS' marketing program eventually caused CVS to abandon this practice, but not before several lawsuits were filed by consumers who received these solicitations. Several plaintiffs accordingly brought suit under, inter alia, Massachusetts's statutory right of privacy,[326] "tortuous misappropriation of private and personal information,"[327] and state unfair trade practices, premised on the defendant's violation of the plaintiffs' privacy rights.[328] The court denied the defendants' motion for summary judgment, and found that the question of whether the systematic searching of a computer database in conjunction with the use of the name and address of the plaintiffs for the defendant's benefit constituted a violation of the plaintiff's statutory right of privacy was a "novel question suitable for initial resolution by a jury."[329] In analyzing the applicability of the common law appropriation tort to the facts of the case, the court looked at whether the use of the information was for socially beneficial purposes or whether such use was merely for defendants' financial gain.[330] Next, the court noted the inherent invasiveness of the profiling of medical records.[331] The court had separately found that the consumer had a reasonable expectation of privacy in his prescription drug information.[332] The court therefore held that the use of plaintiff's pharmaceutical records for the defendant's financial gain fell within the scope of the common law appropriation privacy cause of action.[333]

There is no reason not to apply the same rationale to the profiling of

---

containing a listing of the targeted customers' names, addresses, and dates of birth. The third party then provided the disk to a mail fulfillment house, which sent out mailings to the customers. The mailings reminded the customers to refill their prescription medications, provided information concerning new drugs, or encouraged them to discuss certain conditions with their doctors. Funding for these mailings was provided entirely by the drug manufacturers. CVS' customers were never informed nor did they give consent to the disclosures that occurred under this program. *See* Weld I, *supra* note 301, at *1–2.

326. MASS. GEN. LAWS ch. 214, § 1B (1974).

327. Weld I, *supra* note 301, at *6–8. The court extrapolated the common law appropriation privacy cause of action from the pleadings, regardless of the fact that the appropriation privacy tort does not depend on the confidential nature of the information or on any disclosure. *Id*. Whether the plaintiff actually intended to plead the common law appropriation tort is unclear; the plaintiff did plead the analogous statutory cause of action. *Id*. at *3–5.

328. *Id*. at *6.

329. *Id*. at *5.

330. *Id*. at *6.

331. *Id*.

332. *Id*.

333. *Id*. at *6–7.

financial information, which has been analogized to medical information.[334] First, profiling for marketing purposes cannot be said to have a purpose that is beneficial for any other goal than the financial institution's own profit motive. Second, aggregated financial data is deemed predictive of future behavior and, unlike a simple address list, can be used to manipulate a consumer and create meaning and value for the data collector.[335] Sensitive financial transaction data cannot be described as trivial but rather can include hundreds of thousands of purchases that produce a very invasive picture of the individual consumer. And that picture may be used for such nontrivial uses as predicting that individual's future behavior and thereby shifting the economic balance of power from the consumer. Third, profiling of financial data provides a very granular picture of an individual's personal behavior and beliefs that is inherently intrusive. Furthermore, in the same way as a customer of a pharmacy has a reasonable expectation of privacy in prescription drug information, a customer of a financial institution also has a reasonable expectation of privacy that his or her personal financial profile will not be used for marketing purposes without express or implied consent.

---

334. Rob Blackwell, *Bush Privacy Decision: Financial Data Next?* AM. BANKER, April 18, 2001, at 1 ("Financial privacy is in many ways just as sensitive as medical privacy, in that much of our private personal spending involves health. Your financial records are your family's DNA and should not be reproduced or transmitted to others without your permission.").

335. An approach that distinguishes a simple customer list, phone number or other solitary data point from an aggregated profile of an individual for purposes of liability under the tort is in accord with economic analysis as well. Posner in his law review article containing an economic analysis of the law of privacy, approves withholding any privacy right in a name or address because it follows an efficient economic rationale. Posner, *supra* note 81, at 398–99. In Posner's view, the high transaction costs inherent in obtaining a customer's consent prior to any disclosure of their information to third parties in a mailing list outweigh any possible worth to the individual of being shielded from that disclosure. This is because, in Posner's words, the information about the subscribers that is disclosed is "trivial." *Id.* However, Posner goes on to suggest that the economic analysis of personal information changes when the purchaser of the information can use that information to "impose substantial costs on the subscribers" or otherwise can use the information to gain an economic advantage over the person to whom the information pertains. *Id*. at 399. Thus, under Posner's economic analysis of the tort, because profiling allows a business to use a customer's information to gain a distinct economic advantage, profiling should bring liability under a privacy cause of action. An argument can also be made that a financial institution is the cheaper cost avoider and, just as a consumer goods manufacturer is required to design all reasonable safety features into its products, a data collector should similarly be required to obtain a consumer's express consent prior to using a consumer's data for profiling purposes. The transaction costs of protecting privacy are actually quite low. An opt-in program for data sharing would cost a mere seventeen cents per day per customer if, in a worst-case scenario, less than ten percent of customers agreed to opt-in. Frank Hayes, *Privacy? Bank on It*, COMPUTERWORLD, May 7, 2001, at 78.

C. The Limits of Consent: The Right to Privacy Versus the Privacy Policy

Whether the right of privacy against the profiling of personal financial information arises out of the intrusion branch or the appropriation branch of the privacy tort, it is likely that a colorable claim of invasion of privacy could be made. Indeed, the fact that financial information is accorded a particularly private status is a concept that has long been ingrained in the social consciousness.[336] In recognition of this fact, financial institutions have traditionally published privacy policies that served to articulate and clarify the general parameters of their existing common law duties for the protection of personal financial information.[337] However, gradually the privacy policy has ceased to fill this traditional role and now under the GLBA, operates to contract around a consumer's reasonable expectation of privacy and permits the financial institution to sell a customer's private account information to third parties unless the customer opts out of that disclosure.[338] However, the states are permitted to establish laws that are more protective of privacy than those set forth in the GLBA.[339] And judicial recognition of the common law privacy torts in the context of financial privacy, no less

336. Until recently, the fact that a bank would even consider itself at liberty to use its customer's personal financial information for marketing purposes would have been unthinkable. *See* Peterson v. Idaho First Nat'l Bank, 367 P.2d 284, 290 (Idaho 1961) ("It is inconceivable that a bank would at any time consider itself at liberty to disclose the intimate details of its depositors' accounts. Inviolate secrecy is on of the inherent and fundamental precepts of the relationship of the bank and its customers . . . .").

337. *See* FISCHER, *supra* note 157, at 5-15 (stating that the privacy policy has "the goal of making disclosures of customer information conform to the norm of confidentiality in the industry to which the institution belongs"). This is consistent with the general law applicable to adhesion contracts; that is, they generally are enforceable only to the extent they do not deviate significantly from an implied "set of background rules" grounded in common law and social norms. *See* Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1179, 1181–83 (1983).

338. *See, e.g.*, J.P. MORGAN CHASE & CO., CHASE PRIVACY POLICY 2 (n.d.) ("Chase shares information it has about you . . . to give you superior customer service, provide convenient access to our services and make a wider range of products available to you.").

339. Existing federal legislation is likely not to pre-empt state tort law which would mandate an opt-in standard. The GLBA provides the states with the opportunity to enact laws that are more protective of privacy if these laws are not in conflict with the GLBA. *See supra* note 230 and accompanying text. It is doubtful that an opt-in standard would be in conflict with the GLBA, which sets forth as its controlling purpose the proposition that financial institutions have an "affirmative and continuing obligation to respect the privacy of [their] customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a) (2000).

than action by the legislature, would be one mechanism for the states to establish such privacy protections.[340] If the privacy tort were given such judicial recognition, the question would then arise as to whether the opt-out privacy policies currently in use by financial institutions would operate as a waiver of the consumer's right of privacy.

The ancient legal maxim, *volenti fit injuria* sets forth the fundamental legal principle that there is no wrong done to one who consents.[341] Consent is therefore an affirmative defense to a privacy cause of action.[342] Consent is willingness for conduct to occur.[343] To be deemed effective, consent (1) must be made by one who has the capacity to consent, and (2) is effective only within the scope and within any conditions of the consent.[344] Consent is void where given under a substantial misrepresentation or mistake.[345] Under the stringent informed consent parameters of tort law, it is unlikely that an opt-out process demonstrates sufficient consent to waive a privacy right.[346]

McCarthy views the principle of consent to be synonymous to a license to the privacy right.[347] Under this analysis, recent decisions concerning the enforceability of "click-wrap" licenses are instructive in analyzing the enforceability of privacy polices. In *Specht v. Netscape Communications Corp.*,[348] the District Court for the Southern District of

---

340. As was expressed by Nimmer in his argument for the establishment of the right of publicity:

> This raises the final question of the right of our courts, in the absence of legislation, to enforce a right not previously recognized. Here we may return to the essay by Brandeis and Warren . . . . The argument was there advanced that 'the beautiful capacity for growth which characterizes the common law' would with respect to the right of privacy 'enable the judges to afford the requisite protection, without the interposition of the legislature.' That this proved true is attested by judicial opinions in fifteen jurisdictions.

Nimmer, *supra* note 284, at 223 (quoting Warren & Brandeis, *supra* note 134, at 195).

341. Under the *Restatement (Second) of Torts*: "One who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct or harm resulting from it." RESTATEMENT (SECOND) OF TORTS § 892 A (1977).

342. FED. R. CIV. P. 8(c).

343. RESTATEMENT (SECOND) OF TORTS § 892 (1977). Although consent does not need to be manifested by express words or action, no cases have been reported where consent was not manifested but was still proved. *Id*. cmt. b reporters' notes.

344. *Id.* § 892A. Consent can also generally be revoked at any time. *Id*. There is a strong presumption of revocability where the consent is gratuitous. *See* McAndrews v. Roy, 131 So. 2d 256, 259 (La. Ct. App. 1961); Garden v. Parfumerie Rigaud, Inc., 271 N.Y.S. 187, 188–89 (Sup. Ct. 1933).

345. RESTATEMENT (SECOND) OF TORTS § 892B (1977).

346. *See* Litman, *supra* note 116, at 1310–11 ("The tort law version of consent doesn't depend on formalities like opt-in or opt-out. Rather it requires that the subject appreciate the act that she consents to and be in fact willing that it occur.").

347. *See* MCCARTHY, *supra* note 277 §10:21, at 10-31 to 10-32 ("There is no reason [the rules of consent] could not also be viewed as rules governing a '*license'* of the privacy right . . . .").

348. 150 F. Supp. 2d 585 (S.D.N.Y. 2001).

New York, using California law, reviewed the enforceability of an online license that did not require the licensee to click "I agree" before downloading the licensor's software.[349] The court, comparing the license to a "browse-wrap" license,[350] refused to hold the arbitration clause in the license enforceable. The court reasoned that because the licensee was not made aware that he was entering into a contract and not required to do anything to manifest assent other than take possession of the product,[351] no contract was formed.[352] *Specht* is a significant case, because the court based its holding not on any substantive unconscionability of the arbitration clause, but rather on *procedural* unconscionability, based on the lack of the adherent's actual assent.[353] Although procedural unconscionability has been a largely dormant legal principle in light of the practical necessity for adhesion contracts in mass market transactions, the *Specht* case demonstrates that there are still limits to consent by adhesion.[354] A similar recognition of procedural unconscionability is

349. This license permitted the licensee to download the software absent any requirement to affirmatively to indicate their assent to the license agreement, or even to view the license agreement. If the licensee chose to click on the underlined text in the invitation, a hypertext link took the licensee to a Web page entitled "License & Support Agreements" where the licensee could view the terms of the license. *Id*. at 588. Plaintiffs alleged that their usage of the software improperly permitted the defendant to receive private information about the user's file transfer activity on the Internet. *Id*. at 587.

350. A browse-wrap license refers to where a Web site offers proprietary information, subject to the user's acceptance of an online license agreement. The user is not required to click on an icon expressing assent to the license, or even to view its terms, before proceeding to use the information on the site. *Id*. at 594.

351. *Id*. at 595 ("The only hint that a contract is being formed is one small box of text referring to the license agreement, text that appears below the screen used for downloading and that a user need not even see before obtaining the product . . . .").

352. *Id*. at 596 ("The case law on software licensing has not eroded the importance of assent in contract formation. Mutual assent is the bedrock of any agreement to which the law will give force. Defendants' position, if accepted, would so expand the definition of assent as to render it meaningless.").

353. *Id*. Unconscionability takes both a procedural and substantive form. *See* Arthur Allen Leff, *Unconscionability and the Code—The Emperor's New Clause*, 115 U. PA. L. REV. 485, 487 (1967). Procedural unconscionability relates to the inability of the consumer to negotiate terms of the contract. Substantive unconscionability relates to the imposition of harsh or oppressive terms on the adherent. *See* Ingrid Michelsen Hillinger et al., *Consumer Protection Rules in and Around the Uniform Computer Information Transactions Act (UCITA)*, INTERNET L. & BUS., Nov. 2001, at 11. Because contracts of adhesion are an accepted form of transacting commerce in mass-market consumer transactions, which by definition involve procedural unconscionability, most unconscionability claims in the online environment either must involve the imposition of oppressively harsh terms (a rare instance) or (more typically) must involve a limitation of remedies. *Id*. at 11–13.

354. *See also* Margaret Jane Radin, *Humans, Computers, and Binding Commitment*,

found in the Uniform Computer Information Transactions Act (UCITA), whereby a "procedural breakdown" in an online contract can invalidate a contractual term.[355]

If this analysis is applied to an information transfer under an opt-out privacy policy, a similar conclusion results, even though the licensor of personal information fills the unusual role of the adherent to the purported contract.[356] Under opt-out privacy policies, the adherent is not required to do anything to manifest assent to be bound to the terms of the privacy policy. An opt-out privacy policy written in fine print, containing highly complex terms, received with a monthly billing statement stuffed with advertisements, is perhaps more suspect on procedural grounds than an online license that does not require the adherent to click "I agree" to the license terms. Furthermore, the privacy policies developed by financial institutions in the wake of the GLBA are particularly suspect procedurally, because they often contain unusually broad or rather vague statements of the permissible uses of customer data.[357] And although a consumer ostensibly has the right to opt-out of information sharing, a broad interpretation of the exceptions in the GLBA may encourage a financial institution to utilize these exceptions to substantially eviscerate the consumer's opt-out choice.[358] It is therefore likely that the only contract for the licensing of personal information formed by these opt-out privacy policies is the implied contract defined by the social norms set forth by the financial institution's duty of confidentiality and the customer's reasonable expectation of privacy.[359]

Therefore, in the face of a privacy tort claim, a privacy policy based on an opt-out mechanism would probably be effective to show consent only

---

75 IND. L.J. 1125, 1159 (2000) ("[W]e should notice that it matters to what extent the world of exchange consists of these contracts that are suspect on autonomy grounds. If people right and left are having their entitlements rearranged . . . without their consent, that is a different social world.").

355. UCITA § 111 Official Cmt. 3 (2001), *available at* http://www.law.upenn.edu/bll/ulc/ucita/ucita01.pdf. UCITA is a model statute focusing on electronic commerce. *See id.* at Prefatory Note.

356. Margaret Jane Radin suggests that adhesion contracts for privacy rights may be suspect on *substantive* unconscionability grounds as well. "[P]olicymakers [must] take on the task of deciding which terms it is important to draw buyers' attention to in order to preserve their autonomy, and which kinds of terms must be simply excluded on autonomy grounds. Redress limited to Los Angeles could be in the first category; waiver of all personal privacy rights could be in the second." Radin, *supra* note 354, at 1161 (discussing whether or not the liberal social construct of consent should be retained).

357. *See, e.g.*, BANK OF AM. CORP., PRIVACY POLICY FOR CONSUMERS (2002) ("We collect and use various types of [customer] information to service your accounts, save you time and money, and better respond to your needs.").

358. *See supra* notes 222–26 and accompanying text.

359. The few courts that have construed privacy policies have interpreted them very narrowly. *See, e.g.*, Taylor v. Nationsbank, 776 A.2d 645, 651–53 (Md. 2001).

to the extent it materially aligns with the consumer's reasonable expectation of privacy. As previously demonstrated, most profiling activities are quite likely to fail this test. A financial institution is therefore well-advised to refrain from undertaking profiling activities merely on the basis of an opt-out privacy policy. Rather, it should fully disclose and obtain the consumer's express opt-in consent prior to undertaking any intrusive profiling activities and prior to any sharing of data with third parties for such purposes. Practices that do not conform to this standard may subject a financial institution to liability under common law privacy causes of action. And, the common law privacy tort can also serve as a foundation for a consumer to launch additional statutory claims.

D. Potential Remedies Under the Theory: Utilizing the "Little FTC Acts"

Although the privacy tort may provide a valid cause of action with which to challenge profiling activities by financial services entities, the difficulty of establishing damages significant enough to make the claim worthwhile serves as an impediment to any practical use of the cause of action. In cases involving tortious use of the plaintiff's financial information, the plaintiff's actual damages may be quite small or otherwise difficult to prove or quantify.[360] The only practical method of litigating the claim would be by virtue of a class action. And class actions founded on a privacy tort claim are quite difficult to certify and are subject to numerous other procedural challenges.[361]

For these reasons, a privacy cause of action is perhaps useful only in the respect that it can serve as leverage to support a cause of action under existing consumer fraud and unfair trade practices statutes.[362]

360. Under the appropriation tort, a plaintiff may recover for the loss of the exclusive use of the value so appropriated. One who suffers intrusion on seclusion may recover damages for deprivation of that seclusion. In addition, the plaintiff may recover damages for emotional distress or humiliation that *normally results from such an invasion*. RESTATEMENT (SECOND) OF TORTS § 652H cmt. a (1977) (emphasis added).

361. *See, e.g.*, Shibley v. Time, 341 N.E.2d 337, 340 (Ohio Ct App. 1975) ("Because this right to privacy which is being asserted differs from person to person . . . it cannot be said that appellants' claims are typical of the class as a whole.").

362. Other statutes provide remedies as well. For instance, the appropriation and intrusion privacy torts, if expanded to information privacy issues, could substantially change the analysis of liability for Internet profiling under the Wiretap Act. 18 U.S.C. § 2511 (2000). Recent cases where plaintiffs have sought to obtain relief from corporate profiling practices under this statute have been dismissed for failure to state a claim, inter alia, because the plaintiff was not able to fulfill the requirement of the statute that

Recognizing the effectiveness of the consumer fraud statutes in the protection of information privacy, state attorneys general have recently utilized these laws to attempt to protect financial privacy.[363] These actions evolved from some rather egregious behavior by banks in their use of consumer transaction data—financial institutions quietly began trading their customers' personal financial information to direct marketers (perhaps relying on their privacy policies that purported to permit such unlimited uses). The consumer outrage quickly led the attorneys general of several states to bring investigations of these practices based on state consumer protection laws.[364] These actions have deterred not only the institutions that were subject to the investigations, but have also spurred quite a bit of self-regulation by financial institutions in general,[365] and many institutions have even temporarily halted or reduced many disclosures of financial information to third

---

plaintiff prove that he or she had been harmed by defendant's commission of a tortious act. *Id*. § 2511(2)(d) ("It shall not be unlawful under this chapter . . . unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or law of the United States or of any State."). *See, e.g.*, *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1277–78 (C.D. Cal. 2001) (finding a "bare allegation" not enough to survive motion to dismiss, thus the court concluded not that plaintiffs' claims were false, but simply that they failed to allege a tortious purpose); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 519 (S.D.N.Y. 2001) (dismissing plaintiffs' claims under the Wiretap Act as follows: "In light of the abundant evidence that DoubleClick's motivations have been licit and commercial and the utter lack of evidence that its intent has been *tortious*, we find as a matter of law that *plaintiffs have failed to allege that DoubleClick has acted with a 'tortious' purpose*.") (emphasis added).

363. *See generally* Fickenscher, *supra* note 257.

364. Most notable was the New York Attorney General's consent decree with Chase Manhattan. The attorney general made an inquiry and found that Chase had violated, inter alia, the consumer protection laws of the State of New York. *See In re* Chase Manhattan Bank USA, N.A., (N.Y. Bureau of Consumer Frauds and Prot. Jan 21, 2000) (assurance of discontinuance pursuant to executive law § 63(15)), *reprinted in* SECOND ANNUAL INSTITUTE ON PRIVACY LAW, *supra* note 13, at 247–58. *See generally* Fickenscher, *supra* note 257. Chase Manhattan was reportedly selling account information about its customers to several marketers of nonfinancial products. Chase's privacy policy was central to the attorney general Spitzer's case. Because Chase allegedly did not follow its own privacy policy, the state lawsuit would largely have been based on state laws against deceptive labor practices. After meeting with the attorney general, Chase agreed to limit its information sharing to names, addresses and telephone numbers of customer's approving of such uses. *Id.* U.S. Bancorp was investigated by twenty state attorneys general for similar practices including the sale of consumer credit report information. The bank was sued by the Minnesota Attorney General for allegedly violating the Fair Credit Reporting Act. *Id.* More recently, the Minnesota Attorney General filed suit against Fleet Mortgage Corporation on state consumer fraud and deceptive trade practices laws pursuant to Fleet's use of customer information for a telemarketing campaign. State v. Fleet Mortgage Corp., 158 F. Supp. 2d 962, 964–65 (D. Minn. 2001). Fleet's motion to dismiss was denied on all counts. *Id*. at 968.

365. *See* SCHWARTZ & REIDENBERG, *supra* note 6, at 263–66. But some of the self-regulatory behavior results only in the publication of information without offering any real protections to consumers. *Id*. at 264.

party marketing organizations.[366] Some have thus suggested that the solution for information privacy in general may lie in the effective utilization of unfair competition laws.[367]

However, consumer protection laws do have limitations in their application to information privacy. State consumer protection laws generally require proof of an unfair, unlawful, or deceptive trade practice to be successful.[368] Because state statutes generally are modeled after the Federal Trade Commission Act (FTC Act),[369] a showing of unfairness requires a practice to "cause[ ] or [be] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[370] Because this is a very difficult burden for the plaintiff to meet, most litigated cases are based instead on the "deception" subset.[371] The practical effect of this is that the financial institution's publication of a privacy policy that informs the customer of the uses and disclosures of transaction data and complies with the requirements of the GLBA generally is not deemed deceptive.[372] Any use of deceptive trade

366. Fickenscher, *supra* note 257. However, these salutary effects precede the enactment of the GLBA, which may reverse this trend by legitimizing the transfer of transaction data to affiliates as well as to third parties, subject to financial institutions' compliance with the GLBA's notice requirements. *See supra* notes 227–31 and accompanying text.

367. *See, e.g.*, Sovern, *supra* note 111; *see also* Fickenscher, *supra* note 257 (stating that the New York Attorney General's privacy settlement with Chase Manhattan Corp. could be a "blueprint for addressing the issue of the use of customer data"). Fickenscher suggests that New York's action against Chase would likely have centered on allegations of Chase's deceptive contravention of its own privacy policy. *Id.*

368. *See, e.g.*, CAL. BUS. & PROF. CODE § 17200 (Deering 1992 & Supp 2002). California's Business and Professions Code, regulating unfair business practices, requires the commission of "*any* unlawful, unfair or fraudulent business *act or* practice and unfair, deceptive, untrue or misleading advertising" to be actionable. *Id*. Courts have construed the Act to be based in the right of the public to protection from fraud and deceit. *See* People *ex rel*. Mosk v. Nat'l Research Co. of Cal., 20 Cal. Rptr. 516, 520–21 (Dist. Ct. App. 1962). An unfair business practice is one that "offends an established public policy or when the practice is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." State Farm Fire & Cas. Co. v. Superior Court, 53 Cal. Rptr. 2d 229, 234–35 (Ct. App. 1996) (quoting People v. Casa Blanca Convalescent Homes, Inc., 206 Cal. Rptr. 164, 177 (Ct. App. 1984)).

369. Sovern, *supra* note 111, at 1352.

370. 15 U.S.C. § 45(n) (2000).

371. *See* Sovern, *supra* note 111, at 1352; *see also* Michael M. Greenfield, *Unfairness Under Section 5 of the FTC Act and Its Impact on State Law*, 46 WAYNE L. REV. 1869, 1877 (2000) (discussing cases litigated before the FTC).

372. *See* Cel-Tech Communications, Inc., v. Los Angeles Cellular Tel. Co., 973 P.2d 527, 541 (Cal. 1999) (holding that under the California Business and Professions

practices law would therefore normally require a fact pattern where a financial institution violates it own privacy policy, greatly limiting the scope of use of state consumer protection laws for financial privacy.

The Federal Trade Commission's (FTC) enforcement of federal unfair and deceptive trade practice laws under the FTC Act[373] reflects this same limitation. While banks, savings and loan institutions, and federal credit unions are outside of the Act's purview,[374] the FTC's enforcement of the FTC Act does serve as a guideline to the states' unfair and deceptive trade practices regulation. The FTC has recently taken the approach that the publication of a privacy policy satisfies the institution's obligations to consumers and provides that any use and disclosure of that data in accord with that privacy policy will not be in violation of deceptive trade practices laws.[375] The FTC takes this approach in spite of the fact that the privacy policy effectively operates as a contract of adhesion. Furthermore, privacy policies are subject only to industry self-regulation and are not currently subject to any specific FTC requirements for what minimally constitutes a fair privacy policy.[376] Moreover, because institutions are free to craft the terms of their privacy policies as they see fit, the actions of the state attorneys general for an institution's breach of its own privacy policy under the aegis of unfair trade practices laws may have the practical effect of causing the institution to water down the privacy policies they publish in order to avoid any risk of liability for noncompliance under the FTC Act. Thus, unless the FTC changes its current policy to include a watchdog role for patently unfair privacy policies, the FTC Act is likely to provide protection for information privacy only in very limited situations.[377]

However, if a tort privacy claim is deemed to exist for intrusive profiling activities, the analysis changes radically. As discussed above,

---

Code, courts may not impose their own notions of what is unfair, and legislation may limit the judiciary's power to determine certain conduct as unfair).

373. 15 U.S.C. § 45(a)(2) (2000).

374. *Id.*

375. *See, e.g.*, *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 506 (S.D.N.Y. 2001) (quoting a letter from the Federal Trade Commission to DoubleClick's outside counsel concerning DoubleClick's collection of clickstream data: "Based on this investigation, it appears to staff that DoubleClick never used or disclosed consumers' [personally indentifiable information] for purposes *other than those disclosed in its privacy policy*.") (emphasis added); *see also* Sovern, *supra* note 111, at 1322 (stating that the deceptive trade practices under the FTC Act are invoked only with respect to affirmative misrepresentations made with respect to the collection of information and occasionally when information is collected from children online).

376. The FTC does, however, articulate a suggested formulation for fair information practices, including notice, choice, access, and security. FTC 1998 REPORT, supra note 12.

377. The author favors an FTC definition of "patently unfair" including any privacy policy that either fails to mention the existence of profiling activities or allows any profiling of consumers' data without their prior express written consent.

the current weakness in many consumer protection statutes aimed at information privacy issues is the fact that the publication of a privacy policy often negates the critical element of deception necessary to establish the cause of action. However, if a privacy tort cause of action is recognized, and intrusive profiling is therefore deemed tortious, it would enable the use of the unlawful branch of federal and state consumer protection statutes.[378] In addition, recent FTC statements indicate that a plaintiff showing a "tangible *misappropriation* of personal protected information" could establish a "substantial injury" and thus show a violation of the "unfair" branch of the FTC Act.[379]

A consumer would therefore have ample opportunities for redress under the state consumer protection laws, often called the "Little FTC Acts." First, a state attorney general can bring action on behalf of the state. Next, most states provide a consumer with a private right of action to bring suit. And not only would the plaintiff be availed of tort damages, but the statutes usually provide statutory damages for a consumer who is successful in litigating a claim, including punitive damages, a minimum statutory amount, and often recovery of attorney fees.[380]

VI. CONCLUSION

Consumer profiling is becoming a common practice by banks, brokerages, and insurance companies due to improvements in technology, increasing competitive pressures in the industry, and the changing legislative and regulatory parameters for the financial services sector. Legislative measures to protect consumers' financial privacy, such as the GLBA, have failed to include any protections against consumer profiling, and such protections are unlikely to be introduced by legislation in the near future because of the very powerful industry

378. *See, e.g.*, CAL. BUS. & PROF. CODE § 17200 (Deering 2001) (includes any unlawful act or practice); *see also* State Farm Fire & Cas. Co. v. Superior Court, 53 Cal. Rptr. 2d 229, 234 (Ct. App. 1996) (stating that the Business and Professions Code "borrows" violations of other laws and treats them as unlawful practices); Saunders v. Superior Court, 33 Cal. Rptr. 2d 438, 441 (Ct. App. 1994) (stating that unlawful practices under the Act may be court made).

379. Statement of Commissioner Mozelle W. Thompson, *in* FTC v. ReverseAuction.com, Inc., No. 0023046 (emphasis added), *at* http://www.ftc.gov/os/2000/01/reversemt.htm (last visited May 27, 2002). The case eventually ended in a consent agreement. FTC v. ReverseAuction.com, Inc., No. 00 0032, 2000 U.S. Dist. LEXIS 20761 (D.D.C. Jan. 10, 2000). *See also*, Sovern, *supra* note 111, at 1343–48 (discussing the potential ramifications of the *ReverseAuction.com* case).

380. *See* Sovern, *supra* note 111, at 1350–51.

lobbies that tend to militate against any divestment of the industry's current entitlement to a consumer's transaction data.

The courts' recognition of the applicability of either the common law intrusion on seclusion or the appropriation privacy torts to the practice of consumer profiling would set a tort liability rule in motion that would require a consumer's express opt-in consent before his or her personal financial information was disclosed or otherwise used for profiling purposes outside the scope of the consumer's reasonable expectation of privacy. For any breach of this privacy right, state and federal consumer protection laws could be leveraged to provide a private right of action that would enable consumers to recover statutory minimum damages for any breach of their privacy rights.

America's core values of equality, autonomy, and human dignity may be diminished if the use of profiling technology is embraced by the financial services industry and if society acquiesces to this practice without the concurrent adoption of equivalent legal protections against its abuses. The common law privacy tort provides a flexible and workable mechanism by which individuals might control the use of their personal information profile, without precluding socially beneficial or necessary uses of that information in the process. But unless this right is soon given formal recognition by the courts, information privacy rights in personal financial information remain tenuous at best.

The right is fundamental and rooted in antiquity. The remedy is within reach. The words of Warren and Brandeis are as applicable now as when they were first written: "[T]he protection of society must come mainly through a recognition of the rights of the individual. . . . It is believed that the common law provides . . . [a weapon] forged in the slow fire of the centuries, and to-day fitly tempered to [the] hand."[381]

JANET DEAN GERTZ

381. Warren & Brandeis, *supra* note 134, at 219–20.