It's Personal But Is It Mine? Toward Property Rights in Personal Information

Vera Bergelson[*]

"On the Internet, nobody knows you're a dog."

[*] Assistant Professor, Rutgers School of Law-Newark; J.D., University of Pennsylvania; Ph.D., Institute of Slavic and Balkan Studies at the Academy of Sciences of the Soviet Union. I would like to thank Professors Norman L. Cantor, Howard Latin, John Leubsdorf, James Pope and all participants of Rutgers School of Law-Newark Faculty Colloquium for their insightful comments and suggestions. I am also grateful to my research assistants Dina J. Yin and Eilleen S. Ingram for their capable assistance and The Dean's Research Fund of Rutgers School of Law-Newark for its financial support.

TABLE OF CONTENTS

INTRODUCTION

When in 1993 *The New Yorker* published its now famous cartoon[1] showing a dog surfing the web and telling another dog, "On the Internet, nobody knows you're a dog," we laughed because the "information superhighway" seemed a place where everyone was totally anonymous. Today, looking at that same cartoon, we find amusing the proposition itself and laugh, if at all, at our own past naiveté.

The computer revolution has dramatically affected our privacy by making it possible to record, store, and process every scrap of personal information we leave behind.[2] In the course of our everyday activities,[3] we routinely reveal our names, addresses, and social security numbers as well as our financial decisions, health problems, tastes, habits, political and religious affiliations, sexual orientation, hobbies, and love affairs.[4]

For decades, companies have collected such information and used it internally for marketing or research and development.[5] The growth of computer technology in the 1990s allowed them to distribute the data far and wide[6] and promoted the development of a new phenomenon — a

---

[1] Peter Steiner, Cartoon, *On the Internet, nobody knows you're a dog*, NEW YORKER, July 5, 1993, at 61.

[2] I am using terms "personal information" and "personal data" interchangeably and in the meaning assigned to the term "personal data" in the European Union Data Protection Directive (i.e., "any information relating to an identified or identifiable natural person" where an identifiable person is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."). *See* Council Directive 95/46 of 24 October 1995 Protection of Individuals with Regard to the Processing of Personal Data and on Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive]; *see also* LAURENCE TRIBE, AMERICAN CONSTITUTIONAL LAW §§ 15-17, at 966 (1978) (defining "personal information" as any information which identifies or relates to specific individual).

[3] Joel R. Reidenburg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 205 (1992) ("It is probably not commonly known that credit card companies develop lifestyle profiles of card holders, that telecommunications companies track users' calling patterns, that product manufacturers track the habits of individual customers, and that credit reporting agencies also assemble data on household composition (such as marital status of occupants) and on legal disputes involving individuals.").

[4] *See* Adam L. Penenberg, *The End of Privacy*, FORBES, Nov. 29, 1999, at 1 (describing experiment pursuant to which Penenberg hired web detective and asked him to find as much information as possible about Penenberg using only phone and computer). The results of the experiment were rather shocking. It took the detective only a few days to uncover "the innermost details of my life — whom I call late at night; how much money I have in the bank; my salary and rent." *Id.* The detective also uncovered Penenberg's unlisted phone numbers and a record of monthly payments to his psychotherapist. *Id.*

[5] This Article also refers to such companies as "primary collectors."

[6] *See* Penenberg, *supra* note 4, at 1.

secondary market[7] in which personal information itself became a valuable commodity.[8] Today, billions of dollars are made annually from the sale of mailing lists alone,[9] and the direct-marketing industry continues to grow.[10]

The expansion of the market for personal information resulted in the unprecedented erosion of individual privacy. The value of a personal information database depends to a large degree on how precisely it captures a segment of a community with well defined purchasing susceptibilities. For that reason, lists brokers began to focus on more and more private and sensitive characteristics of people's lives.[11] Such specialized lists may include names of men who called various phone-sex numbers; gay and lesbian magazine subscribers; women who requested free samples of adult diapers; or men who sought medical help for impotency.[12]

---

[7] This Article refers to companies that obtain personal information in the secondary market as "secondary collectors." In addition, this Article sometimes refers to both primary collectors and secondary collectors as "collectors" generally.

[8] *See, e.g.*, Native Forest Network, *Native Forest Network's Guide to Stop Junk Mail, at* http://www.nativeforest.org/stop_junk_mail/nfn_junk_mail_guide.html [hereinafter *Native Forest Guide*] (estimating that value of each name is typically worth 3 to 20 cents each time it is sold); *see also* Walter W. Miller, Jr. & Maureen A. O'Rourke, *Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?*, 38 HOUS. L. REV. 777, 779 (2001) (noting that, in many cases, an e-commerce company's most valuable asset is its customer database).

[9] *See* William J. Fenrich, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 956 (1996) (stating that "[t]he annual market for mailing lists alone, without factoring in sales attributable to their use, has been estimated at approximately $3 billion.").

[10] The direct-marketing industry employs more than eighteen million people and is growing at a rate estimated at twice that of the United States' gross national product; *see* ARTHUR M. HUGHES, THE COMPLETE DATABASE MARKETER 5 (rev. ed. 1996) (discussing expansion of database marketing and direct marketing); Fenrich, *supra* note 9, at 956; Scott Foster, *Online Profiling Is on the Rise: How Long Until the United States and the European Union Lose Patience With Self-Regulation?*, 41 SANTA CLARA L. REV. 255, 260 (2000) (discussing online profiling and impact of self-regulation); *see also* U.S. News & World Report, Inc. v. Avrahami, No. 95-1318, 1996 Va. Cir. LEXIS 518, at *1 (Va. Cir. June 13, 1996) (noting that, in 1995, direct marketing accounted for approximately one trillion dollars of revenues generated for goods and services).

[11] *See* Judith Waldrop, *The Business of Privacy*, AM. DEMOGRAPHICS, Oct. 1994, at 46, 49 (noting that people who meet sensitive and personal criteria have particularly good chance of being on list); *see also* Mary Zahn & Eldon Knoche, *Electronic Footprints: Yours Are a Lot Easier to Track Than You May Think*, MILWAUKEE J. SENTINEL, Jan. 16, 1995, at 1A ("Any lesbian or a diabetic has a good chance of being on a list. A Jew has an excellent chance of making some marketing list.").

[12] *See* Zahn & Knoche, *supra* note 11, at 1A; *see also* Fenrich, *supra* note 9, at 953 n.17 (discussing lists that are routinely sold by list brokers, including names of following people: more than 300,000 men who called various phone fantasy numbers; 55,912 gay and lesbian magazine subscribers; 5,000 women who responded to 800 phone number offering

Over the years, various privacy groups and members of the general public have voiced concerns that people in this country have lost all control over their personal information.[13] Scholars from diverse backgrounds have supported these concerns, pointing out that existing laws are insufficient to protect privacy and fall far behind the developmental trajectory of information technology.[14] Under the current law, individuals neither own their personal information, nor have a recognized privacy interest in it.[15] Thus, on the one hand, they are powerless to prevent its unauthorized dissemination, and on the other, they are excluded from its profitable commercial exchange. In other words, individuals have all the downside and practically no upside of the commodification of personal information.

This Article takes the position that, in order to protect privacy, individuals must secure control over their personal information by becoming its real owners. Similar views have already been expressed in a number of legal and non-legal publications concerning information privacy.[16] While making an important contribution to the privacy debate, the vast majority of those publications have focused primarily on the social utility of granting individuals property rights in personal information. This Article adopts a somewhat different approach.

The first half of this Article reviews the current treatment of personal information by industries (Part I) and law (Part II), and briefly addresses the constitutionality of expanding individual rights in personal

---

information and samples of adult diapers (this list sold for $270); and 82,000 men 55 and older who sought help for impotency at medical clinics).

[13] *See* Kenneth C. Laudon, *Markets and Privacy; Privacy Regulation in National Networks*, COMM. OF THE ACM, Sept. 1996 at 92, 94 (reporting that, according to an Equifax poll, 76% of U.S. citizens believe they have lost all control over personal information); *see also* Penenberg, *supra* note 4, at 1 (discussing how, due to development of computer technology "America, the country that made 'right to privacy' a credo, has lost its privacy to the computer").

[14] *See* Penenburg, *supra* note 4, at 1 (reporting that scholars specializing in history, sociology, business, and political science have all concluded that current privacy laws are insufficient and outdated); *see also* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1462 (2000) (arguing that unprecedented variety of technologies collect personal information in ever-increasing variety of contexts).

[15] *See* discussion *supra* Part II.

[16] *See, e.g.*, Laudon, *supra* note 13, at 92; Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63-65 (2000); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 26-41 (1996); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2383 (1996); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003).

information (Part III). Against this background, I confront two related normative questions that have not yet been specifically addressed in the privacy literature: why the property regime is the most appropriate regime for regulating rights in personal information (Part IV); and why individuals have a stronger moral claim to personal information than collectors (Part V). In my view, exploring these two questions is essential for building a foundation for a comprehensive theory of information privacy.

In the second half of this Article, I seek to translate my normative arguments into legal rules and propose a way to balance the rights of individuals, collectors, and the public at large (Part VI); explore a range of legal and practical implications that the new rules may create (Part VII); and conclude with some suggestions regarding the enforcement of individual rights in personal information (Part VIII). My research focuses only on the relationship between individuals and commercial enterprises, not the government,[17] and only on the kind of identifiable personal information that individuals provide or make visible incidentally to entering into a transaction or utilizing services of these or other enterprises.

I. REALITY CHECK: WHAT HAPPENS TO OUR PERSONAL INFORMATION?

"I bought the Social Security numbers of John Ashcroft, CIA Director George Tenet and Karl Rove for $26 each on the Internet," relates Jamie Court.[18] "Their home addresses and telephone numbers cost a little more. For $295, another Internet service says it will sell me bank account balances."[19]

The development of computer technology and of the Internet raised the collection, processing, and further use of personal information to a new level.[20] It is now both technologically possible and economically

---

[17] In most instances, principles and solutions suggested in this paper apply to public entities as well. A Department of Motor Vehicles, for example, should have no more right to sell personal information supplied by its customers than does a drugstore. However, certain governmental agencies, dealing for instance with law enforcement, may have additional rights and limitations. Those rights and limitations are outside the scope of this Article.

[18] *MarketPlace: Interview with Jamie Court* (Minn. Pub. Radio broadcast, July 16, 2003). Jamie Court is a consumer activist and co-author (with Michael Moore) of CORPORATEERING: HOW CORPORATE POWER STEALS YOUR PERSONAL FREEDOM... AND WHAT YOU CAN DO ABOUT IT (2003).

[19] *Id.*

[20] *See Statements on Introduced Bills and Joint Resolutions*, 146 CONG. REC. S7656-68 (daily ed. July 26, 2000) (statement of Sen. McCain). Senator McCain argued:

viable to capture and store for long periods of time information about minute, transient aspects of peoples' lives — information that before the computer revolution was simply lost or immobilized on "remote mainframes that were difficult to access, even for the techies who put it there."[21] Today, computers hold half a billion bank accounts, half a billion credit card accounts, hundreds of millions of mortgages, retirement funds, and medical claims,[22] as well as information about consumers' purchases, travel, hobbies, sexual orientation, and religious and political affiliations.[23]

This data comes from a variety of sources: online and offline purchase records, supermarket savings cards, white pages, surveys, sweepstakes and contest entries, financial and property records, U.S. Census data, motor vehicle registration information, credit card transactions, phone records, product warranty cards, the sale of magazine and catalog subscriptions, and public records.[24] In addition, Internet retailers ("e-tailers") use more subtle methods of data collection such as offering customers free Internet access and free e-mail.[25] Another widespread form of inconspicuous tracking of personal data is through the use of

---

> The ability of the internet to aid business in the collection, storage, transfer, and analysis of information about a consumer's habits is unprecedented. While this technology can allow business to better target goods and services, it also has increased consumer fears about the collection and use of personally identifiable information.

Id.; *see also* Mary Culnan, *Online Privacy Alliance, Privacy and the Top 100 Sites: A Report to the Federal Trade Commission, available at* http://www.msb.edu/faculty/culnanm/gippshome.html (finding that 98% of major computer websites collect personal information) (June 1999).

[21] Penenberg, *supra* note 4, at 1.

[22] *See id.* (describing variety of personal information that is available on web and predicting that "[a]s e-commerce grows, marketers and busybodies will crack open a cache of new consumer data more revealing than ever before.").

[23] *See* Waldrop, *supra* note 11, at 49 (noting that Standard Rate and Data Service mailing-list catalog that is widely used by direct-marketing industry includes lists reflecting customers' "religion, sexual orientation, medical information and political contributions").

[24] *See EPIC Privacy and Consumer Profiling, at* http://www.epic.org/privacy/survey/ (last updated Sept. 25, 2002) (listing sources of personal information available to collectors); *see also* FEDERAL TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 2 (1999) (discussing different direct methods of data collection); Foster, *supra* note 10, at 259 (discussing ways to collect personal information from Internet users).

[25] *See* Deborah Kong, *GM Offers a "Honey" of a Deal on Net Service*, S.J. MERCURY NEWS, Jan. 14, 2000, at 1C (quoting NetZero's chairman Mark Goldston, who stated that company uses "the free access, the free e-mail, as the honey to attract bees," and pointed out that technology company use it "like a GPS tracking system. The minute you come on, it knows who you are, it knows where you go.").

"cookies"[26] which allow a web site provider to monitor every page on its site that users visit, every online advertisement that they view, and every mouse click that they make.[27] Major advertisement services, such as DoubleClick, Inc., now use cookies to monitor and profile Internet users' activities on any site where the company places its advertisements.[28]

The end result of direct and indirect tracking of consumer behavior, purchases, and exchanges of information in the secondary market, as well as data sharing by affiliates of multi-profile companies,[29] is that collectors now have data on broad segments of the population. At its recent workshop, the Federal Trade Commission (FTC) has reported that some collectors have data on most of the U.S. population.[30] More importantly, collectors are in a position to compile various consumer data from different sources to form comprehensive profiles of

---

[26] A cookie is a set of data that a website server gives to a browser the first time the user visits the site. It is updated with each return visit. The remote server saves the information about the user contained in the cookie. The user's browser does the same and stores the information as a text file in the Netscape or Explorer system folder. *See, e.g., High-Tech Dictionary, available at* http://www.currents.net/resources/dictionary/index.htm (last visited Sept. 13, 2003); *see also EPIC Public Opinion on Privacy, at* http://www.epic.org/privacy/survey/ (last updated Sept. 25, 2002) ("Many Internet users cannot identify the most basic tracking tool on the Internet: the cookie. In an August 2000 study conducted by the Pew Internet and American Life Project, 56% of Internet users could not identify a cookie."); *see also* Steve Lohr, *Internet Companies Set Policies to Help Protect Computer Privacy*, N.Y. TIMES, Nov. 5, 1999, at C1 (reporting that 56% of Internet users could not explain what "cookie" is).

[27] *No Hiding Place*, ECONOMIST, Jan. 23, 2003, *available at* www.economist.com.Cfm?Story_ID1534283 (reporting that almost every website attempts to plant "cookie" on your computer — "[y]our every move on the internet is being recorded by someone, somewhere.").

[28] *See* Robert O'Harrow, Jr., *Honing in on Privacy; As Databases Collect Personal Details Well beyond Credit-Card Numbers, It's Time to Guard Yourself*, WASH. POST, Jan. 2, 2000, at H1 (explaining that cookies provide information about behavior patterns of computer users, often without their knowledge).

[29] *See* Martin Abrams, Executive Director of the Center for Information Policy and Leadership, Hunton & Williams, Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data* (Mar. 13, 2001), *quoted in* Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete, available at* http://www.epic.org/reports/dmfprivacy.html#2 (Mar. 2002) ("The data comes from many, many sources. As we discussed, some of them are public record sources. Some of them are surveys. Some of them are purchase data, but the data comes from many sources, not a single source.").

[30] *Id.* ("Aggregators have data on a broader population. Some aggregators have most of the U.S. population."); *see* Zahn & Knoche, *supra* note 11, at 1A (reporting that company, which deems itself world's leading broker and manager of Jewish lists, claims it "can identify and mail to 85% of the 2.6 million Jewish households in the United States").

individuals, their lifestyles and preferences.[31]

In the personal data market, the whole is greater than the sum of its parts. For example, a partnership between Kmart and Yahoo! allowed the two companies to apply the real-world data that Kmart had collected from eighty-five million households to targeted marketing on the Internet.[32] In addition, the recent merger of DoubleClick, Inc., the largest advertising network on the web, with Abacus Direct Corporation, which runs America's largest database of catalog-buying behavior, made it

---

[31] Profiling companies have well-developed lexicons to classify individuals. Claritas, for instance, divides individuals into fifteen different groups, which are in turn categorized into various subgroups. These include:

- "Elite Suburbs" (Blue Blood Estates, Winner's Circle, Executive Suites, Pools & Patios, Kids & Cul-de-Sacs);
- "Urban Uptown" (Urban Gold Coast, Money & Brains, Young Literati, American Dreams, Bohemian Mix);
- "2nd City Society" (Second City Elite, Upward Bound, Gray Power);
- "Landed Gentry" (Country Squires, God's Country, Big Fish Small Pond, Greenbelt Families);
- "Affluentials" (Young Influentials, New Empty Nests, Boomers & Babies, Suburban Sprawl, Blue-Chip Blues);
- "Inner Suburbs" (Upstarts & Seniors, New Beginnings, Mobility Blues, Gray Collars);
- "Urban Midscale" (Urban Achievers, Big City Blend, Old Yankee Rows, Mid-City Mix, Latino America);
- "2nd City Center" (Middleburg Managers, Boomtown Singles, Starter Families, Sunset City Blues, Towns & Gowns);
- "Exurban Blues" (New Homesteaders, Middle America, Red White and Blues, Military Quarters);
- "Country Families" (Big Sky Families, New Eco-topia, River City USA, Shotguns and Pickups);
- "Urban Cores" (Single City Blues, Hispanic Mix, Inner Cities);
- "2nd City Blues" (Smalltown Downtown, Hometown Retired, Family Scramble, Southside City);
- "Working Towns" (Golden Ponds, Rural Industria, Norma Rae-ville, Mines and Mills).
- "Heartlanders" (Agri-Business, Grain Belt);
- "Rustic Living" (Blue Highways, Rustic Elders, Back Country Folks, Scrub Pine Flats, Hard Scrabble);

See EPIC Privacy and Consumer Profiling, at http://www.epic.org/privacy/survey/ (last updated Sept. 25, 2002).

[32] *See* Kalinda Basho, *The Licensing of Our Personal Information: Is It a Solution to Internet Privacy*, 88 CAL. L. REV. 1507 n.4 (2000) (quoting Ken Magill, *Kmart, Yahoo Deal a Databaser's Dream?*, MARKETING NEWS, Dec. 24, 1999, at 1). Kmart chairman Floyd Hall stated that Kmart has the capability to figure out not only what type of toothpaste a consumer will buy but also what brand, how much, and what items they will be interested in buying in the future. *See id.*

possible to bring together anonymous clickstream data "from the five billion ads DoubleClick serves per week and the two billion personally identifiable consumer catalog transactions recorded by Abacus."[33]

At the time of the merger, DoubleClick's customer database, according to the company's chief privacy officer, included profiles on forty to fifty million Internet users.[34] Today, DoubleClick reportedly maintains cookies on one hundred million Internet users.[35] DoubleClick's announcement that it plans to combine its data with that of Abacus has outraged privacy-rights advocates. This has prompted a series of lawsuits filed in several state and federal courts around the country,[36] and an FTC investigation of the company's practice of profiling web users without adequate disclosure.[37] Although the FTC eventually closed its investigation without action, a coalition of ten states pursued DoubleClick's practices and forced the company to accept a binding agreement regarding privacy policies and disclosure, and required the company to pay a fine of $450,000 to reimburse the states' investigative costs.[38]

---

[33] Courtney Macavinta, *DoubleClick, Abacus Merge in $1.7 Billion Deal* (Nov. 24, 1999), *at* http://www.cnet.com/news/0-1005-200-1463444.html?tag+st.ne.1002 (pointing out potential effects of DoubleClick's merger on privacy groups and Internet marketing industry).

[34] John T. Acquino, *Senate Online Profiling Hearing Suggests Movement Toward Federal Legislation, E-Com. L. Wkly.* (June 15, 2000), *available at* http://www.law.com/servlet/ContentServer?pagename=OpenMarket/Xcelerate/View&c=LawArticle&cid=1015973967146&live=true&cst=1&pc=0&pa=0 (citing testimony of DoubleClick's chief privacy officer Jules Polonetsky to U.S. Senate Committee on Commerce, Science, and Transportation).

[35] *No Hiding Place*, *supra* note 27, at 8 (discussing immense capacity of DoubleClick's database).

[36] Courtenay Youngblood, *Case Notes and Comments: A New Millennium Dilemma: Cookie Technology, Consumers, and the Future of the Internet*, 11 J. ART & ENT. LAW 45, 53-54 (2001) (exploring DoubleClick's lawsuit, which focused on need for enhanced consumer privacy protection on Internet).

[37] *See* Acquino, *supra* note 34 (discussing FTC investigation of DoubleClick and testimonies of advertisement companies to U.S. Senate Committee on Commerce, Science, and Transportation concerning use of personal information in online profiling).

[38] *See In the Matter of DoubleClick: Agreement between the Attorneys General of the States of Arizona, California, Connecticut, Massachusetts, Michigan, New Jersey, New Mexico, New York, Vermont, and Washington and DoubleClick* (Aug. 26, 2002), *available at* http://www.oag.state.ny.us/press/2002/aug/aug26a<uscore>02<uscore>attach.pdf; Press Release, N.Y. *State Att'y Gen., Major Online Advertiser Agrees to Privacy Standards for Online Tracking* (Aug. 26, 2002), *available at* http://www.oag.state.ny.us/press/2002/aug/aug26a<uscore>02.html; *see also* Andrea Petersen, *DoubleClick Reverses Course After Privacy Outcry*, WALL ST. J., Mar. 3, 2000, at B1 (reporting that DoubleClick decided to suspend its plan of combining databases with Abacus until government and industry develop guidelines on what practices are appropriate for collection of personal information through Internet).

A recent wave of bankruptcy filings and business liquidations by numerous dot-coms[39] raised another question: may a bankruptcy trustee sell consumer data in an effort to maximize the size of the estate available for unsecured creditors even if such sale would violate the insolvent company's privacy policy?[40] "That question exploded into the collective consciousness when Toysmart.com, an e-tailer of educational toys, sought to sell its customer list in bankruptcy despite its promise never to share such data."[41]

At the time of its bankruptcy in June, 2000, Toysmart's customer database contained information on approximately 250,000 individuals,[42] including "name, address, billing information, shopping preferences, order history, gift registry selections, [and] family profile information about consumers' children, such as name, gender, birthday, and toy interests."[43] Toysmart sought to sell the database as part of its bankruptcy estate.[44] It even ran an ad in the *Wall Street Journal* that read, "We will sell you our data. We will sell you the names and addresses and family profiles of everyone who is registered with our site."[45] There would have been nothing unusual in such a sale but for Toysmart's explicit promise to its customers never to share their personal information with a third party.[46]

---

[39] *See* Luis Salazar, *FTC Takes Action*, NAT'L L.J., Oct. 9, 2000, at B6 (citing expectations for "deluge of Internet bankruptcies" and estimating that as many as 75% of e-tailers will fail); *see also* Victoria Slind-Flor, *Privacy or Creditors: Who Holds the Trump?*, NAT'L L.J., Sept. 4, 2000, at A1 (listing dot-coms going out of business).

[40] *See* Miller & O'Rourke, *supra* note 8, at 792 (using Toysmart's bankruptcy as example of recent bankruptcy filings).

[41] *Id.* at 780.

[42] Matt Richtel, *Toysmart.com in Settlement with F.T.C.*, N.Y. TIMES, July 22, 2000, at C1, C14 (discussing large size of Toysmart's consumer database).

[43] *In re* Toysmart.com, L.L.C., No. 00-13995-CJK, *Stipulation and Order Establishing Conditions on Sale of Customer Information* (D. Mass. July 21, 2000) [hereinafter *Stipulation and Order*], *available at* http://www.ftc.gov/os/2000/07/toysmartbankruptcy.1.htm (last visited Mar. 1, 2003).

[44] *See Toysmart.com's Plan to Sell Consumer Data is Challenged by FTC*, WALL ST. J., July 11, 2000, at C8, *available at* 2000 WL-WSJ 3035966 (discussing Toysmart.com's plan to violate its privacy agreement with its consumers).

[45] *See* Glenn R. Simpson, *FTC Is Set to Challenge Toysmart.com to Prevent the Sale of Consumer Data*, WALL ST. J., July 10, 2000, at A3 (reporting on Toysmart's attempt to sell its customer database); *see also* Gary M. Schober et al., *Colloquium on Privacy & Security*, 50 BUFF. L. REV. 703, 717 (2002) (quoting text of ad but incorrectly attributing it to *New York Times*).

[46] First Amended Complaint for Permanent Injunction and Other Equitable Relief ¶ 8, F.T.C. v. Toysmart.com, L.L.C., Civ. Action No. 00-11341-RGS, (D. Mass. July 21, 2000), *available at* http://www.ftc.gov/us/ 2000/07/toysmartcomplaint.htm (last visited Mar. 1, 2003). Toysmart provided that:

The FTC filed a complaint, arguing that such a sale would constitute a deceptive practice prohibited by Section 5(a) of the Federal Trade Commission Act.[47] In addition, the attorneys general of a number of states intervened in bankruptcy proceedings under their respective consumer protection acts.[48] Over vigorous objections of thirty-eight attorneys general,[49] the FTC and Toysmart reached a settlement that permitted the company to sell its customer database.[50] The case was finally resolved when one of Toysmart's investors agreed to purchase and destroy the list.[51] The questions the case raised, however, remain far from resolution.

The Toysmart bankruptcy, just like the DoubleClick-Abacus merger, attracted significant public attention and once again raised the problem of the inadequacy of current privacy laws and the need for comprehensive federal legislation protecting personal information. [52]

> Personal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party. All information obtained by Toysmart.com is used only to personalize your experience online. . . . When you register with Toysmart.com, you can rest assured that your information will never be shared with a third party.

Id.

[47] 15 U.S.C. § 45(a)(1) (2000) (proscribing unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce).

[48] *See* Miller & O'Rourke, *supra* note 8, at 792 (providing details of Toysmart's bankruptcy); *see also Toysmart.com's Plan to Sell Consumer Data is Challenged by FTC*, *supra* note 44 (reporting that FTC objected to sale of customer information in light of explicit promise to maintain customer privacy); Stephanie Stoughton, *States Weigh in on Toysmart Privacy Case, 38 Attorneys General Join Opposition to Sale of Data*, BOSTON GLOBE, July 26, 2000, at C1, *available at* 2000 WL 3336111 (reporting involvement of attorneys general of many states into Toysmart's bankruptcy litigation).

[49] *See* Stoughton, *supra* note 48, at C1 (pointing out that thirty-eight state attorneys general opposed FTC's settlement with Toysmart.com and permitting sale of its customer list).

[50] *See Stipulation and Order*, *supra* note 43 (authorizing sale of customer database as part of company's goodwill but only to "an entity that (1) concentrates its business in the family commerce market, involving the areas of education, toys, learning, home and/or instruction, including commerce, content, product and services, and (2) expressly agrees to be Toysmart's successor-in-interest as to the Customer Information, and expressly agrees to [certain other] obligations.").

[51] *See, e.g.*, Paul Davidson, *Hot Commodity: Dot-Com Lists: Creditors' Asset of Choice*, NAT'L POST, Mar. 5, 2001, at E02, *available at* 2001 WL 14437954 (reporting that Walt Disney agreed to pay Toysmart $50,000 to destroy its customer list); *see also Toysmart Database to Be Destroyed*, N.Y. TIMES, Jan. 10, 2001, at C7 (reporting that decision to destroy Toysmart's customer list effectively concluded FTC's suit against Toysmart).

[52] Diane Anderson, *Wisconsin Woman Auctions Personal Info Online*, June 16, 2000, *available at* http://www.cnn.com/2000/TECH/computing/06/16/wisconsin.info.for.sale.

Before turning to the question of how the law should change, it is important to map out the boundaries of already existing privacy law.

II. CURRENT STATE OF AMERICAN LAW WITH RESPECT TO PERSONAL INFORMATION

Currently, American law covering personal information is "a patchwork of uneven, inconsistent, and often irrational" federal and state rules.[53] Most of them protect individuals from dissemination of their personal information by governmental entities.[54] The few federal regulations that apply to the transfer of personal information in the private market cover certain areas of banking and financial services,[55]

---

idg/index.html (noting that DoubleClick-Abacus merger made number of web surfers realize that, as they surf, they leave behind wealth of information).

[53] FRED H. CATE, PRIVACY IN THE INFORMATION AGE 80 (1997).

[54] *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552(a) (2000) (permitting individual to determine which personal records are collected, maintained, or disseminated by federal agencies); Right to Financial Privacy Act, 12 U.S.C. § 3401 (2000) (providing procedural requirements for sharing financial information among federal agencies); Privacy Protection Act of 1980, 42 U.S.C. § 2000(aa) (2000) (protecting work products of individuals against searches and seizures by law enforcement officers); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2000) (limiting circumstances under which drivers' personal information may be disclosed); Family Educational Rights and Privacy Act 20 U.S.C.S. § 1232(h) (Law. Co-op. 2002) (prohibiting collection of students' personal information by Department of Education to be disclosed for purposes of marketing or selling); Department of Transportation and Related Agencies Appropriations Act 2002 § 311(a), 115 Stat. 833 (2001) (requiring that "no recipient of funds made available in this Act shall disseminate personal information obtained by a State department of motor vehicles in connection with a motor vehicle record"); CAL. VEH. CODE § 1808.45 (Deering 2001) (stating that right to privacy protects personal information given by individuals to Department of Motor Vehicles); GA. CODE ANN. § 40-3-23(d.1)(1) (2002) ("Personal information of any registrant, including name, address, date of birth, or driver's license or social security number, shall not be furnished or transferred by or to any person"); MASS. GEN. LAWS. ANN. ch. 66A, § 2(c) (2002) (forbidding "any other agency or individual not employed by the holder [from having] access to personal data" unless it is for purposes of medical treatment, application to professional licenses, special investigation bureau, or for detection of fraud and control); MO. REV. STAT. § 32.091(2) (2001) (prohibiting Department of Revenue from disclosing personal information collected "without expressed consent given by the person to whom such information pertains"); MONT. CODE ANN. § 61-3-101(8) (2002) (prohibiting Montana Department of Motor Vehicles from furnishing personal information for public inspection); S.C. CODE ANN. § 30-15-60 (Law. Co-op. 1976) (codified as amended at 2001 S.C. S.B. 1087 (2002)) (amending South Carolina law to prohibit dissemination of veterans' discharge records for commercial uses); Information Practices Act of 1977, CAL. CIV. CODE § 1798 (Deering 2001) (prohibiting "disclosure of personal information, such as employment history information, by any state agency except under certain circumstances, including situation where disclosure of information is relevant and necessary.").

[55] *See, e.g.*, Fair Credit Reporting Act of 1970, 15 U.S.C.S. § 1681 (2002) [hereinafter Gramm-Leach-Bliley Act] (recognizing individual's right to privacy with regard to disclosure of personal credit records); Right to Financial Privacy Act of 1976, 12 U.S.C.A. §

entertainment, cable and telecommunications,[56] education,[57] and postal services.[58] Adopted in response to specific violations or concerns relating to a particular industry, these regulations are not based on any uniform theory of rights and differ significantly in the scope of protection offered to individuals. Scholars and privacy advocates have criticized most of these regulations as inadequate, largely attributing their weakness to the lobbying efforts of the interested industries.[59] In addition to the federal laws, many states have enacted industry-specific legislation.[60] Like their federal counterparts, state laws generally seek to resolve a specific set of problems within a given industry and fail to provide coherent and

---

3401 (2002) (recognizing individual's right to privacy with regard to disclosure of financial records by banks to governmental agencies); Financial Modernization Services Act, 15 U.S.C.S. §§ 6701, 6801, 6901 (2003) (requiring that financial institutions allow customers to "opt out," i.e., object to disclosure of their personal information).

[56] *See, e.g.*, Children's Online Privacy Protection Act of 1999, 15 U.S.C.S. § 6501 (2003) (prohibiting Internet service providers from collecting personal information from children under the age of thirteen); Telecommunications Act of 1996, 47 U.S.C.S. § 251 (2003) (offering limited protection to customers' proprietary information); Video Privacy Protection Act, 18 U.S.C.S. § 2701 (2003) (recognizing privacy of video rental customer as to specific movies bought or rented); Telephone Consumer Protection Act of 1991, 47 U.S.C.S. § 227 (2003) (protecting individuals' privacy against unwanted phone solicitation); Cable Communications Policy Act of 1984, 47 U.S.C.S. § 521 (2003) (recognizing cable television's subscriber's privacy as to viewing habits); Electronic Communication Privacy Act of 1986, 18 U.S.C. § 2701 (protecting individuals against interception and disclosure of wire, oral, or electronic communications).

[57] *See, e.g.*, Family Educational Rights and Privacy Act of 1974, 20 U.S.C.A. § 1232(g) (2002) (recognizing students' privacy rights with respect to access and disclosure of student records).

[58] *See, e.g.*, 39 C.F.R. § 268.2 (2003) (stating that any postal employee who violates Private Information Act and disburses individual's personal information shall be fined at minimum of $1,000).

[59] *See* Fenrich, *supra* note 9, at 966-67 (discussing that lobbying efforts of Direct Marketing Association with respect to Video Privacy Protection Act resulted in weaker privacy protection: the bill, as adopted, disallows only unauthorized disclosure of specific titles of movies rented by customer; other personal information, including video preferences categorized by subject matter, may be transferred without customers' consent as long as they had opportunity to opt out); *see also MarketPlace: Interview with Jamie Court*, *supra* note 18 ("Corporations have so freely traded in the individual's private information that almost everyone's privacy is at risk, so much so that nine out of ten people think that corporations should obtain consent before selling an individual's private information, but year after year, this simple proposition has been defeated in statehouse after statehouse by America's biggest banks and insurers.").

[60] *See* PRIVACY LAWS BY STATE, *available at* http://www.epic.org/privacy/consumer/states.html (last visited Mar. 1, 2003) (providing detailed information about privacy-related topics covered by each state law); *see also* J. THOMAS MCCARTHY, THE RIGHT OF PUBLICITY AND PRIVACY §§ 6.5-6.127 (2d ed. 2000) (reviewing state statutes protecting various forms of privacy).

systematic protection of personal information.[61]

Practically all federal and state laws that address the issue of individual consent to collection and use of personal information apply the "opt-out" rule, which requires companies to give individuals an opportunity to opt out of the company's standard practices.[62] Very few laws are based on the more protective "opt-in" model, which obligates companies to obtain express customer consent before they can share or sell customer information.[63]

The choice of the privacy-protection regime is critical because of consumers' tendency to stay with the default option.[64] Moreover,

---

[61] *See* Reidenberg, *supra* note 3, at 222-23 (criticizing state industry-specific regulations for their limited and *ad hoc* nature, including failure to address systematic protection of privacy concerns relating to acquisition, storage, transmission, use, and disclosure of personal information).

[62] *See, e.g.*, Angela R. Karras, *The Constitutionality of the Driver's Privacy Protection Act: A Fork in the Information Access Road*, 52 FED. COMM. L.J. 125, 133 (1999) (providing list of following states that gave drivers or vehicle owners opt-out option to choose level of confidentiality for personal information open to public: Alaska, Arizona, Colorado, Florida, Idaho, Indiana, Iowa, Kansas, Maryland, Michigan, Minnesota, Mississippi, Missouri, Montana, Nevada, New Hampshire, New Mexico, North Dakota, Ohio, Oregon, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, West Virginia, Wisconsin, and Wyoming).

[63] Laws requiring "opt-in" consent include the Cable Communications Policy Act of 1984 and the Video Privacy Protection Act. *See* discussion *supra* note 56; *see also* Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U.S.F. L. REV. 633, 665 (2000) (noting opt-in provisions of Video Privacy Protection Act); *Colloquium on Privacy & Security*, *supra* note 45, at 729 (commenting that "in the United States you, in fact, have more right to privacy in your video rental records than you do in the amount of money you have in your financial accounts. You have more privacy in the fact that you rent Bambi than your medical records.").

An important recent development is a rule adopted by the FCC designed to protect sensitive personal information of customers of telecommunications carriers. The FCC Order provides for express customer approval for carriers' release of customer information to third parties, but permits opt-out consent for release of information to affiliated parties. *See* Third Report and Order and Third Further Notice of Proposed Rulemaking, July 16, 2002, *at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-214A1.pdf. Following the FCC Order, Washington State adopted "the nation's strongest rules protecting telephone customer privacy." *See Washington Regulators Adopt Nation's Strongest Telephone Customer-Privacy Rules*, *at* http://www.wutc.wa.gov/webdocs.nsf/6f0baa33f074e151882566c20000604d/93d4130392518ad988256c6a0060f5a5 (Nov. 7, 2002). The Washington rules mandate express approval for all "call detail" information, and permit information sharing only within companies under common ownership. *Id.*

[64] *See* Kent Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL'Y 87, 116 (2001). If a merchant chooses an "opt-out" regime in which the permission box is pre-checked and consumers need to uncheck it to withhold permission, a large majority of consumers will leave it checked. If the site chooses an "opt-in" regime, in which the permission box is unchecked and consumers need to check it to give permission, a large majority of consumers will leave it unchecked.

companies have little incentive to facilitate the opt-out process. Privacy advocates often describe opt-out notices as "deceptive" and buried in "legalese."[65] Since the laws do not provide any guidelines or standards for the opt-out mechanics, "each process is likely to include unique hurdles, requiring consumers to muddle through a different opt-out process for each firm."[66] Opt-out procedures are often cumbersome. For example, many companies require their customers to first request an opt-out form, wait for its arrival by mail, and then mail it back.[67]

As for the common law treatment of personal information, there have been only a few decisions, which were rather fact-specific and based on a mix of legal theories. In all of those, the courts refused to recognize the plaintiffs' claims since they did not fit under the existing categories of protected interests. Some courts have also pointed out that the appropriate remedy would be creation of a statutory right.[68]

The existing piecemeal approach brings into focus the need for comprehensive, (not industry-specific) legislation regulating the respective rights of individuals and commercial enterprises that collect personal information.[69] This need has become even more urgent now due to the development of privacy laws in the international arena. In

---

[65] Eric Roston, *How to Opt Out of Database Sharing: Who's Got your Number?*, TIME, July 2, 2001, at 46.

[66] Jolina C. Cuaresma, *Business Law: The Gramm-Leach-Bliley Act*, 17 BERKELEY TECH. L.J. 497, 513 (2002) (criticizing personal data protection provisions of Gramm-Leach-Bliley Act).

[67] *See* Kathy Kristof, *Choice Words for Opting Out; Consumers Run into Trouble With Privacy Forms*, CHI. TRIB., Aug. 7, 2001, at 7N (describing opt-out procedures); *see also* Robert MacMillan, *Few Net Banks Offer Clear Privacy Protections*, NEWSBYTES, Aug. 29, 2001, LEXIS, General News & Information, NYSBYT (stating that Center for Democracy and Technology has reported that less than one-third of banks offer online opt-out option and some firms require customers to first call to request opt-out form that would be sent via U.S. mail). Some 86% of Internet users favor an "opt-in" privacy policy and say that Internet companies should ask people for permission to use their personal information. *See* Trust and Privacy Online: Why Americans Want to Rewrite the Rules, *available at* http://www.pewinternet.org/reports/reports.asp?Report=19&Section=ReportLevel2&Field=Level2ID&ID=37 (Aug. 20, 2000).

[68] *See* Shibley v. Time, 341 N.E.2d 337, 340 (Ohio Ct. App. 1975) (rejecting subscriber's claim for unauthorized sale of subscriber lists in absence of specific right recognized by common law and pointing out that "this is the case peculiarly within the province of a legislative branch").

[69] Acquino, *supra* note 37 (quoting Sen. John McCain, Chairman of U.S. Senate Committee on Commerce, Science and Transportation, saying that "[a]bsent legislation, meaningful enforcement, and airtight coverage, online profiling will eviscerate personal privacy."); *see also* Joel R. Reidenberg, *supra* note 16, at 898 (observing that "[a]t present, without clear statutory rights, there is an important lack of legal accountability or liability for the unfair treatment of personal information by the private sector.").

October 1998, the European Union's Directive on Data Protection took effect.[70] It permits transfers of personal information only to those countries outside the European Union ("EU") that provide an "adequate" level of privacy protection.[71] Unsurprisingly, the United States was not viewed as such a country.[72]

The ban on transfers of personal information to the United States jeopardized not only cross-border transactions between American and EU companies, but also everyday operations of multinational corporations with offices on both sides of the Atlantic. Negotiations between the United States and the EU lasted for two years and resulted in an agreement known as "Safe Harbor Privacy Principles," which became effective in October 2000.[73] The agreement allows American companies to receive data from their EU counterparties, provided that they either adhere to a set of privacy-protection principles embodied in the Safe Harbor Privacy Principles and publicly declare that they do so, or develop another self-regulatory privacy-protection program that is in accord with the Safe Harbor Privacy Principles.[74]

---

[70] *See* Press Release, European Union, EU Directive on Personal Data Protection Enters Into Effect, *at* http://www.eurunion.org/news/press/1998-4/pr89-98.htm (Oct. 23, 1998).

[71] *Id.*

[72] *See* Data Protection Working Party, Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government 2 (Jan. 26, 1999), *available at* http://europa.eu.int/comm/internal_market/privacy/index_en.htm (opining that "the current patchwork of narrowly-focused sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union.").

[73] Issuance of Principles and Transmission to European Commission: Procedures and Start Date for Safe Harbor List, 65 Fed. Reg. 56,534 (Sept. 19, 2000); *see* U.S. Dep't of Commerce, *Commission Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions*, Annex I, *at* http://www.europa.eu.int/comm/internal_market/en/dataprot/news/shprinciples.pdf (last visited Mar. 1, 2003).

[74] The Safe Harbor Principles require companies to give notice to individuals before any identifiable personal information is transferred to a third party. Individuals should have an opportunity to object to any transfers of their personal information. If this information is of a particularly sensitive nature (specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or the sex life of the individual), an affirmative consent of the individual is required. Third parties acting as agents must assure at least the same level of privacy protection as the transferring company itself. In addition, companies must protect personal information from misuse and process it only for the purposes for which it has been collected or authorized by the individual. Finally, the individual should have access to his personal information and the right to correct or delete inaccurate information. *See* U.S. Dep't of Commerce, Safe Harbor Overview, *at* http://www.export.gov/safeharbor/sh_sh_documents.html (last visited Sept. 30, 2003) (establishing guidelines for U.S.

The Safe Harbor Privacy Principles are an important step in establishing a data protection regime in this country. At the same time, they are just an emergency measure designed to deal with the ultimatum issued by the EU to the United States — either to satisfy the EU privacy requirements or face grave economic consequences. As a permanent solution, the "Safe Harbor" approach is much more problematic. It requires U.S. companies to establish an internal legal regime that is at odds with the current national law and market practice.[75] The exact costs of establishing such a regime are unclear but the strong objections to international privacy standards from parts of the business community suggest that they are high.[76]

In addition, the "Safe Harbor" approach creates an incentive for U.S. participants to maintain two privacy standards — the higher one for European consumers and the lower one for domestic consumers.[77] Moreover, domestic consumers are likely to carry, at least partially, the costs involved in satisfying the higher "Safe Harbor" requirements from which they themselves will not be able to benefit. All these monetary and moral costs could have been avoided had the United States itself enacted adequate data privacy-protection laws.[78]

III. CAN AMERICAN LAW PROTECT PERSONAL INFORMATION PRIVACY WITHOUT VIOLATING THE CONSTITUTION?

Most scholars agree that individuals' loss of control over personal information may lead to undesirable societal consequences.[79] What they disagree on is how to balance two conflicting societal interests — in privacy and in the free flow of information.[80] The main principled objection to expanding data privacy laws comes from defenders of free speech who argue that granting individuals control over personal

---

companies that process personally identifying information relating to EU citizens).

[75] Gellman, *supra* note 29 (pointing out that costs incurred by Safe Harbor participants would have been avoided had United States enacted laws that meet international privacy standards).

[76] *Id.*

[77] *Id.* (explaining that Safe Harbor solution creates "the possibility of maintaining different privacy regimes for different customers as well as the unattractive possibility of having lower privacy standards for American customers").

[78] *Id.* (arguing that "U.S. privacy laws could have avoided some costs for American multinational companies while providing improved privacy protections for Americans").

[79] *But see* DAVID BRIN, THE TRANSPARENT SOCIETY (1998) (expressing view that privacy is no longer option because government and corporations will always have privacy-invasive technologies and arguing in favor of "transparent" society).

[80] *See* discussion *infra* notes 234-40 and accompanying text.

information would be unconstitutional.[81]

These authors maintain that any transfer of information is speech. Thus, "the right to information privacy — my right to control your communication of personally identifiable information about me — is a right to have the government stop you from speaking about me."[82] This argument raises a fundamental question: even assuming there is a need to protect personal information, *can* American law afford to do so without violating the Constitution? In confronting this issue, it is important to keep in mind that we are talking not about any speech (newspaper publications, gossip, political debate) but only about identifiable personal data supplied by an individual incidentally to a business transaction.

The freedom of speech guaranteed to American citizens by the First Amendment is one of the main characteristics of a democratic society. Yet "from obscenity to intellectual property, from defamation to insider trading, from the Fair Credit Reporting Act to the FDA's mandatory labeling requirements," there are many different regulations that restrict speech and information.[83] One may add to this list the obligation of confidentiality that the law imposes on lawyers, doctors, and certain other professionals.

There may be several ways to justify restrictions on transfers of personal data in light of the requirements of the First Amendment jurisprudence. The most developed argument is that such transfers amount only to "commercial speech" and thus, should enjoy limited constitutional protection. A number of advocates on both sides of the debate have classified the collection and exchange of personally identifiable information as commercial speech.[84] The few courts that have addressed the issue tend to agree with this classification.[85] In *U.S.*

---

[81] *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1122 (2000) [hereinafter Volokh, *Freedom of Speech and Information Privacy*] (arguing that "restrictions on speech that reveals personal information are constitutional under current doctrine only if they are imposed by contract, express or implied"); *see also* Eugene Volokh, *Freedom of Speech and the Constitutional Tension Method*, 3 U. CHI. L. SCH. ROUNDTABLE 223 (1996) (criticizing argument that Constitution's free speech guarantee must sometimes yield to other constitutionally-protected values).

[82] Volokh, *Freedom of Speech and Information Privacy*, *supra* note 81, at 1050-51.

[83] Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97, 132 (2000).

[84] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1409-10 (2000) (discussing theories of commercial speech and justifications for data privacy protection).

[85] *See* U.S. West, Inc. v. FCC, 182 F.3d 1224, 1232-33 (10th Cir. 1999); United Reporting

West v. FCC, the Tenth Circuit stated: "[W]hen the sole purpose of... speech... is to facilitate the marketing of telecommunications services to individual customers, we find the speech integral to and inseparable from the ultimate commercial solicitation. Therefore, the speech is properly categorized as commercial speech."[86] Practically all transfers of personal data to the secondary market are done for the purpose of facilitating future marketing of services to the customers who are the subjects of that personal data. Thus, there is a strong argument in favor of viewing these communications as commercial speech.

Regulation of commercial speech must satisfy the constitutional test articulated in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*.[87] Under that test, if the law targets a communication that is not misleading or related to an unlawful activity, the regulation, in order to pass constitutional muster, must: (i) be supported by a substantial governmental interest, (ii) materially advance that interest, and (iii) be no more restrictive than necessary to serve that interest.[88] A similar standard applies to content-neutral laws that burden speech only indirectly.[89] In other instances, the governmental interest must be compelling and the regulation must be narrowly tailored to promote that interest in the least restrictive way.[90]

A democratic society does have a strong interest in protecting privacy in personal information.[91] If people know that they are being watched

---

Publ'g Corp. v. Cal. Highway Patrol, 146 F.3d 1133, 1136-37 (9th Cir. 1998), *rev'd sub nom.* Los Angeles Police Dep't v. United Reporting Publ'g Corp., 528 U.S. 32 (1999).

[86] *See U.S. West*, 182 F.3d at 1233.

[87] 447 U.S. 557 (1980).

[88] *See id.* at 564.

[89] *See* United States v. O'Brien, 391 U.S. 367, 376-77 (1968) (holding that incidental limitations of freedom of speech are permissible if essential to furtherance of substantial governmental interest unrelated to suppression of speech).

[90] *See* Burson v. Freeman, 504 U.S. 191, 198 (1992) (plurality opinion); Boos v. Barry, 485 U.S. 312, 321 (1988); Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45 (1983).

[91] *See* Laudon, *supra* note 13, at 92 (observing that protection of privacy is widely accepted value in democratic societies "without which the concept of democracy based on individual choice makes little sense"). That was also Alexander Solzhenitsyn's concern when he wrote more than three decades ago:

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions.... There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands, buses, trams and even people would lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city.

and their activities are recorded forever, they tend to conform their behavior to the requirements of the observing authority, and that conformism may seriously imperil the diversity and freedom of society.[92] Therefore, the government has at least a substantial interest in protecting individual privacy, and a regulation that materially advances this interest, without being more restrictive than necessary, would satisfy constitutional requirements for a restriction on commercial speech.

Some scholars have argued that the state's interest in protecting the privacy of its citizens is not merely substantial but compelling because the right to privacy is an important constitutional right,[93] and protection of a constitutional right is a compelling interest.[94] If that argument

---

ALEXANDER SOLZHENITSYN, CANCER WARD 192 (1969).

[92] *See, e.g.*, PAUL M. SCWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 39-42 (1996) (arguing that free society depends on individual self-determination, autonomy, and dignity which may be guaranteed only if individuals have control over personal information). *See also* Edward Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1003 (1964) ("The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity."); Thomas Huff, *Thinking Clearly About Privacy*, 55 WASH. L. REV. 777, 779-81 (1980) (arguing that unauthorized disclosure of personal information subjects individuals to fear of "presumptuous evaluation" and restricts their liberty).

[93] *See, e.g.*, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1651 (1999) (arguing that information privacy speech restrictions are needed to promote democratic self-rule). *But see* Volokh, *Freedom of Speech and Information Privacy, supra* note 81, at 1106-10 (criticizing attempts to restrict free speech). Courts have not been in accord as to whether there is a constitutional right to nondisclosure of personal information. *Compare* Am. Fed'n of Gov't Employees v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 791 (D.C. Cir. 1997) (noting that Supreme Court has addressed issue in recurring dicta without resolving it, but recognizing that several circuit courts have concluded that there is constitutional right to privacy in nondisclosure of personal information) *with* Doe v. Wigginton, 21 F.3d 733, 740 (6th Cir. 1994) (holding that there is no general right to nondisclosure of private information).

[94] *See* Volokh, *Freedom of Speech and Information Privacy, supra* note 81, at 1106-10 (discussing "constitutional tension" argument). In addition, arguments have been made that the government has a compelling interest in protecting people's dignity, emotional tranquility, and safety. *See, e.g.*, Robert S. Gerstein, *Intimacy and Privacy*, 89 ETHICS 76, 76 (1978) (arguing that without privacy, "intimate relationships simply could not exist"); Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26, 39 (1976) (arguing that privacy is "an essential part of the complex social practice by means of which the social group recognizes — and communicates to the individual — that his existence is his own. And this is a precondition of personhood."); Matthew Childs, *Computer Cops Versus the First Amendment*, PLAYBOY, May 1992, at 46 (quoting Lawrence Tribe's proposal made at Computers, Freedom and Privacy conference to add new Amendment to United States Constitution, reading:

> This Constitution's protections for the freedoms of speech, press, petition and assembly, and its protections against unreasonable searches and seizures and the

succeeds, a data privacy regulation may be able to withstand even higher scrutiny than that applicable to non-commercial speech.[95] Even if it does not, a regulation that gives control over transfers of personal information to the individual while recognizing both society's legitimate interests in hearing about matters of public concern, as well as the legitimate interests of commercial enterprises in collecting, analyzing, and using this information, should not be in conflict with First Amendment requirements. As the forthcoming discussion shows, this is exactly the kind of regulation advocated in this Article.[96]

IV. WHAT LEGAL THEORY SHOULD REGULATE RIGHTS IN PERSONAL INFORMATION?

One of the most serious obstacles to a successful legislative action is "the absence of a coherent understanding of the nature of information privacy interests."[97] What legal theory should underlie such legislation and in what context should courts review competing claims? As Raymond T. Nimmer has correctly pointed out:

> In the United States, privacy is a subject of rhetoric and ideas, not consistent or forceful legal analysis. The idea that privacy rights exist is an accepted political and judicial principle. Most agree that protecting personal privacy in the Information Age is a fundamental challenge in this era. Yet the idea of privacy provides limited guidance in the information age.[98]

Privacy is a notoriously amorphous concept that has been said to include a variety of rights held by an individual against both state and private actors — from the right to be free from certain kinds of intrusion to the right to make certain personal decisions.[99] The right of

---

deprivation of life, liberty or property without due process of law, shall be construed as fully applicable without regard to the technological method or medium through which information content is generated, stored, altered, transmitted or controlled.).

[95] *See, e.g.*, Trans Union Corp. v. Fed. Trade Comm'n, 267 F.3d 1138, 1140-42 (D.C. Cir. 2001) (per curiam) (finding that corporation's target marketing lists comprised speech of purely private, personal information and denied application of strict scrutiny to those lists because Fair Credit Reporting Act advanced public's concern for privacy over corporation's speech interest).

[96] *See* discussion *infra* Part VI.

[97] Jonathan P. Graham, *Privacy, Computers and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1424 (1987).

[98] RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY, ¶ 16.02, at 16-4 (2001).

[99] *See, e.g.*, Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1092-126

information privacy is a subcategory of privacy in general, and, like the "parent" concept, it reflects the uneasy coexistence of two major competing paradigms: "privacy as secrecy" and "privacy as control."

Historically, privacy has been viewed as a personal right, structured around the secrecy paradigm. This understanding takes origin in the famous definition authored by Judge Thomas M. Cooley[100] and made known by Louis Brandeis and Samuel Warren,[101] who described privacy as the "right to be let alone."[102] Under this view,[103] the information kept private (that is, secret) by an individual is entitled to legal protection from intrusion by others.[104] In recent years, however, it has become apparent that the secrecy model is unable to address information privacy concerns arising out of the realities of a modern economy in which individuals "routinely and daily place information concerning themselves into the hands of others, thereby in effect disclosing that information. Being 'let alone' in that setting is less relevant than being in control of the distribution and use by others of knowledge regarding our life."[105]

(2002) (discussing various conceptions of privacy). Solove finds six recurrent themes in the privacy discourse:

> (1) the right to be let alone — Samuel Warren and Louis Brandeis's famous formulation for the right to privacy; (2) limited access to the self — the ability to shield oneself from unwanted access by others; (3) secrecy — the concealment of certain matters from others; (4) control over personal information — the ability to exercise control over information about oneself; (5) personhood — the protection of one's personality, individuality, and dignity; and (6) intimacy – control over, or limited access to, one's intimate relationships or aspects of life.

Id.

[100] *See* THOMAS M. COOLEY, THE LAW OF TORTS 29 (1888) (declaring that person has "the right to be let alone").

[101] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) (discussing various notions of privacy and privacy rights).

[102] *Id.*

[103] *See* NIMMER, *supra* note 98, ¶ 16.02[1], at 16-5 ("The idea of a right to be let alone suggests a legal right to be free from intrusion by others into the sphere of protected or secret information concerning the person."); *see also* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1431 (2001) ("It was out of this paradigm that the Big Brother metaphor emerged. Under the paradigm, privacy is about concealment, and it is invaded by watching and by public disclosure of confidential information.").

[104] This theory has traditionally helped define the boundaries of an individual's claim to privacy in the area of constitutional law. *See, e.g.*, Katz v. United States, 389 U.S. 347, 351 (1967) (holding that no Fourth Amendment protection exists for information knowingly exposed to public, but that Fourth Amendment protects information that individual seeks to preserve in private).

[105] NIMMER, *supra* note 98, ¶ 16.02[1], at 16-5 ("The idea of a right to be let alone

Conversely, the privacy-as-control model has gained significant academic support in recent years.[106] This model treats information privacy as a form of power, the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[107] The control paradigm implements the liberal autonomy principle by seeking to place the individual at the center of decision-making about personal information use.[108] In many respects, it is a property paradigm: it presumes that an individual has a qualified right to exclude others from accessing his personal information as well as a similarly qualified right to determine the terms on which this information may become available to others.

The control paradigm has been criticized by some scholars[109] for underestimating the socio-political value of privacy and the role of the government in shaping and enforcing this value.[110] Placing reliance entirely on individual control and industry self-regulation, without further legislative or enforcement action, may, in fact, lead to further erosion of privacy. The control model, however, does not necessitate that. It is quite possible to combine that model with governmental supervision. Moreover, it is possible to allocate control so that competing interests and values of different societal groups are taken into account. Individuals' control in that case would not be absolute, just like the privacy interest is never absolute in a society; nevertheless, implementing the control model would provide a realistic and fair mechanism for the protection of that interest.

The two paradigms — "privacy as secrecy" and "privacy as control" — are reflected in attempts to define individual rights with respect to personal information through either torts or property. From the perspective of torts, an individual's right to personal information is an

---

suggests a legal right to be free from intrusion by others into the sphere of protected or secret information concerning the person.").

[106] Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000) (observing that "leading paradigm on the Internet and in the real, or off-line world, conceives of privacy as a personal right to control the use of one's data").

[107] ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).

[108] *See* Schwartz, *supra* note 106, at 820.

[109] Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 865 (2000) (pointing out that "[w]hile some of the theorists who reject the control-emphatic definition have done so as part of an effort to supplant liberalism, even liberals have rejected control-based definitions of privacy").

[110] *See* Allen, *supra* note 109, at 868 (arguing that control over personal data is neither necessary nor sufficient to protect privacy); Schwartz, *supra* note 106, at 818-34 (criticizing "bottom-up" privacy-control model).

extension of traditionally understood privacy, a personal right that may not be unreasonably infringed upon. The role of the court in such a case is to determine what kind of infringement amounts to a violation of the individual's privacy. From the property perspective, personal information is not a personal right but rather a good, and the court's job is to determine who has a prior claim to that good and how to regulate any coexisting and competing claims.

A. Current Treatment of Personal Information Under the Property and Tort Regimes

1. Current Treatment of Personal Information Under the Property Regime

Currently, neither property nor torts theory recognizes individuals' rights in their information. At the heart of that nonrecognition is a view that personal information is no ones until collected, a view similar to the "wild animals' theory" set forth in *Pierson v. Post*.[111] In that famous early American case, the court concluded that wild animals in the state of nature are not owned by anyone until captured, and that whoever captures the animal first has the prior claim to it. Today, courts view personal information in a similar fashion. Even though they often acknowledge that personal information has become a valuable commodity, they believe that it belongs to no one until collected. Accordingly, it can only be the property of a collector.[112]

This belief stands behind the decision in *Moore v. Regents of the University of California*[113] in which the court denied the plaintiff property rights in his body and his biological information. This belief is even more explicit in a few cases[114] in which plaintiffs made unsuccessful attempts to block unauthorized dissemination of personal information based on the theory of misappropriation of an individual's name.[115] The courts rejected these claims, stating, *inter alia*, that individuals do not

---

[111] 3 Cai. R. 175 (N.Y. Sup. Ct. 1805).

[112] Theoretically, individuals can compile and sell their personal data. *See Wisconsin Woman Auctions Personal Info Online*, *supra* note 52 (reporting story of Tracy Coyle, who prepared detailed docket of data about herself and announced that she would auction it to highest bidder). So far, however, this example appears to be unique.

[113] 51 Cal. 3d 120 (1990).

[114] *See, e.g.*, Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995); U.S. News & World Report, Inc. v. Avrahami, No. 95-1318, 1996 Va. Cir. LEXIS 518, at *1 (Va. Cir. June 13, 1996); Shibley v. Time, Inc., 341 N.E.2d 337, 340 (Ohio Ct. App. 1975).

[115] *See* discussion *infra* notes 159-81 and accompanying text.

have property rights in the names they use.[116]

Both federal[117] and most states'[118] laws punish identity theft. But despite the name of the offense, what these laws really aim at is future crime (e.g., theft, fraud) the commission of which is facilitated by identity theft.[119] Unless there is intent to commit that future crime, an unlawful use or transfer of identifying information does not constitute a theft of identity.

And yet, courts have consistently recognized the property rights of business enterprises in their customer lists under both state and federal laws, including laws on secured transactions, bankruptcy, and taxation.[120] Article 9 of the Uniform Commercial Code covers security interests in personal property,[121] and various state courts have held that customer lists are general intangibles, a subset of personal property.[122] Similarly, the Internal Revenue Code considers customer lists to be intangible property.[123] Bankruptcy cases view customer lists as part of the debtor's estate, which is itself comprised of property.[124]

---

[116] *Avrahami*, No. 95-1318, slip op. at *16.

[117] *See* Identity Theft and Assumption Deterrence Act ("Identity Theft Act"), 918 U.S.C. 1028, *amended by* Pub. L. No. 105-318, 112 Stat. 3007 (1998).

[118] *See* http://www.consumer.gov/idtheft/federallaws.html#statelaws (providing a list of states that have passed laws related to identity theft) (last revised Sept. 30, 2003).

[119] *See, e.g.*, Identity Theft Act, *supra* note 117, ¶ 003 (making it illegal for someone to "knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law"); *cf.* American Law Institute Model Penal Code Official Draft § 232(2) (1962) ("A person is guilty of theft if he unlawfully transfers immovable property of another or any interest therein with purpose to benefit himself or another not entitled thereto.").

[120] Miller & O'Rourke, *supra* note 8, at 788 (noting that various sets of laws, including laws on secured transactions and bankruptcy, have reinforced "property-like" nature of customer lists).

[121] *See* U.C.C. § 9-109(a)(1) (2000) (revised) ("This article applies to: (1) a transaction. . . that creates a security interest in personal property").

[122] *See, e.g., In re* Roman Cleanser Co., 802 F.2d 207, 209 (6th Cir. 1986) (holding that valid grant of security interest in general intangibles covered company's customer lists); *see also* John C. Minahan, Jr. & Bryan G. Handlos, *Scope of Article 9 of the Uniform Commercial Code*, 390 PLI/PAT 205, 212 (1986) ("Property such as customer lists. . . have been held to be general intangibles, obtaining an interest in which is subject to Article 9."); Dan L. Nicewander, *General Intangibles Under Revised Article 9*, 54 CONSUMER FIN. L.Q. REP. 169, 170 (2000) (comparing former and revised versions of Article 9 and concluding that, despite more narrow scope of definition of "general intangibles" in revised Article 9, customer lists remain within its scope).

[123] *See* Miller & O'Rourke, *supra* note 8, at 789 n.6 (noting that § 936(h)(3)(B)(v) of Internal Revenue Code defines "intangible property" to include customer lists).

[124] *See, e.g., In re* El Paso Refinery, L.P., 196 B.R. 58, 70-71 (Bankr. W.D. Tex. 1996) (citing foreclosure order naming customer lists among general intangibles); *In re* Collated Prods.

2. Current Treatment of Personal Information Under the Tort Regime

In the torts area, American courts recognize several privacy-related causes of action. Pursuant to the authoritative classification of Dean Prosser,[125] they are usually unified into four groups — false light,[126] intrusion upon seclusion,[127] public disclosure of embarrassing facts,[128] and the appropriation of name or likeness.[129] Out of those, the last three could provide a basis for recovery for an unauthorized acquisition or transfer of personal information.[130] All three theories, however, have been tested and rejected by courts in that context.

Corp., 121 B.R. 195, 197 (Bankr. D. Del. 1990) (including customer lists in general intangible assets owned by corporation), *aff'd*, Collated Prods. Corp. v. United Jersey Bank Cent., N.A., 937 F.2d 596 (3d Cir. 1991); *see also* Miller & O'Rourke, *supra* note 8, at 790 (concluding that customer lists are "almost certain 'property' within the meaning of the Bankruptcy Code").

[125] *See generally* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960) (exploring theory of privacy and four privacy torts).

[126] *Id.* at 398. The false light tort protects the individual's right to be secure from publicity that places a person in a "false light before the public." RESTATEMENT (SECOND) OF TORTS § 652E (1977).

[127] The intrusion tort protects the individual against intentional intrusion "upon the solitude or seclusion of another or his private affairs." RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[128] Prosser, *supra* note 125, at 392. This tort protects the individual against giving of "publicity to a matter concerning the [individual's] private life" where such matter is not of legitimate concern to the public, and the nature of the disclosure would be "highly offensive" to a reasonable person. RESTATEMENT (SECOND) OF TORTS § 652D (1977).

[129] Prosser, *supra* note 125, at 389. This tort protects the individual against the appropriation of his name or likeness to the use or benefit of another. *See* RESTATEMENT (SECOND) OF TORTS § 652C (1977).

[130] The false light tort is unlikely to apply to unauthorized dissemination of personal information because, under that tort, the information has to be false or erroneous. Personal information transferred by primary collectors into the secondary market usually has been provided by individuals themselves and is, in most instances, true and correct. An argument may be made that a certain "profile" that is the subject matter of a transfer may put an individual in a false light just by virtue of being limited and/or one-sided. This argument is unlikely to succeed because no information is "complete;" therefore, it could lead to a rule where no information may be transferred at all. Even if such a rule is to be made, it should be made on a theory other than "false light." This tort nonetheless may have a limited application to protect an individual against dissemination of erroneous information in situations when the information was not provided by the individual and when the defendant has not taken proper steps to ensure its correctness. *See, e.g.*, Dun & Bradstreet, Inc. v. Greenmoss Builders, 472 U.S. 749 (1985) (allowing suit against credit bureau for incorrect credit report disseminated to third parties).

a. Intrusion Upon Seclusion

Invasion of privacy by "intrusion" occurs when a person intentionally intrudes, physically or otherwise, into the solitude or seclusion, or private affairs or concerns, of another in a manner that is highly offensive to a reasonable person.[131] In the context of personal information, the utility of this tort is rather limited because it may apply only to unlawful collection of data, not to its use or disclosure.[132] Courts generally require plaintiffs to establish the following four elements: (i) an unauthorized intrusion or prying into the plaintiff's seclusion; (ii) which is offensive or objectionable to a reasonable person; (iii) as to a matter which is private; and (iv) which has caused anguish and suffering.[133]

The intrusion does not have to be of a physically defined place — it can be of one's "personality" or "psychological integrity."[134] Based on that theory, a group of American Express cardholders filed a class action against American Express companies for their practice of renting information regarding cardholder-spending habits.[135] The practice included categorizing and ranking cardholders into tiers based on their spending record, and then renting this information to participating merchants.[136] In order to draw spending profiles, American Express analysts considered where their cardholders shopped and how much they spent, as well as their behavioral characteristics and spending histories.[137] Plaintiffs argued that, because American Express rented lists based on this compiled information, such practice involved the disclosure of private financial information and resembled cases involving intrusion into private financial dealings, such as bank account transactions.[138]

---

[131] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[132] *See* Fenrich, *supra* note 9, at 972 n.150 (pointing out that tort of intrusion may be relevant to data collection rather than dissemination); *see also* Reidenberg, *supra* note 3, at 222-23 (noting that intrusion tort does not address such data protection practices as storage, use, or disclosure of personal information).

[133] *See* Miller v. Motorola, Inc., 560 N.E.2d 900, 904 (Ill. App. Ct. 1990) (listing elements of tort of intrusion); PETA v. Bobby Berosini, Ltd., 895 P.2d 1269, 1279 (Nev. 1995); Davis v. Temple, 673 N.E.2d 737, 744 (Ill. App. Ct. 1996).

[134] *See* Phillips v. Smalley Maint. Servs., 435 So. 2d 705, 711 (Ala. 1983) ("One's emotional sanctum is certainly due the same expectations of privacy as one's physical environment.").

[135] Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1352-53 (Ill. App. Ct. 1995).

[136] *Id.* at 1353.

[137] *Id.*

[138] *Id.* at 1354.

The court rejected the claim of intrusion, stating that the plaintiffs failed to establish the first element of the tort — an unauthorized intrusion or prying into the plaintiffs' seclusion: "[b]y using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences."[139] Therefore, the court concluded, American Express did not commit unauthorized intrusion upon cardholders' seclusion by merely compiling and renting information voluntarily given to it.[140]

In a recent case, the Supreme Court of New Hampshire added a twist to this analysis.[141] In *Remsburg v. Docusearch, Inc.*, the court had to decide whether an investigator may be held liable for obtaining a person's social security number from a credit reporting agency without her knowledge or consent, as well as for obtaining her work address by making a pretextual phone call.[142] The *Remsburg* court differentiated between information that may be reasonably expected to remain private even after it was disclosed by the plaintiff to a third party (social security number) and information that is not so "secret, secluded or private" (work address).[143] It concluded that only in the first case may a plaintiff maintain a cause of action for intrusion upon seclusion, and only if the plaintiff can prove that such intrusion would be offensive to a person of ordinary sensibilities.[144] In determining whether the intrusion was sufficiently offensive, the fact finder was to consider "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded."[145]

These two cases reveal why the tort of intrusion upon seclusion cannot serve as a mechanism for regulating rights in personal information in general. The intrusion upon seclusion tort protects only "secret" information, i.e., the information that either has never been communicated to anyone (*Dwyer*) or is highly personal in its character

---

[139] *Id.*

[140] *Id.*

[141] Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003).

[142] *Id.* at 1004-05.

[143] Fischer v. Hooper, 732 A.2d 396, 400 (N.H. 1999) (quoting Hamberger v. Eastman, 106 N.H. 107, 110 (1964)).

[144] *Remsburg*, 816 A.2d at 1008-09.

[145] *Id.* (quoting Bauer v. Ford Motor Credit Co., 149 F. Supp. 2d 1106, 1109 (D. Minn. 2001)).

(*Remsburg*). Since the problem of unauthorized transfers of personal information involves information of various degrees of secrecy, disclosed by individuals sometimes more, sometimes less consciously, this tort is unable to provide a comprehensive solution.

b. Disclosure of Private Facts

The disclosure tort is triggered by public disclosure of private facts in which the disclosure is highly offensive to a reasonable person.[146] Several requirements, however, limit the availability of this tort. One limitation is that the information must be communicated to a sufficient number of people, so that it is "substantially certain to become. . . public knowledge."[147] It is a matter of degree as to how many persons must have seen or heard the information to constitute the "public" but, under the prevalent standard, it is unlikely that a sale of personal information by a primary collector to a secondary collector would meet the requirement of publicity.[148]

Another limitation imposed on this cause of action is that the disclosed information be offensive and objectionable to a reasonable person of ordinary sensibilities.[149] Courts have proclaimed that the disclosure tort "is not intended for the protection of any shrinking soul who is abnormally sensitive about such publicity."[150] The more personal the information disclosed, the greater the intrusion upon an individual's

---

[146] *See* Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1353 (Ill. App. Ct. 1995).

[147] RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (1977); *see also* Tureen v. Equifax, Inc., 571 F.2d 411, 419 (8th Cir. 1978) (holding that disclosure of health record by consumer credit reporting firm to insurance firm client does not rise to level of "publication"); Houghton v. New Jersey Mfrs. Ins. Co., 615 F. Supp. 299, 307 (E.D. Pa. 1985), *rev'd on other grounds*, 795 F.2d 1144 (3d Cir. 1986) (finding that circulation of investigative report in personal injury suit to "only a very small group of persons" does not satisfy publicity requirement); Porten v. Univ. of San Francisco, 134 Cal. Rptr. 839, 841 (Cal. Ct. App. 1976) (holding that disclosure by University to State Scholarship and Loan Commission of student's grades is not communication "to the public in general or to a large number of persons"); Robins v. Conseco Fin. Loan Co., 656 N.W.2d 241, 245 (Minn. Ct. App. 2003) (disclosure of applicant's negative credit information by lender to applicant's fellow employee is not public disclosure even if fellow employee repeated information to others); Childs v. Williams, 825 S.W.2d 4, 9 (Mo. Ct. App. 1992) (letter from physician to patient's employer was not public disclosure where letter was available only to small group of supervisors).

[148] *See* MCCARTHY, *supra* note 60, § 5:80 (discussing publicity requirement).

[149] *See* WILLIAM L. PROSSER, LAW OF TORTS § 117, at 811 (4th ed. 1987).

[150] Prosser, *supra* note 125, at 397; *see also* Forsher v. Bugliosi, 608 P.2d 716, 723 (Cal. 1980) ("[s]ome person with extra sensitive perception. . . cannot compel this court to establish liability at so low a threshold.").

privacy.[151] The disclosure of merely neutral facts — of the kind that once prompted Warren and Brandeis to write their famous article — was held not actionable.[152]

---

[151] *See* Bratt v. Int'l Bus. Mach. Corp., 785 F.2d 352, 360 (1st Cir. 1986); *see also* MCCARTHY, *supra* note 60, § 6:9 (listing cases involving disclosure of private facts). Examples of cases in which courts found a disclosure to be highly offensive to a reasonable person include: Sheets v. Salt Lake County, 45 F.3d 1383, 1388 (10th Cir. 1995) (finding it offensive to disclose diary of deceased spouse, which revealed private thoughts regarding marriage and surviving spouse); Susan S. v. Israels, 67 Cal. Rptr. 2d 42, 47 (Cal. Ct. App. 1997) (holding that defendant's unauthorized reading and dissemination of plaintiff's mental health records constituted serious invasion of privacy); Urbaniak v. Newton, 277 Cal. Rptr. 354, 360 (Cal. Ct. App. 1991) (ruling that disclosure of HIV positive status is invasion of privacy right and offensive to reasonable person); Doe v. High-Tech Inst., Inc., 972 P.2d 1060, 1066-67 (Colo. Ct. App. 1998) (rejecting defendant's argument that plaintiff had no privacy interest in blood sample); Green v. Chicago Tribune Co., 675 N.E.2d 249 (Ill. App. Ct. 1996) (finding that newspaper's public disclosure of mother's spoken farewell to dead son over body in hospital room after he had been shot to death may constitute invasion of privacy); Miller v. Motorola, Inc., 560 N.E.2d 900, 903 (Ill. App. Ct. 1990) (reversing dismissal of plaintiff's claim because employer's disclosure of mastectomy may be invasion of privacy); Doe v. Mills, 536 N.W.2d 824, 829-30 (Mich. Ct. App. 1995) (deciding that anti-abortion protestor's public disclosure of plaintiff's name and future plans for abortion on poster may be invasion of privacy); Young v. Jackson, 572 So. 2d 378, 382 (Miss. 1990) (affirming district court's summary judgment in favor of defendant despite plaintiff's legal right in keeping hysterectomy private); Mason v. Williams Disc. Ctr., Inc., 639 S.W.2d 836, 838 (Mo. Ct. App. 1982) (concluding that plaintiff had actionable claim against local store for posting sign implying that plaintiff wrote bad checks); Hillman v. Columbia County, 474 N.W.2d 913, 920 (Wis. Ct. App. 1991) (finding potential violation of constitutional right to privacy in prison's disclosure of inmate's HIV status to fellow inmates).

[152] Examples of situations in which courts have found that a reasonable person would not be highly offended by the disclosure of neutral information include: Howell by Goerdt v. Tribune Entm't, 106 F.3d 215, 220-21 (7th Cir. 1997) (airing television show in which plaintiff was depicted as rowdy teenager is not invasion of privacy); Wood v. Nat'l Computer Sys., Inc., 814 F.2d 544, 545 (8th Cir. 1987) (noting that defendant's inadvertent revelation of plaintiff's passing test score to one person is not highly objectionable); Lodge v. Shell Oil Co., 747 F.2d 16, 20 (1st Cir. 1984) (holding that termination from employment is not private fact); Med. Lab. Mgmt. Consultants v. Am. Broad. Cos., 30 F. Supp. 2d 1182, 1191 (D. Ariz. 1998) (broadcasting undercover investigation of plaintiff's medical lab was not highly offensive); Briggs & Stratton Corp. v. Nat'l Catholic Reporter Publ'n Co., 978 F. Supp. 1195, 1200 (E.D. Wis. 1997) (disclosing person's religious affiliation is not defamatory); Galdauckas v. Interstate Hotels Corp., 901 F. Supp. 454, 470 (D. Mass. 1995) (writing plaintiff's age on birthday card circulated to fellow employees is not invasion of privacy); Grunseth v. Marriott Corp., 872 F. Supp. 1069, 1075-76 (D.D.C. 1995) (staying overnight in a certain hotel is not grounds for invasion of privacy suit); Wolf v. Regardie, 553 A.2d 1213, 1215, 1220 (D.C. Cir. 1989) (publishing article about plaintiff's wealth is not private matter highly offensive to reasonable person); Int'l Ass'n of Fire Fighters Local 1264 v. Mun. of Anchorage, 973 P.2d 1132, 1136 (Alaska 1999) (holding that municipal employees do not have legitimate expectation of privacy in their salaries); Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1354 (Ill. App. Ct. 1995) (selling plaintiff's credit card information is not unauthorized intrusion); Bisbee v. John C. Conover Agency, 452 A.2d 689, 691 (N.J. Super. Ct. App. Div. 1982) (affirming motion for summary judgment because

In most instances the lifestyle information that is the subject of commercial transfers does not reach the level of "highly personal and embarrassing."[153] Combined with the fact that a transfer of personal information from the primary collector to the secondary market is unlikely to be viewed as public disclosure, that more or less disqualifies this tort as a possible cause of action for plaintiffs attempting to control the use and transfer of their personal information.

c. Invasion of Privacy by Appropriation and the Right of Publicity

The appropriation tort, as well as the related right of publicity,[154] consists of the appropriation of the plaintiff's name, picture, or likeness for the defendant's benefit or advantage.[155] Classic examples that give rise to both torts include unauthorized use of an individual's name or picture to advertise the defendant's product,[156] to add luster to the name of a corporation,[157] or for other business purposes.[158] The appropriation tort or the right of publicity is recognized virtually in every state through either statutory or common law,[159] the difference between the two often

---

disclosure that plaintiff bought expensive house is not invasion of privacy); Johnson v. Harcourt, Brace, Jovanovich, Inc., 118 Cal. Rptr. 370, 380 (Cal. Ct. App. 1974) (sustaining defendant's demurrer because revealing that plaintiff found and returned large sum of money was laudatory and not invasion of privacy).

[153] *See, e.g.*, King County v. Sheehan, 57 P.3d 307, 316 (Wash. Ct. App. 2002) (opining that state statute based on *Restatement (Second) of Torts* would not protect names of county police officers from disclosure because statute "only applies to personal information that employees would not normally share with strangers"); Webb v. City of Shreveport, 371 So. 2d 316, 319 (La. Ct. App. 1979) (holding that people have no reasonable expectations of privacy as to their identity or as to where they live or work).

[154] The difference between the appropriation tort and the right of publicity stems not from the actions of the defendant but rather from "the nature of the plaintiff's rights and the nature of the resulting injury. [W]hile the appropriation branch of the right of privacy is invaded by an injury to the psyche, the right of publicity is infringed by an injury to the pocketbook." Prosser, *supra* note 125, at 402.

[155] *See* Prosser, *supra* note 125, at 401.

[156] *See, e.g.*, Pavesich v. New England Ins. Co., 50 S.E. 68 (Ga. 1905) (recognizing, for the first time, individual's rights in identity, this case involved artist whose picture was used by insurance company to promote life insurance).

[157] *See, e.g.*, Cordell v. Detective Publ'n Inc., 307 F. Supp. 1212 (D. Tenn. 1968) (involving claim of invasion of privacy by appropriation to add luster to corporation's name when defendant company published story about murder of plaintiff-mother's daughter); Martinez v. Democrat-Herald Publ'g Co., 669 P.2d 818 (Colo. Ct. App. 1983) (holding that defendant's portrayal of plaintiff as drug user in photograph published in newspaper did not constitute appropriation).

[158] MCCARTHY, *supra* note 60, § 5:61.

[159] *See* W. PAGE KEETON ET AL., PROSSER & KEETON ON THE LAW OF TORTS § 117, at 851-54 (4th ed. 1987) (discussing appropriation tort and protection of one's name, image, or likeness under statutory law in states such as New York).

being ignored.[160]

In recent years, plaintiffs in three different state court cases (*Shibley v. Time, Inc.*,[161] *Dwyer v. American Express Co.*,[162] and *U.S. News and World Report v. Avrahami*[163]) attempted to apply some form of the appropriation tort to enjoin unauthorized dissemination of personal information through the sale of mailing lists. All those attempts have failed.[164]

In *Shibley*, a class action against *Time Magazine, Esquire, Playboy, Ladies Home Journal*, and the issuer of American Express credit cards, the court rejected plaintiffs' claim that the defendants' practice of selling subscription lists to direct-mail advertisers without the prior consent of subscribers amounted to an "appropriation of one's personality."[165] The court opined that the "appropriation or exploitation of one's personality" recognized by Ohio law may be invoked only in "those situations where the plaintiff's name or likeness is displayed to the public to indicate that the plaintiff endorses the defendant's product or business."[166] The *Shibley* court rejected plaintiffs' claim as a matter of either privacy or property right.

---

[160] In this paper, the "right of publicity" and the "tort of appropriation" are often used interchangeably.

[161] Shibley v. Time, Inc., 341 N.E.2d 337, 340 (Ohio Ct. App. 1975).

[162] Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1351 (Ill. App. Ct. 1995).

[163] U.S. News & World Report, Inc. v. Avrahami, No. 95-1318, 1996 Va. Cir. LEXIS 518, at *1 (Va. Cir. June 13, 1996).

[164] Another case that deals with unauthorized commercial dissemination of personal information has yet to reach trial. In *Weld v. CVS Pharmacy, Inc.*, 1999 Mass. Super. LEXIS 261 (Mass. Super. Ct. 1999); *cert. of class action aff'd sub nomo* Weld v. Glaxo Wellcome, Inc., 746 N.E.2d 522 (Mass. 2001), a group of customers sued a pharmacy for sharing customer prescription information with certain drug manufacturers. The court rejected the defendants' motion for summary judgment, acknowledging that, as a matter of law, CVS's marketing activities with drug manufacturers could amount to a violation of customers' privacy as well as to a "sale of the plaintiffs' names, addresses and personal prescription information, from which the defendants profited." *Id.* at *20. The court opined that although Massachusetts did not expressly recognize a separate cause of action for tortious misappropriation of private information, and although that claim was probably preempted by a state statute prohibiting the use of an individual's name for "the purposes of trade without his written consent," the plaintiffs should still be allowed to proceed with their claim. *Id.* at *21, n.19. The court concluded that the "facts alleged by plaintiffs, (i.e. the use of plaintiffs' private information for the defendants' financial gain), falls [sic] within the scope of [the appropriation] cause of action." *Id.* at *22. That conclusion does not by itself imply that the court views personal information as the property of the plaintiffs, but it does not preclude such interpretation either.

[165] *Shibley*, 341 N.E.2d at 339.

[166] *Id.*

In *Dwyer*, the court used the same argument[167] to deny relief to a group of American Express cardholders who claimed that American Express's practice of selling their spending profiles to participating merchants amounted to the appropriation of cardholders' names and perceived lifestyles.[168] The court opined that "an individual name has value only when it is associated with one of defendants' lists"[169] and that "[d]efendants create value by categorizing and aggregating these names."[170] Implicit in that conclusion was the court's view that, to the extent personal information may be viewed as property, that property belongs to the one who collects it.

The arguments in *Avrahami* resemble those made in *Shibley* and *Dwyer*. In that case, an individual plaintiff sued *U.S. News & World Report* for renting out his name (or rather one of the names he used) as a part of its subscriber lists. The appellate court of Virginia rejected the plaintiff's claim, stating that the tort of appropriation is intended only to give redress to a person whose name, portrait, or picture was used for advertising purposes or for the purposes of trade.[171] The inclusion of an individual name in a mailing list did not constitute a use for either advertising or trade, as defined by Virginia statute.[172] Moreover, the court stated that Mr. Avrahami had no property rights in the names he used, therefore *U.S. News* neither violated the statute nor committed common-law conversion by including his name as part of a mailing list exchange.[173]

It is not quite clear how broadly the *Avrahami* opinion should be read. On the one hand, the language of the opinion is rather sweeping — individuals have no property right in the names they use.[174] On the other hand, that broad language may be qualified by the fact that the name in question was not Mr. Avrahami's true name, i.e., arguably, it was not really a part of his personality. The court repeatedly emphasized the fact that Mr. Avrahami had used "nineteen names... in the past five

---

[167] *Dwyer*, 652 N.E.2d at 1355 (holding that tort of appropriation is inapplicable because it only protects "a person from having his name or image used for commercial purposes without consent").

[168] *See id.* at 1356.

[169] *Id.*

[170] *Id.*

[171] U.S. News & World Report, Inc. v. Avrahami, No. 95-1318, 1996 Va. Cir. LEXIS 518, at *16 (Va. Cir. June 13, 1996).

[172] *See id.*

[173] *Id.*

[174] *Id.*

years,"[175] that he "had intentionally used a false name"[176] and "affirmatively created this litigation by using a false name."[177] Finally, it is possible that the court may believe that individuals have property rights in their name (or true name), but that the practice of selling or renting mailing lists does not give rise to either a statutory appropriation or a common-law conversion because such practice does not constitute exercise of dominion or control of such magnitude as to deprive a person of possession of his name.[178] Or, using the words of the opinion, such practice does not "invade any property right [an individual] *may have* in his name."[179]

Finally, the most recent unsuccessful attempt to the appropriation theory for protection of personal information is *Remsburg*,[180] a case concerning a woman killed by a stalker who acted on the information supplied by a private investigator. The New Hampshire Supreme Court did not allow a misappropriation claim against the investigator, explaining that the tort "does not protect one's name per se; rather it protects the value associated with that name."[181] There is no cause of action if a person's name was published for purposes other than taking advantage of the "reputation, prestige or other value" associated with the person.[182] In this case, the investigator capitalized not on the victim's reputation or prestige but rather on his client's willingness to pay.[183] Accordingly, the court held that "a person whose personal information is sold does not have a cause of action for appropriation against the investigator who sold the information."[184]

---

[175] *Id.* at *4, *15.

[176] *Id.* at *14.

[177] *Id.* at *18. The court viewed with skepticism Mr. Avrahami's motives for commencing the litigation, which appeared to be a public relations campaign. Mr. Avrahami had made a statement that "one of the primary reasons he filed suit was that the notoriety would help him meet 'chicks.'" *Id.* at *15. Later, Mr. Avrahami wrote a letter to the Direct Marketing Association (the "DMA"), proposing a mechanism for handling personal information that requires explicit consent of consumers. For the text of the letter see http://www.epic.org/privacy/junk_mail/DMAletter.html (June 24, 1996). The DMA president has rejected the suggestion. For the text of the reply, see http://www.epic.org/privacy/junk_mail/DMAresponse.html (July 15, 1996).

[178] *See Avrahami*, 1996 Va. Cir. LEXIS 518, at *18.

[179] *Id.* (emphasis added).

[180] Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003).

[181] *Id.* at 1009 (quoting Matthews v. Wozencraft, 15 F.3d 432, 437 (5th Cir. 1994)).

[182] *Id.* (quoting RESTATEMENT (SECOND) OF TORTS § 652C cmt. d, at 382-83).

[183] *Remsburg*, 816 A.2d at 1010.

[184] *Id.* The *Remsburg* court nevertheless concluded that the defendant may be held liable under the general negligence theory. It held:

The lesson of the outlined opinions is quite uniform: courts are reluctant to expand the scope of the appropriation tort beyond advertising and related purposes. Although courts admit that personal information compiled by collectors is property, they deny that it was property before it was collected. It is easy to see a flaw in the logic of the courts: not only do they equate property with monetary value (which is not always the case — my drawings may have no monetary value but they are still my property), but even when individual personal information has a price tag attached (*Remsburg*), they still refuse to enforce the plaintiff's right to it. Thus, in their current form, none of the privacy-related torts are conceptually suited to protect an individual's personal information.

B. Property or Torts?

As the preceding discussion shows, the current law recognizes neither personal nor property rights of individuals in personal information. That conceptual lacuna makes the choice of an appropriate legal theory particularly important. In this section, I argue in favor of the property regime as opposed to the tort regime, for the following three reasons: (i) the torts approach cannot support a consistent, workable mechanism for the enforcement of information privacy rights; (ii) U.S. law, explicitly or implicitly, already regards personal information as property; and (iii) the property regime better serves the interests of individual parties and society in general.

Several scholars have argued that individual privacy with respect to personal information should be protected through the expansion of either the disclosure tort[185] or the appropriation tort.[186] These proposals

---

> The threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client.... This is especially true when, as in this case, the investigator does not know the client or the client's purpose in seeking the information.

Id. at 1008.

[185] *See* Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 574 (1998) (arguing that courts should "take affirmative steps to prohibit [Social Security Number] and name dissemination" by expanding the use of disclosure and appropriation torts); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1312 (2000) (arguing in favor of tort regime over property regime because it "avoids the trap of alienability the perverse incentives that a market in alienable personal data would create.").

may mitigate some of the current problems but would leave most significant issues unresolved.

As for the disclosure tort, it protects only information that is kept secret. The secrecy model of privacy, however, is not able to address many of the vital personal interests involved in the modern information economy.[187] Specifically, that model fails to take into account that in today's world "individuals are encompassed within a web of information about what they do, and when and why."[188] Most of that information is voluntarily disclosed by individuals, and therefore is not eligible for protection under the disclosure tort.

Another problem with the tort of disclosure is that, even if the boundaries of protected information were expanded, courts would still have to measure alleged violations against a *reasonable* expectation of privacy. That raises both moral and practical concerns because what is *reasonably* private varies dramatically across different social, economic, and cultural groups.[189] Someone who lives in a mansion would probably have different expectations of privacy than someone who lives on the street. Unless we, as a society, are prepared to treat individuals in different socio-economic groups differently, we cannot accept this approach. In addition, as concerns surrounding transfer of personal information become increasingly international in scope, what is or is not reasonable will depend on the standard adopted in each particular jurisdiction. For instance, as has been already suggested,[190] American companies trying to qualify for the "Safe Harbor" may end up adopting two different standards — the higher one for European customers and the lower one for domestic customers.

Making "reasonable expectations of privacy" a cornerstone of a regulatory structure is problematic even on the most basic theoretical

---

[186] *See* Fenrich, *supra* note 9, at 994-1003 (arguing that courts should apply either appropriation tort or right of publicity to protect individuals from unwanted commercial use of their personal information); *see also* Mary Jo Obee & William C. Plouffe, Jr., *Privacy in the Federal Bankruptcy Courts*, 14 NOTRE DAME J.L. ETHICS & PUB. POL'Y 1011, 1027 (2000) (discussing that various torts, including tort of appropriation, "provide the basis for causes of action for violation of information privacy," *noted in* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1159 (1997)).

[187] *See* discussion *supra* notes 101-04 and accompanying text.

[188] NIMMER, *supra* note 98, at 16-5.

[189] *Cf.* Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 125 n.18 (2002) (noting, in context of Fourth Amendment inquiry, that "reasonable expectations of privacy" are formed by individual's political and cultural background).

[190] *See* discussion *supra* notes 75-77 and accompanying text.

level because the question begs the answer — what expectations are reasonable depends on the existing practice, which in turn depends on the allocation of legal entitlements. At this point, the balance of rights is so heavily tilted in favor of collectors, that it is probably unreasonable to expect that our personal information will not be abused.

The proposal to expand the appropriation tort does not create a comprehensive solution to the problem either. Both courts and scholars have pointed out that the tort of appropriation differs from other privacy-based torts in that, unlike the other three torts that safeguard the personal rights of an individual, this tort is proprietary in nature,[191] it protects "a right of value upon which the plaintiff [should be able to] capitalize by selling licenses."[192]

Expanding the appropriation tort to cover personal information would mean implicitly recognizing the proprietary nature of such information.[193] But why should a proprietary interest be regulated entirely through torts? Torts give individuals only negative rights by protecting recognized interests of individuals from infringement by others. Why shouldn't the owner of personal information have affirmative rights as well, including the right to alienate it like any other property? The question is particularly salient in the American legal system, which disfavors restrictions on free alienation of property.

The appropriation tort is, in essence, a form of the tort of conversion[194] that protects an individual's proprietary interest from misappropriation. No one suggests, however, that claims of individuals with respect to real or personal property should be regulated entirely through the tort of conversion. In other words, the tort theory can help to regulate some incidents of ownership; but where proprietary interests are involved, it plays only a secondary role compared to the property regime.

---

[191] *See* Prosser, *supra* note 125, at 406 ("It seems sufficiently evident that appropriation tort is quite a different matter from intrusion, disclosure of private facts, or a false light in the public eye. The interest protected is not so much a mental as a proprietary one, in the exclusive use of the plaintiff's name and likeness as an aspect of his identity.").

[192] *Id.*

[193] In fact, in many areas of the law, personal information is already viewed as property, just not the property of an individual. *See* discussion *supra* notes 118-22 and accompanying text.

[194] "Conversion" is defined as the wrongful possession or disposition of another's property as if it were one's own; an act or series of acts of willful interference, without lawful justification, with a chattel in a manner inconsistent with another's right, whereby that other person is deprived of the use and possession of the chattel. BLACK'S LAW DICTIONARY 333 (7th ed. 1999).

On a more abstract level, the choice between the tort regime and the property regime for the protection of personal information means the choice between property rules and liability rules as defined in the seminal article authored by Calabresi and Melamed.[195] According to their theory, an "entitlement is protected by a property rule to the extent that someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in which the value of the entitlement is agreed upon by the seller."[196] The liability rule protects an entitlement in the sense that holders must be compensated whenever the entitlement is taken away from them without their consent, the value of the entitlement being "determined by some organ of the state rather than by the parties themselves."[197]

A society chooses which rule to employ in relation to a particular entitlement based on a variety of considerations. For Calabresi and Melamed, the main reason to choose one rule over another is efficiency, although the authors recognize that other reasons, such as distributional goals[198] and avoiding moral harm to the individual or the society at large,[199] are also valid considerations. The property rule requires the least amount of state intervention since the value of an entitlement is determined by two willing participants in a voluntary transaction.[200] Therefore, unless there are special circumstances, the property rule is the most efficient. The liability rule may be preferred where a "market valuation of the entitlement is deemed inefficient," i.e., "either unavailable or too expensive compared to a collective valuation,"[201] or where it "facilitates a combination of efficiency and distributive results which would be difficult to achieve under a property rule."[202]

From the utilitarian perspective, it may appear more efficient to value personal information objectively, thus avoiding the costs of negotiations with each particular individual. The preference for the liability rule, however, would mean that individual entitlements to personal information recognized under tort law would have to be enforced

---

[195] *See* Guido Calabresi & Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972) (discussing different entitlement regimes in society).

[196] *Id.* at 1092.

[197] *Id.*

[198] *See id.* at 1110.

[199] *Id.* at 1112-13 (discussing external costs in constructing rules of alienability).

[200] *See id.* at 1092.

[201] *Id.* at 1110.

[202] *Id.*

exclusively by litigation, on a case-by-case basis, which would involve considerable expenditures of funds and time, both by litigants and the judicial system. Moreover, in order to recover, the plaintiff will have to prove actual damages, which most likely will be trivial. That by itself will discourage people from bringing lawsuits against those who violate their rights in personal information, thereby making the rule inefficient.

The choice of the liability regime is even less persuasive if utility is not limited to efficiency but instead is understood, in Mill's words, as "utility in the largest sense, grounded on the permanent interests of man as a progressive being."[203] By that, Mill spoke to everyone's right of free choice, which may be curtailed only to prevent "harm to others."[204] In light of this understood utility, a society may be justified in interfering with a voluntary transfer of personal information between an individual and a collector only if the society can show that allowing a free exchange would hurt someone else or the public in general.

Arguments have been made that the property regime may hurt the public in general:[205] if collectors are forced to negotiate with individuals for the sale of personal information, transaction costs would rise and the scope of personal information available to various industries would decrease.[206] Even assuming *arguendo* that a certain decrease does follow,[207] it is far from clear that it would noticeably hurt the public. Most probably, under Mill's theory, it would be one of those "constructive injur[ies] which a person causes to society, by conduct which neither violates any specific duty to the public, nor occasions perceptible hurt to any assignable individual except himself [and] which society can afford to bear, for the sake of the greater good of human freedom."[208]

---

[203] JOHN STUART MILL, ON LIBERTY, ch. 1, ¶ 11 (New York 1869).

[204] *Id.*

[205] *See, e.g.*, Ian Ayres & Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 YALE L.J. 1027, 1032 (1995) (arguing in favor of liability rule rather than property rule because liability rule "possess[es] an information-forcing" quality which facilitates "more efficient trade"); Neil W. Netanel, *Copyright and a Democratic Civil Society*, 106 YALE L.J. 283, 334-35 (1996) (arguing in favor of liability rules to promote bargaining around compulsory licenses).

[206] *See, e.g.*, Ayres & Talley, *supra* note 205, at 1093-94 (arguing that, in case of dispute, liability rule would minimize costs by facilitating exchange of information, while property right rule would lead to deadlocks in negotiations). *But see* Robert P. Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 CAL. L. REV. 1293, 1304-05 (1996) (showing that Ayres & Talley's model is inapplicable when more than two parties are negotiating).

[207] *See* discussion *infra* notes 234-49 and accompanying text.

[208] MILL, *supra* note 203, at ch. 4, ¶ 11.

From a broader perspective, not limited to utilitarian or libertarian arguments, it would be even more difficult to justify the choice of the liability regime — the regime that, on the one hand, recognizes the alienability of personal information and gives the initial entitlement therein to individuals but, on the other hand, allows anyone but individuals to decide whether that entitlement should be transferred and at what price. It is preferable from the viewpoint of individual fairness and collective benefit, as well as logic and intellectual consistency, to regulate personal information through the property rule, which affords the individual maximum control over personal information and allows all interested parties to enter into mutually acceptable transactions without tying up valuable societal resources. Privacy torts may still play an important role under specific circumstances defining those torts — as a separate claim (e.g., the tort of disclosure where the defendant published highly embarrassing information voluntarily supplied by the plaintiff for a narrow purpose) or an additional theory for recovery. However, property should serve as a general paradigm for new legislation regulating issues relating to personal information.

V. WHOSE PROPERTY?

The choice of the property regime for regulating personal information does not by itself determine how property rights should be allocated between the individual and collectors. Why should the individual's claim to her personal information be prior to the claim of collectors? On the intuitive level, the answer is that this information exists regardless of whether or not it has been collected. It exists as an extension of the individual's personality — just like the individual's name or likeness that are protected by the right of publicity:

> if one's own image, for example, is treated as an object capable of 'being yours or mine,' why should it not be claimed by the person who is its natural source? To the extent it is available as some person's property... its source would seem to have the strongest claim.[209]

Various theories of property may serve to support this intuitive conclusion. Most recognized among those[210] are Lockean labor-desert

---

[209] Alice Haemmerli, *Whose Who? The Case for a Kantian Right of Publicity*, 49 DUKE L.J. 383, 418 (1999).

[210] *See* Symposium, *Cyberspace and Privacy: A New Legal Paradigm? Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1380 (2000)

theory,[211] the utilitarian theory,[212] and the "personality" theory.[213]

A. Locke: Labor-Desert Theory

The labor-desert theory, at first glance, seems to protect the rights of collectors rather than the rights of individuals because it suggests that a person who invests her labor in a common good acquires a property right in it.[214] At a closer look, however, one would reach a different conclusion. Locke based his theory on the assumption that in the primitive state of nature there are enough unclaimed goods so that everyone can appropriate the objects of their labor without infringing upon goods that have been appropriated by others.[215] It follows that one may acquire property rights in a good by investing one's labor only if the good is not already owned by someone else.

At the same time, Locke's primary underlying assumption is that "every Man has a Property in his own Person."[216] A "person" for Locke is "a thinking intelligent being, that has reason and reflection, and can consider itself as itself, the same thinking thing in different times and places."[217] Using modern terms, Locke defines a person through the individual's personal identity, which, among other things, should include the individual's personal information — the unique collection of facts that makes the individual who she is. If that is the case, then everyone has an original property right in her personal information, i.e., personal information does not exist in the state of nature, it is already

---

("Mainstream property theorists recognize two main theoretical justifications for ownership: Lockean labor-desert theory, and a more explicitly utilitarian theory that focuses on economic efficiency."); Justin Hughes, *The Philosophy of Intellectual Property*, 77 GEO. L.J. 287, 288 (1988) ("The main alternative to a labor justification is a 'personality theory' that describes property as an expression of the self.").

[211] *See generally* JOHN LOCKE, TWO TREATISES OF GOVERNMENT (Peter Laslett ed. rev. 1963) (1690) (developing theory of property based on individual investment of labor in common good).

[212] *See generally* JEREMY BENTHAM, *Principles of Morals and Legislations*, *in* 1 SELECT EXTRACTS FROM THE WORKS OF JEREMY BENTHAM 1, 1-4, 11-12 (Thoemmes Press 1995) (1843) (developing theory of property of law based on maximization of welfare).

[213] *See generally* GEORG WILHELM FRIEDRICH HEGEL, PHILOSOPHY OF RIGHT (T. M. Knox trans., 1942) (developing theory of property and personhood).

[214] *See, e.g.*, Harris S. Gordon, et al., *Customer Relationship Management: A Senior Management Guide to Technology for Creating a Customer-Centric Business*, *at* http://www.the-dma.org/bookstore/cgi/displaybook?product_id=009163 (last visited Mar. 1, 2003) (regarding personally identifiable data as property of collectors who have invested in compiling databases).

[215] *See* LOCKE, *supra* note 211, at 33.

[216] *See id.* at 328-29.

[217] *Id.* ¶ 9.

owned. Under Lockean theory, therefore, collectors of personal information should not be permitted to acquire a property right that is superior to the property right of the individual who is the subject matter of the collected data — just as someone who picks flowers in a neighbor's front yard may not acquire property rights in these flowers superior to the property rights of the neighbor.[218]

B. Utilitarian Theory

Under the utilitarian theory, rights should be allocated so as to maximize human satisfaction or benefit.[219] Modern utilitarians have interpreted this to mean mainly economic efficiency.[220] The role of property law in such interpretation is to facilitate wealth-maximizing transactions.[221]

For that reason, in deciding "whether the law should allow a magazine to sell its subscriber list to another magazine without obtaining the subscribers' consent,"[222] Richard Posner looks only to transaction-cost considerations. Posner concludes that the property right in personal information should be assigned away from the individual because to the seller "the cost of obtaining the subscriber approval would be high relative to the value of the list."[223] On the other hand, the cost to the subscriber would be low since the disclosed information is trivial; therefore, the purchaser of the list would not be able to "use it to impose substantial costs on the subscribers."[224]

This view is vulnerable on both empirical and theoretical grounds. Empirical studies do not seem to support the assumption that the assignment of property rights in personal information to its collectors reduces transaction costs. As pointed out by Kenneth C. Laudon, those

---

[218] *See infra* notes 289-94 and accompanying text (discussing whether collector should have *any* property rights in acquired data).

[219] *See generally* BENTHAM, *supra* note 212.

[220] *See* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 36-39, 271-89 (4th ed. 1988) [hereinafter POSNER, ECONOMIC ANALYSIS]; RICHARD A. POSNER, THE PROBLEMS OF JURISPRUDENCE 357 (1990) [hereinafter POSNER, JURISPRUDENCE] (applying economic approach to law and legal doctrine). *See generally* Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. 347-48 (1967) (developing theory of property rights and externalities, including costs and benefits).

[221] *See* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243, 1244-45 (1968) (arguing that rational actors seek to maximize their wealth when they covet common property as their own).

[222] Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 398 (1978).

[223] *Id.*

[224] *Id.* at 398-99.

who advocate maintaining the *status quo* for the sake of efficiency "are ignorant of the enormous cost of the existing set of arrangements,"[225] under which individuals are bombarded by calls, e-mails, and mailings that they do not wish to receive.

It has been estimated that telemarketers make eighteen million calls a day,[226] the vast majority of which are unsuccessful.[227] Each year, one hundred million trees are cut down in the United States to produce 4.5 million tons of junk mail; 44% of it goes straight to the waste dumps unopened and unread.[228]

Studies have shown that, frustrated with inadequate laws and practices, individuals spend inordinate amounts of time and money trying to protect themselves from unwanted intrusion. These costs constitute a *privacy toll* and are associated with stopping spam, junk mail, and telemarketing calls, avoiding identity theft,[229] and protecting privacy on the Internet.[230] A privacy-sensitive family could spend between $200

---

[225] Laudon, *supra* note 13, at 102-03 (reporting that out of 14.5 billion catalogues distributed to homes in 1994, 75% were tossed out within five seconds of receipt).

[226] Liz Crenshaw, *Telemarketers & Direct Mail*, NBC4.COM, *available at* http://www.nbc4.com/frequentlyaskedforarchive/1165499/detail.html (last visited Mar. 1, 2003).

[227] Laudon, *supra* note 13, at 103.

[228] *See Native Forest Guide*, *supra* note 8.

[229] *See Identity-Theft Complaints Almost Double in 2002*, *at* http://www.cnn.com/2003/TECH/ptech/01/22/identity.theft.ap/index.html (Jan. 23, 2003) (reporting that, according to Justice Department, up to 700,000 people in United States may be victimized by identity bandits each year). The FTC has reported that the number of identity theft complaints rose from about 86,000 in 2001 to about 162,000 in 2002. Of last year's incidents, 42% involved credit card fraud. Other major categories involved fraudulent bank and cell phone accounts. According to the FTC, it costs an average victim more than $1,000 in expenses to cope with the damage to her accounts and reputation. *Id.*

[230] Elements of the Privacy Toll:

Identity Theft			
	Credit Watch	$39.95 a year for two adults	$79.90
	Credit Reports	$8.50 a year for two adults at two credit bureaus	$34.00
	(There are three major credit bureaus. These services will cover all three.)		
Telemarketing Avoidance			
	Caller ID with Name	$7.50 per month	$90.00
	Unlisted Number	$1.50 per month	$18.00

and $300 and many hours annually to protect their privacy.[231] Consumers, businesses, and the public at large pay the privacy toll.[232] In a recent report to Congress, the FTC estimated that online retail sales lost due to privacy concerns may be worth as much as $18 billion.[233]

In addition to the empirical evidence disclosing the losses resulting from the current allocation of property rights in personal information, economists have argued that the current property regime is inefficient by

Internet Privacy			
	Anonymization Service	$50 per year	$50.00
Junk Mail			
	Opting out	12/year @ $.50 per opt-out	$6.00
	Total Annual Costs		$277.90
Time Losses			
	Spam download time		5 hours/year
	Spam deletion time		2 hours/year
Intangible and Unmeasured Costs			
	Higher credit costs due to ID theft		
	Costs incurred directly by ID theft victims (hundreds or thousands of dollars per victim)		
	Disruptions and aggravation from unwanted telemarketing calls		
	Consumer losses due to telemarketing fraud that rely on targeted marketing data		
	Internet service outages and delays due to spam (losses to consumers and to businesses)		
	Internet costs due to capacity necessary to support spam (costs to ISPs, users, and others)		

Gellman, *supra* note 29.

[231] *See id.*

[232] *Id.* (noting that people will not purchase items on Internet and otherwise when they fear that their personal information may be misused).

[233] *See* Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* 2 (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited Mar. 1, 2003); *see also* Gellman, *supra* note 29 (pointing out that consumers routinely abandon shopping carts on websites because of demands for too much personal information).

its very design since it generates externalities.[234] In this context, externalities mean that social costs (economic as well as non-economic) associated with the accumulation and trading of personal information are not fully borne by primary and secondary collectors. Instead, part of the cost is imposed on individuals whose privacy is invaded, and another part on society in general.[235] The "subsidy" enjoyed by collectors encourages wasteful behavior — companies over-invest in reaching consumers who do not wish to hear from them and under-invest in technology that would permit them to satisfy individual privacy preferences.[236]

Proponents of the law and economics theory often argue that "restrictions on the free flow of information in the name of privacy are generally not social wealth maximizing, because they inhibit decisionmaking, increase transaction costs, and encourage fraud."[237] They maintain that the more information about an individual is available, the more difficult it is for people to lie about themselves, and the cheaper it is for their counterparties to evaluate the risks associated with dealing with them.[238]

The efficiency of this regime, however, is less than obvious. In the real world, information about an individual is never absolutely complete or accurate.[239] It is also never objective in the sense that the very method of its selection (what facts are relevant) reflects certain ideology as well as

---

[234] Laudon, *supra* note 13, at 103 (criticizing Posner for failure "to account for the negative information externalities inherent in the new information age").

[235] *Id.* at 99 (citing "regulatory agencies, congressional hearings, federally funded study groups, and a small industry of privacy experts" as examples of expenditures imposed on society at large).

[236] *See* Schwartz, *supra* note 106, at 833; *see also* Ian Ayres & Matthew Funk, *Marketing Privacy*, 20 YALE J. ON REG. 77, 87 (2003) (suggesting that telemarketers create externalities by ignoring costs they impose on consumers and other telemarketers).

[237] Murphy, *supra* note 16, at 2382 (summarizing principal arguments of law and economics scholars); *see also* Posner, *supra* note 222, at 397-400 (arguing that privacy claims often reflect attempts of plaintiffs to perpetrate fraud by maintaining public image they do not deserve); George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 632-33 (1980) ("The more costly the acquisition of knowledge, the more expensive it becomes to enter into transactions with new parties. We should expect less mobility of laborers, creditors, etc., and some increase in the dispersion of prices."). *See generally* Symposium, *The Law and Economics of Privacy*, 9 J. LEGAL STUD. 621 (1980).

[238] *See* Stigler, *supra* note 237, at 628-33.

[239] *See Privacy and Consumer Profiling*, *available at* http://www.epic.org/privacy/profiling/#introduction#introduction (last updated Feb. 3, 2003) (reporting serious problems with accuracy of profiling data). For instance, in April 2001, former Privacy Foundation CTO Richard Smith requested his ChoicePoint dossier and concluded that the file contained "more misinformation than correct information." *Id.*

biases and prejudices. If an individual has no control over dissemination of her personal information, does not know what facts may determine a counterparty's decision, and has no ability to correct errors in her record, that by itself may lead to economically inefficient behavior by all parties to a transaction. Furthermore, many potential participants may be deterred from entering the market much in the same way many able candidates are already deterred from entering political life by fear of unlimited exposure and unwanted publicity.[240] As a result, the legal regime that, in the name of efficiency, imposes the burden of protecting privacy on individuals is likely, in the long run, to be inefficient.

Even if this law and economics analysis were correct, the collective lack of privacy may still be inefficient.[241] The unlimited dissemination of personal information restricts individuals' ability to present themselves differently to different people, which, apart from any fraud, is important for establishing new relationships as well as for personal change and growth.[242] Unavoidable clerical errors[243] put at risk the legitimate interest people have in their reputations.[244] This interest is not only personal in nature — it is also an investment, similar to the investment a corporation makes in its good will; therefore, on a societal scale, damage to personal reputations results in an economic loss to the society as a whole. These costs, shifted from specific market participants to the public at large are, however, not accounted for in the current property regime.

---

[240] *See, e.g.*, Gerald F. Seb, *Powell's Exit Sparks Debate Over Shape of Politics in America*, WALL ST. J., Nov. 9, 1995, at A1 (stating that Powell's reluctance to enter race is partly due to concern for family's privacy).

[241] *See* Gellman, *supra* note 29, § 3.F.3 (arguing that greater use of personal information for enhancement of private sector marketing activities has significant slippery slope problem, and that targeted marketing might be greatly enhanced if personal income tax records or medical records were freely available to marketers). However, it is clear that most Americans would not tolerate this type of activity. *Id.*

[242] *See* Graham, *supra* note 97, at 1404.

[243] Stigler concedes that "[e]rror is of course unavoidable" but argues that "there are substantial incentives for information agencies to keep the error in reasonable bounds. The rejection of a sound debtor or acceptance of a deadbeat are clearly costly to a merchant." Stigler, *supra* note 237, at 626. In a law and economics dream world, with complete information on all sides of a transaction and zero transaction costs, this argument would be true. However, in the real world, neither merchants nor customers learn about clerical errors as soon as they happen. Thus, the cost of such errors may factor into a price differential. The value of an error to a customer may significantly exceed its value to a merchant, i.e., the merchant will have no incentive to correct it. In theory, a customer could go to a different merchant, the one that produces fewer errors. Yet, in a world in which individuals have no control over their personal information, how will the customer compare which merchant keeps the most accurate files?

[244] *See* Murphy, *supra* note 16, at 2385 (arguing that reputations are valuable personal assets).

A standard remedy[245] to the externalities problem is "internalizing" the costs, i.e., reallocating property rights[246] or creating other incentives that would spread the costs of producing a benefit to all parties involved.[247] Carl Shapiro and Hal R. Varian, who view privacy as an externality problem, explain:

> I may be adversely affected by the way people use information about me and there may be no way that I can easily convey my preferences to these parties. The solution to this externality problem is to assign property rights in information about individuals to those individuals. They can then contract with other parties, such as direct mail distributors, about how they might use the information.[248]

To summarize my arguments, both the empirical evidence and theoretical considerations of economists support the view that the current property regime with respect to personal information is inefficient and should be revised. Even if, as a result of that revision, transaction costs rise, they will rise only as far as necessary to pay for the cost of invading privacy.[249] Additionally, the increased cost would discourage "the obnoxious use of information that could undermine the foundations of a free society if left unchecked."[250] As Kenneth C. Laudon has pointed out, "[t]here should be no free lunch when it comes to invading privacy."[251]

---

[245] Some economists have argued that it may be in the interests of society as a whole not to fight externalities if doing so would discourage some socially valuable activity. For instance, taxing a manufacturer for pollution that damages a neighboring property is inefficient compared to simply removing or compensating the owners of the damaged properties. *See, e.g.*, R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 2-8 (1960) (comparing two regimes — one where business is liable for damage it causes, and the other where injured party is held responsible for damage to its property). However, as Kenneth C. Laudon correctly points out, "[t]his argument makes little sense when applied to either privacy invasion or to environmental pollution on a massive scale. How do you move away from privacy invasion and avoid experiencing the costs?" Laudon, *supra* note 13, at 103.

[246] *See* Demsetz, *supra* note 220, at 352 (noting that internalizing usually involves change in property rights).

[247] *See id.* at 347-57.

[248] Carl Shapiro & Hal R. Varian, *U.S. Government Information Policy, available at* http://www.sims.berkeley.edu/~hal/Papers/policy/policy.html (July 30, 1997) ("The right way to think about privacy, in our opinion, is that it is an externality problem.").

[249] Laudon, *supra* note 13, at 103.

[250] *Id.*

[251] *Id.*

Moreover, economic costs and benefits represent only one, albeit important, consideration in evaluating the social benefits of the current allocation of property rights in personal information.[252] The legal system protects and advances many values and concerns, both economic and non-economic.[253] Certain values in our society are considered so important that distribution of property rights contradicting those values would be viewed as impermissible even if it were economically efficient.

> The nineteenth century arguments about the abolition of slavery did not in the slightest depend upon the relationship of slavery to material output. The abolitionist of that or any other era regards it as immaterial that the liberation of the slaves might reduce transaction costs or increase the gross national product.... This position... rests upon the... belief that each person has a natural right to own his person as a condition of birth and as part of the recognition of his common humanity. Liberty, freedom and personal autonomy are ideals of the law, and they cannot be reduced to simple efficiency considerations, however important efficiency may be in its own right.[254]

Privacy is certainly perceived as one of such values.[255] As one poll showed, 79% of the public believe that, if the Framers of the Declaration of Independence were rewriting that document today, they would add privacy to the trinity of life, liberty, and the pursuit of happiness.[256] Privacy serves numerous non-economic functions, including freedom and liberty, essential for a democratic society.[257] For that reason, the Constitution protects privacy rights of individuals against the federal and state governments. In recent years, however, exchange of personal data between the public and private sectors has significantly expanded,

---

[252] *See* Gellman, *supra* note 29 ("Arguments that focus solely on monetary costs and benefits miss a major part of the privacy debate.").

[253] Richard Epstein, *Privacy, Property Rights, and Misrepresentations*, 12 GA. L. REV. 455, 456 (1978).

[254] *Id.* at 456-57.

[255] In a recent poll, participants ranked privacy just behind the freedom of speech and ahead of the freedom of religion and the right to vote as the most important American right. *See* Alan F. Westin, *Intrusions. Privacy Trade-Offs in a Free Society*, PUBLIC PERSPECTIVE (Nov./Dec. 2000), *available at* http://216.239.51.100/search?q=cache:zhMy9VKOf_QC:www.ropercenter.uconn.edu/pubper/pdf/pp116a.pdf+harris+poll+1990+79%25+declaration+independence&hl=en.

[256] *See EPIC Public Opinion on Privacy*, *supra* note 26 (reporting results of 1990 Harris Poll).

[257] *See* Laudon, *supra* note 13, at 103 (criticizing Posner for failing to recognize non-economic value of privacy).

thus weakening the constitutional protection against the government.[258] For example, privacy advocates have noted the increasing flow of consumer data from private sector databanks to law enforcement agencies:

> Big Brother isn't gone. He's just been outsourced. After surveillance scandals in the 1960s and 1970s, the Federal Bureau of Investigation and other federal law-enforcement authorities curbed their file-keeping on U.S. citizens. But in the past several years, the FBI, the Internal Revenue Service and other agencies have started buying troves of personal data from the private sector.... Do Americans want the records of their purchases, activities, and interests available online for casual use by the FBI and other law enforcement agencies without any requirement for a court order or search warrant?[259]

Legal ownership of personal information would guarantee individuals the most effective control over their privacy. Each individual would be able to decide on her own how much personal information she is willing to share in exchange for a monetary or non-monetary gain. For utilitarians, concerned with the most complete satisfaction of preferences of as many members of the society as possible, that solution should be completely acceptable.

As for the preferences themselves, numerous polls and studies have consistently demonstrated that people are concerned about their inability to control personal information[260] and that they would like to change the

---

[258] *See, e.g.*, Gellman, *supra* note 29 (expressing concern that, as "the line between the public and private sectors regarding personal data grows ever less clear, the protections against government weaken").

[259] Glenn R. Simpson, *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask Choicepoint*, WALL ST. J., Apr. 13, 2001, at A1 (describing how private sector companies specialize in collecting and compiling personal information from multiple sources, including credit bureaus, marketers and public records, and raising concern that this information is sold to dozens of government agencies).

[260] *See, e.g., EPIC Public Opinion on Privacy*, *supra* note 26 (discussing August 2001 Yankee Group survey of 3000 online consumers that found that 83% of respondents are somewhat or very concerned about privacy on Internet); *see also* Humphrey Taylor, *Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits*, HARRIS INTERACTIVE, *at* http://www.harrisinteractive.com/harris_poll/index.asp?PID=365 (March 19, 2003) (reporting that 79% of participants of most recent Harris poll believe that it is extremely important to be in control of who can get personal information); Marlon Manuel, *What's for Sale? You. Atlantans Feel Victimized by Companies that Require Personal Data, Profit From It*, ATLANTA J. CONST., Mar. 24, 2002, at 1A (discussing poll of 2,400 adults in 15 metro Atlanta counties conducted by Marketing Workshop finding that 65% of participants view selling and buying personal information as invasion of privacy); *IBM-Harris Multi-National Consumer Privacy Survey*, PRIVACY & AM.

current law, which has proven incapable of protecting their privacy.[261] In fact, prior to the events of September 11, many Americans singled out "loss of personal privacy" as the top concern for the twenty-first century.[262] Therefore, changing the current property regime governing rights in personal information to give priority to the individual is warranted under the utilitarian theory by (i) the objective increase of economic and non-economic benefits to the public in general and (ii) the subjective satisfaction of preferences expressed by the significant majority of the society.

C. Personality Theory

The personality theory of property takes its origin in Hegel's philosophy.[263] The underlying premise of the personality theory is that

---

BUS. (Ctr. for Soc. & Legal Research), Jan. 2000, at 1 (discussing December 1999 IBM-Harris Multi-National Consumer Privacy Survey finding that in United States 94% of consumers think that personal information is vulnerable to misuse, compared to 78% in United Kingdom and 72% in Germany).

[261] *See EPIC Public Opinion on Privacy*, *supra* note 26 (reporting that, based on numerous polls, Americans consider current self-regulatory framework insufficient to protect privacy). A February 2003 Harris Poll showed that 53% of all adults disagree that "existing laws and organizational practices provide a reasonable level of protection for consumer privacy today." This is an increase of fifteen points from 38% in 1999. *See* Taylor, *supra* note 260 (analyzing results of most recent Harris poll). A June 2001 Gallup poll indicated that two-thirds of respondents favored new federal legislation to protect privacy online. *See Majority of E-mail Users Express Concern about Internet Privacy*, GALLUP POLL NEWS SERVICE, *available at* http://www.gallup.com/subscription/?m=f&c_id=10732 (6/28/2001). A March 2000 BusinessWeek/Harris Poll found that 57% of respondents favored laws that would regulate how personal information is used. *See Business Week/Harris Poll: A Growing Threat*, BUS. WEEK ON LINE *at* http://www.businessweek.com/2000/00_12/b3673010.htm (Mar. 20, 2000). In that same poll, only 15% supported self-regulation. *Id.*; *see also* Reidenberg, *supra* note 16, at 884 (reporting that at public referendum on privacy citizens of North Dakota repealed recent state law that weakened privacy protection and restored opt-in rule for financial information by vote of 72% to 28%).

[262] EPIC ALERT, *at* http://www.epic.org/alert/EPIC_Alert_6.15.html (Sept. 23, 1999). A 1999 Wall Street Journal/NBC News poll of 2,025 adults by phone found that the loss of personal privacy was the number one concern of Americans. *Id.* In that pre-September 11 poll, 29% of respondents reported that the "loss of personal privacy" was a top concern. *Id.* Privacy outranked other high-profile concerns such as overpopulation (23%), terrorist acts (23%), racial tensions (17%), world war (16%), and global warming (14%). *Id.*

[263] In one of the most quoted paragraphs of the PHILOSOPHY OF RIGHT, Hegel states:

> A person has as his substantive end the right of putting his will into any and every thing and thereby making it his, because it has no such end in itself and derives its destiny and soul from his will. This is the absolute right of appropriation which man has over all "things."

HEGEL, *supra* note 213, ¶ 44.

to achieve proper self-development — to be a person — an individual needs some control over resources in the external environment.[264] That control is most commonly assured through the system of property rights — "property is the first embodiment of freedom and so is in itself a substantive end."[265]

In the last couple of decades, Hegel's theory of "property for personhood" has received interesting development in the work of Margaret Jane Radin.[266] She views ownership as a relationship between an individual and an object and distinguishes two types of property — "property that is bound up with a person and property that is held purely instrumentally — personal property and fungible property, respectively."[267]

Property is bound with an individual if its loss can be remedied only by the return of the lost object.[268] Conversely, property is held only for instrumental reasons if it is "perfectly replaceable with other goods of equal market value."[269] For example, "if a wedding ring is stolen from a jeweler, insurance proceeds can reimburse the jeweler, but if a wedding ring is stolen from a loving wearer, the price of a replacement will not restore the status quo — perhaps no amount of money can do so."[270]

Accordingly, Radin argues that the two types of property should be treated differently, and personal property, the "property for personhood," should receive stronger legal protection because it is essential to the individual's "sense of continuity of self over time."[271] Therefore, in a property dispute between two rival claimants, special, and often decisive, consideration should be given to the relationship of

---

[264] Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957, 957 (1982) (discussing Hegel's philosophy).

[265] HEGEL, *supra* note 213, ¶ 45.

[266] *See generally* Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849 (1987) [hereinafter Radin, *Market-Inalienability*] (exploring significance of market-inalienability and its justifications); Radin, *supra* note 264 (exploring relationship between one's property and personhood); Margaret Jane Radin, *Regulation of Computing and Information Technology: Property Evolving in Cyberspace*, 15 J.L. & COM. 509 (1996) [hereinafter Radin, *Property Evolving in Cyberspace*] (discussing scope of copyright protection in cyberspace); Margaret Jane Radin, *Symposium on the Renaissance of Pragmatism in American Legal Thought: The Pragmatist and the Feminist*, 63 S. CAL. L. REV. 1699 (1990) [hereinafter Radin, *Renaissance of Pragmatism*] (exploring link between pragmatism and feminism with Hegel).

[267] Radin, *supra* note 264, at 960.

[268] *Id.* at 959 ("An object is closely related to one's personhood if its loss causes pain that cannot be relieved by the object's replacement.").

[269] *Id.* at 960.

[270] *Id.* at 959.

[271] *Id.* at 1004.

each claimant to the property in question.[272] For example, "if some object were so bound up with me that I would cease to be 'myself' if it were taken, then a government that must respect persons ought not to take it."[273]

Radin's theory provides strong support for a default rule that would grant initial entitlement in personal information to individuals. In fact, what can be more essential to an individual's "sense of continuity of self over time"[274] than personal information — one's name, personal attributes, and the record of interests, preferences, past acts and choices? Conversely, the same personal information for a collector is just a commodity easily replaceable with money, as that routinely occurs in the course of a transfer from one collector to another.

Although the personality theory supports the priority of the individual's right in personal property, it may also require that the right remain inalienable. Radin has consistently argued that things necessary for human flourishing should not be commodified.[275] On the other hand, she recognizes that "market-inalienabilities are unjust when they are too harmful to personhood in our non-ideal world."[276] To mediate this kind of injustice, Radin has advocated incomplete commodification of things important to personhood. She explains,

> In the non-ideal world we do live in, market-inalienability must be judged against a background of unequal power. In that world it may sometimes be better to commodify incompletely than not to commodify at all. Market-inalienability may be ideally justified in light of an appropriate conception of human flourishing, and yet sometimes be unjustifiable because of our non-ideal circumstances.[277]

Whether we like it or not, in our non-ideal world, personal information has already been commodified. Benefits of that commodification seem to be enjoyed by all market participants, save individuals, which is both unjust and harmful to their personhood. In addition, consensual release of personal information is important to society as a whole. Allowing individuals to decide for themselves whether, and on what terms, they would be willing to release

---

[272] *See id.*

[273] *Id.* at 1005.

[274] *Id.* at 1004.

[275] *See generally* Radin, *Market Inalienability*, *supra* note 266.

[276] *Id.* at 1937.

[277] *Id.* at 1903.

information about themselves to commercial enterprises would promote individuals' sense of control over their lives, which is essential to "human flourishing." I will discuss later in this Article how individual rights should be balanced against the rights and interests of other members of the community (and, in that sense, only partially commodified). However, the fact that personal information is important to personhood should not make it inalienable.

One might argue that assigning individuals property rights in their personal information would transform "property for personhood" into tangible property, thus eliminating the individual's arguable moral advantage over collectors. That is not true. The fact that a person may decide to sell or pawn her wedding ring does not automatically strip the wedding ring of its special emotional value.

State insolvency laws routinely allow individual bankrupts to keep their family homes, photo albums, letters, and diaries.[278] And if the exemption for homes may be partly explained under the theory of a "fresh start," letters and pictures are clearly exempted because of their status as "property for personhood," which does not mean that their owner may not choose at some point to part with them. These examples show that the law already offers special treatment to "property for personhood" even though it is understood that that property is not inalienable in the hands of the owner. Personal information should enjoy similar treatment, and "a government that must respect persons"[279] ought to give property rights of individuals priority over property rights of collectors.

D. Blackmail Argument

In addition to the theories outlined above, the following paradox from the area of criminal law provides logical and moral support to the intuitive sense that individuals should have preferential rights in their personal information. That paradox is blackmail, and over the years it has attracted the attention of numerous legal scholars who tried to explain: why is blackmail illegal?[280]

---

[278] *See, e.g.*, Lee v. Mercantile First Nat'l Bank, 765 S.W.2d 17 (Ark. Ct. App. 1989) (allowing debtors to keep residential property due to homestead exemption but ordering sale of commercial property to satisfy debt).

[279] Radin, *supra* note 264, at 1005.

[280] *See, e.g.*, JAMES BOYLE, SHAMANS, SOFTWARE AND SPLEENS 61 (Harvard University Press 1996) (noting that each generation of scholars comes to blackmail puzzle, "as to some muddy and treacherous test track, to try out their new theories. The test is an apparently simple one: to find out whether their approach will answer the question 'why is blackmail

The essence of the paradox is that the crime of blackmail consists of two elements that, taken separately, are perfectly legal — a demand for payment (or other benefit) and a threat to expose some personal information.[281] Why then does a combination of two non-criminal elements result in a crime? Undeniably, when the concealed information concerns an illegal act, the society has a strong interest in forbidding private arrangements that jeopardize punishment and prevention of illegal behavior. But why should the society criminalize, effectively, a sale of legal and merely embarrassing personal information?

Take the paradigmatic case of marital infidelity. If the blackmailer has a right, but not a duty, to tell the victim's wife about the victim's infidelities, why cannot she agree to forego that right in exchange for a payment? This result seems abnormal because usually when a person has a right to do or not do something, that means she is free to agree not to exercise that right in exchange for some remuneration.[282] Various theories of blackmail seek to explain that abnormality.[283] They can be roughly grouped into: (i) moral arguments; (ii) economic-efficiency arguments; and (iii) consequential arguments.

The essence of the moral argument is that there is something deeply immoral (even if not illegal) either in the threat to expose the victim's secret, or in the exchange of silence for money.[284] Economic theories of

---

illegal?'"); *see also* James Lindgren, *Unraveling the Paradox of Blackmail*, 84 COLUM. L. REV. 670 (1984) (offering classification of theories explaining wrongfulness of blackmail). *See generally* LEO KATZ, ILL-GOTTEN GAINS 140-45 (1996) (analyzing various theories of blackmail, including those by Epstein, Nozick, Feinberg, and Lindgren); Symposium, *Blackmail: Instead of a Preface*, 141 U. PA. L. REV. 1565 (1993).

[281] *See, e.g.*, KATZ, *supra* note 280, at 133 (noting that in canonical blackmail scenario, blackmailer has right both to reveal victim's infidelities to victim's wife and to ask victim for money; "[y]et when he combines these various innocent actions, paradoxically a crime results — blackmail.").

[282] *Id.*

[283] For what James Boyle called "[b]y far the best survey" of the field of blackmail, see James Lindgren, *supra* note 280, at 680-701.

[284] *See, e.g.*, ARTHUR L. GOODHART, ESSAYS IN JURISPRUDENCE AND THE COMMON LAW 179 (1937) (distinguishing between "moral liberties" promoted by society and "immoral liberties" merely tolerated by it, and concluding that surrender of an immoral liberty, like liberty to reveal damaging secret, may not be valid consideration for contract); ROBERT NOZICK, ANARCHY, STATE, AND UTOPIA 85 (Basic Books, Inc. 1974) (condemning blackmail as "unproductive activity" in which victim systematically gains no benefit — victims would be better off "if the blackmailer did not exist at all, and so wasn't threatening them [and] they would be no worse off if the exchange were known to be absolutely impossible"); Wendy J. Gordon, *The Force of Blackmail's Central Case*, 141 U. PA. L. REV. 1741, 1758 (1993) (seeing wrongfulness of blackmail in that "[o]ne person deliberately seeks to harm another to serve her own ends — to exact money or other advantage — and does so in a context where she has no conceivable justification for her act."); KATZ, *supra* note 280,

blackmail are concerned primarily with the inefficiency of blackmail as a system of private enforcement of law where the violator of a legal rule pays the blackmailer a sum up to the amount of what the punishment would be worth to that violator.[285] Finally, consequential arguments put emphasis not on the wrongfulness or inefficiency of blackmail itself but rather on the negative impact it could have on the society if it were legal.[286]

All these arguments explain why the society may find blackmail objectionable — there is no common benefit in immoral, economically inefficient, or potentially dangerous activity. However, there is a long way to go between finding an activity objectionable and criminalizing it. The same moral, economic-efficiency, and consequential arguments can be used against, say, marital infidelity, but most states no longer criminalize adultery,[287] leaving it to the sphere of private relations, like

---

at 158-62 (seeing wrongfulness of blackmail in blackmailer's ability to force victim to choose between two evils — theft (or another criminal encroachment) and revealing victim's secret); Lindgren, *supra* note 280, at 702 (finding blackmail morally objectionable because blackmailer exploits leverage which belongs to someone else, namely, to third party from whom victim is trying to hide secret).

[285] *See, e.g.*, William Landis & Richard Posner, *The Private Enforcement of Law*, 4 J. LEGAL STUD. 1, 42 (1975) (arguing that blackmail is inefficient both when "secret" discovered by blackmailer involves illegal act, as well as when there is nothing illegal about that "secret"). In the former scenario,

> [o]verenforcement of the law would result if the blackmailer were able to extract the full fine from the offenders. . . . Alternatively, the blackmailer might sell his incriminating information to the offender for a price lower than the statutory cost of punishment to the criminal, which would reduce the effective cost of punishment to the criminal below the level set by legislature.

Id. As for the latter case, Landis and Posner argue that, if a society has not prohibited certain behavior that means the society decided not to expend social resources on trying to discover and punish it. *Id.* That social choice would be undermined if blackmailers were allowed to pursue and punish people engaged in a legal activity. *Id.* at 43.

[286] *See, e.g.*, Richard Epstein, *Blackmail, Inc.*, 50 U. CHI. L. REV. 553, 564 (1983) (arguing that blackmail should be outlawed because blackmailer aids victim in concealing some damaging information (i.e., facilitates fraud on third party or public at large)). In addition, Epstein argues that blackmail creates strong incentives for a victim to satisfy the blackmailer's monetary demands: "[d]o we believe that [the victim] would never resort to fraud or theft given this kind of pressure, when the very nature of the transaction cuts off his access to the usual financial sources, such as banks or friends, who would want to know the purpose of the loan?" *Id.*; *see also* Jeffrie Murphy, *Blackmail: A Preliminary Inquiry*, 63 MONIST 156, 164-66 (1980) (expressing concern that without law of blackmail there would be incentives for invasions of privacy).

[287] *See, e.g.*, Martin J. Siegel, *For Better or For Worse: Adultery, Crime & the Constitution*, 30 J. FAM. L. 45, 49-54 (1991-92) (discussing efforts to decriminalize adultery and pointing out that majority of states have now decriminalized adultery, and remaining laws are rarely enforced).

any other private imperfection.

Why then criminalize a voluntary transfer of information from a blackmailer to the victim, or — using the terms adopted in this paper — from a collector to the individual? After all, if the same collector/blackmailer chose to offer the information to a tabloid instead of the individual/victim, there would be nothing legally objectionable. The collector/blackmailer could use identical language in dealing with the individual and the tabloid: "I have some valuable compromising information regarding X. If you want, you can have it for $1000. If not, I am selling it to *The New York Post*." The individual/victim is even likely to be happy that he has received the "right of first refusal" and thus avoided what he perceives as a more serious harm. So why is it legal to sell personal information to a third party but not to the individual himself?

The answer to all these questions lies, in my view, in the respective rights of the collector/blackmailer and the individual/victim to the discovered personal information. They may be compared to the relationship of "bailors" and "bailees." In the situation of involuntary bailment[288] — lost and found property — a finder has rights against the whole world except for the true owner.[289] The finder may sell or pledge the ring she found to a third party; if she later loses the ring, she will have the right to recover it from a subsequent finder.[290] However, she may not sell the ring to the true owner because the finder's property right is inferior to the right of the owner. The same is true in the situation of a voluntary bailment.[291] In both instances, if a bailee conditioned the return of property to its lawful owner on remuneration (other than pursuant to a prior agreement), she would be guilty of

---

[288] Possession by a finder is often characterized as involuntary bailment. *See* JESSE DUKEMINIER & JAMES KRIER, PROPERTY 105-06 n.2 (5th ed. 2002) (comparing rights of owners, voluntary and involuntary bailees, and subsequent possessors).

[289] *See, e.g.*, Armory v. Delamirie, K.B. 1722, 1 Strange 505 (holding that "the finder of a jewel, though he does not by such finding acquire an absolute property or ownership, yet he has such a property as will enable him to keep it against all but the rightful owner"); *see also* RAY A. BROWN, THE LAW OF PERSONAL PROPERTY 26 (Walter B. Raushenbush ed., 3d ed. 1975) (explaining that "the title of a finder is good as against the whole world but the true owner").

[290] DUKEMINIER & KRIER, *supra* note 288, at 104.

[291] Voluntary bailment may, in addition, impose on the bailee higher obligations of care with respect to the entrusted property, although the modern trend is to apply uniform standard of "reasonable care under the circumstances" across the board. *See* Richard H. Helmholz, *Bailment Theories and the Liabilities of Bailees: The Elusive Uniform Standard of Reasonable Care*, 41 KAN. L. REV. 97, 99 (1992).

theft.[292]

A similar principle applies to the rights of a collector and the individual whose personal information has been either discovered by a collector (analogously to involuntary bailment) or entrusted by the individual (analogously to voluntary bailment). The possession of this information may give a collector some property rights but they are subordinate to the rights of the individual. A different default rule, one that assigns priority either to a collector or to the public at large, would lead to an unappealing implication that the blackmailer who collected personal information about her victim should be allowed to make the victim pay for it.[293] The blackmail analogy, together with principal theories of property, demonstrates that, although a collector may have rights in individuals' personal information, these rights should be subordinate to the rights of the individuals.

VI. BALANCING INTERESTS OF THE INDIVIDUAL, SOCIETY, AND COLLECTORS

The fact that individuals should have a prior property right in their personal information does not mean that this right should be absolute or exclusive. Personal information, like information in general, differs from traditional forms of property. It can be possessed by more than one person,[294] it is not destroyed in the act of consumption, it does not lose value when used and, conversely, may lose value when it is not used and becomes obsolete.[295]

Personal information has certain similarities with intellectual property, in particular copyright.[296] One can look at people as the authors of their

---

[292] *See, e.g.*, MODEL PENAL CODE § 223.5 (defining theft of property lost, mislaid, or delivered by mistake).

[293] This conclusion made Posner, for instance, insert a footnote questioning his own argument that personal information about an individual should be public:

> If I am correct that the facts about a person should be in the public domain so that those who have to decide whether to initiate (or continue) social or business relations with the person will be able to do so on full information, does it not follow that the Nosey Parker should be allowed to sell back the information he obtains to the individual?

Posner, *supra* note 222, at 421 n.57.

[294] *See* Douglas G. Baird, *Common Law Intellectual Property and the Legacy of International News Service v. Associated Press*, 50 U. CHI. L. REV. 411, 413 (1983) ("It is the nature of... any... tangible property that possession by one person precludes possession by anyone else.... Many people, however, can use the same piece of information.").

[295] *See* Mell, *supra* note 16, at 69 (noting that in certain respects personal information "does not conform to the existing definitions of either personal or intangible property").

[296] Copyright protection serves to assure an author's priority and limited monopoly in a

own lives, generating information as they develop their personalities.[297] In fact, in Europe, personal information is viewed similarly to intellectual property.[298] In the United States, however, copyright protects only the expressive content of the work, not the ideas or facts contained therein.[299] Consequently, personal information is outside the subject matter of American copyright law. There have been suggestions made to broaden the scope of copyright protection to include personal information.[300] This solution would certainly enhance protection of individual privacy. On the other hand, it raises slippery-slope concerns: it could open the door to treating information in general as a copyrightable material and could lead to creating a monopoly on information.[301]

Instead of trying to stretch one or another traditional category to cover personal information, it may be worth recognizing it as a new bundle of rights, which combines elements of traditional property and intellectual property, as well as property and privacy. Due to its special nature, more than one person in the society may have a legitimate interest in personal information. Accordingly, that limits the scope of property rights that ought to be granted to individuals.

---

particular form of expression and is automatically granted to all "original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced or otherwise communicated, either directly or with the aid of a machine or device." 17 U.S.C. § 102(a) (2000).

[297] Solove, *supra* note 99, at 1112.

[298] Angela R. Broughton et al., *International Employment*, 33 INT'L LAW. 291, 292 (1999) (pointing out that, culturally, Europeans see personal data as akin to intellectual property). Broughton explains:

> Europeans believe corporations should not traffic in information without the consent of its owner. To explain Europeans' distrust of free transfers in personal information, some have cited the Nazi government's abuses of personal data to further its aims. Others note that Europeans are bewildered by the U.S. fixation on politicians' sex lives. Europeans, unlike Americans, consider personal information — be it about politicians, employees, or anyone else — private.

Id.

[299] *See, e.g.*, Salinger v. Random House, Inc., 811 F.2d 90, 100 (2d Cir. 1987) (finding that "Salinger has a right to protect the expressive content of his unpublished writings for the term of his copyright," but did not have protection for ideas or facts that were included within).

[300] *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1151-59 (2000) (advocating licensing regime and privacy protection rules analogous to trade secrets law).

[301] *See* Volokh, *supra* note 82, at 1051 ("Before wholeheartedly endorsing the principle that calling certain information 'intellectual property' lets the government restrict speech communicating that information, we should think about the consequences of such an endorsement.").

In her influential article about a computer "persona,"[302] Patricia Mell likens personal information to real property in medieval England and argues that individuals should own it in "fee simple."[303] In Mell's view, the rights of all other interest groups (commercial enterprises, the public, and the government) should be subordinate to those of the individual.[304]

While agreeing in general with Mell's property-based approach, I see the individual's rights with respect to personal information as significantly less absolute. The society has an interest in the free flow of information, and this interest needs to be taken into account. To give individuals an unabridged right in their data would threaten to immobilize it. Moreover, as has been discussed earlier, personal information is not only property, it is also speech, which gives rise to an inherent conflict between the value of privacy to the individual and the value of free speech to the society.[305] Finally, the original collector has a legitimate interest in the personal information it collects in order to run its business and better serve its customers.

To satisfy all those interests, I suggest that the property right of the individual be limited in three respects. The first limitation should be its duration. Normally, property rights do not expire. If I own a piece of property, my devisees or heirs would inherit it, absent any explicit condition or limitation attached to that particular property. One well known exception to this rule is intellectual property.[306] The limited rights of the owner are the result of a trade-off between the needs of authors in protecting their work and the needs of the society in the free flow of ideas.

Conversely, personal rights, including the right to privacy, do expire.[307] The common-law rule is that "the right of privacy dies with the

---

[302] By "persona" Mell means "the various ways by which a person can be identified by personal information about him." Mell, *supra* note 16, at 3.

[303] *Id.* at 76 (arguing that "[t]he persona should be viewed as property, the ultimate 'ownership' or 'fee simple' of which resides in the individual.").

[304] *Id.* ("The rights of any other entity (i.e., any group, class, association or government) that might obtain, access, make use of, or disclose the persona would be subordinate to those of the individual.").

[305] *See* discussion *supra* Part III.

[306] Copyright protection is limited in duration to the life of the author plus 70 years for individuals and the period of 95 years from the first publication or 120 years from creation, whichever expires first, for works made for hire or by employees. 17 U.S.C. § 302(a)-(c) (2000); *see also* Aldon Accessories, Ltd.v. Spiegel, Inc., 738 F.2d 548, 552-53 (2d Cir. 1984). Patent rights generally expire after 20 years. 35 U.S.C. § 154(a)(2) (2000).

[307] *See* MCCARTHY, *supra* note 60, at 9-2; *see also* PROSSER & KEETON ON THE LAW OF TORTS ¶ 117, at 815 (W. Page Keeton ed., 4th ed. 1987).

individual."[308] The only exception to this rule, recognized in approximately one-third of all states,[309] involves the right of publicity.[310] The majority rule that disallows the postmortem right to privacy (other than the right of publicity) is based on the idea that this right protects dignitary and reputational interests, which are inherently personal.[311] Once the subject is dead, the reason for protecting those rights disappears.[312] The right of publicity, on the other hand, is a property right; it protects against infringement of the commercial value attributable to a human identity.[313] Those states that extend the right of publicity beyond the lifetime of the individual usually limit its postmortem duration from as few as ten to as many as one hundred years.[314]

Arguments in favor of protecting personal information fit under the logic of both traditional privacy (based on the notion that individuals should be able to keep their actions, choices, and preferences secret) and the right of publicity (based on the sense that individuals should receive some economic benefit from the sale of their personal information). In most instances, however, personal information has value for the individual, collectors, and the public only during the lifetime of the individual.

Generally speaking, individuals have few reasons to worry about postmortem commercial use (not involving publication) of their personal information, whether it be for marketing purposes, financial risk assessment, or socio-political profiling. By the same token, commercial enterprises should have very little interest in deceased customers. As for the publication, the current law already protects individuals by disallowing non-media entities to use the identities of deceased persons.[315]

---

[308] Fasching v. Kallinger, 510 A.2d 694, 701 (N.J. App. Ct. 1986).

[309] *See* MCCARTHY, *supra* note 60, at 9-44, 9-45 (listing 13 states that have established right of publicity, or at least most aspects of it, by statute, and noting that in another four jurisdictions courts have found that their respective common law recognizes postmortem right of publicity).

[310] *See id.* at 9-3.

[311] *Id.*

[312] *See id.* at 9-3, 9-4.

[313] *See id.* at 9-9 (listing arguments for and against postmortem right of publicity).

[314] *Id.* at 9-54.1, 9-58 (noting that Oklahoma and Indiana statutes have longest postmortem periods for right of publicity and that under Washington law, postmortem duration of life of publicity where person's identity has no commercial value is 10 years).

[315] *See* Nature's Way Prod., Inc. v. Nature-Pharma, Inc., 736 F. Supp. 245, 252-53 (D. Utah 1990) (rejecting so-called "historical information exception" enjoyed by media when claimed by seller of herbal medicines in order to use name of deceased well known author

Finally, the society has to balance the burdens and benefits of the free flow of information, on the one hand, and privacy, on the other. When the individual whose privacy is at issue is dead, the protection of his privacy loses its all important status compared to the need for full and correct historical data. For all these reasons, the interest of an individual in his personal information should not be a fee simple but rather a life estate, which in the end of the individual's lifetime springs to the public domain.

The second limitation on individual property rights is necessary to recognize the legitimate interest of the original collector. In the context of a voluntary transaction with the individual, the original collector should be granted a non-exclusive and unalienable automatic license in the collected personal information. The collector should be allowed to collect and use this information for its own research and marketing purposes. Before transferring personal information to a third party, however, the collector would have to obtain the affirmative consent of the individual.

Concerns have been raised [316] that a law limiting rights of enterprises in respect of customer data already collected by them may amount to a "taking" of private property for public good under the Fifth Amendment.[317] The Supreme Court has recognized that a privacy regulation that substantially interferes with a collector's use of data that he has collected or processed may constitute a "regulatory taking" and require compensation.[318]

A regulatory taking occurs when the government's regulation "denies an owner economically viable use"[319] of his property. If Congress enacted legislation that completely shifted property rights over personal information from collectors to individuals, that legislation might very well constitute a taking. However, legislation that would permit

---

and lecturer on herbal medicine).

[316] *See* Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 207 (1999) (expressing concern that, "[i]f the government prohibits the processing of personal data, it could deny the owner all or most of the 'economically viable use' of that data.").

[317] The Fifth Amendment states: "No person shall... be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation." U.S. CONST. amend. V.

[318] *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1003-04 (1984) (holding that Environmental Protection Agency's use of plaintiff's proprietary research data constituted compensable taking).

[319] *See* Lucas v. S.C. Coastal Council, 505 U.S. 1003, 1016 (1992); *see also* Agins v. City of Tiburon, 447 U.S. 255, 260 (1980); Andrus v. Allard, 444 U.S. 51, 64 (1979).

enterprises to collect, store, and use personal data for any legitimate business purposes, other than its unauthorized transfer, would not deny collectors all or most of the "economically viable use" of that information.

In addition, the Supreme Court does not find a taking when a regulation merely abates "nuisance-like" conduct,[320] because one never has a property right to harm others.[321] Therefore, legislation that, on the one hand, preserves the economic interests of collectors, and on the other, protects individuals against unauthorized dissemination of their personal information, should not violate the Fifth Amendment.

Finally, the third limitation on individual rights in personal information should come in the form of non-exclusive automatic licenses in favor of the society at large.[322] That limitation would allow the government to collect and transfer certain personal information (e.g., for purposes of tax collection, maintaining public records, or law enforcement),[323] subject, of course, to constitutional constraints. It would also allow private, as well as public non-commercial, exchange of personal information by citizens. Lastly, it would permit public media to collect and publish any "newsworthy" personal information without individual consent.[324] In addition, the license in favor of public media

---

[320] Under the current test, the government must show that the power to promulgate the regulation stems from the "background principles of the State's law of property and nuisance." *See Lucas*, 505 U.S. at 1029.

[321] *See* Jan G. Laitos, *The Takings Clause in America's Industrial States After Lucas*, 24 U. TOL. L. REV. 281, 288 (1993) (pointing out that nuisance exception to Takings Clause is consistent with language and intent of Takings Clause because, under nuisance law theory, one does not have property right to harm others).

[322] The rights and limitations pursuant to this license are beyond the scope of this Article.

[323] *Cf.* The Banks and Banking Regulations, 12 C.F.R. § 332.15(a)(7) (2003) (disposing of requirement of customer consent for disclosure of nonpublic personal information:

> (i) To comply with Federal, State, or local laws, rules and other applicable legal requirements;
> (ii) To comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by Federal, State, or local authorities; or
> (iii) To respond to judicial process or government regulatory authorities having jurisdiction over you for examination, compliance, or other purposes as authorized by law.

[324] *See* Finger v. Omni Publ'ns Int'l, Ltd., 566 N.E.2d 141, 145 (N.Y. Ct. App. 1990) (holding that there was relationship between photograph of large family and fertility article and that use of photograph without plaintiff's consent did not violate prohibitions of New York Rights of Privacy); *see also* NIMMER, *supra* note 98, ¶ 16.08, at 16-25 (stating that there exists right of independent discovery, and information "obtained from unprotected or published sources can be freely used independent of underlying property interest").

would authorize transfer of personal information from a third party, other than a commercial collector, to the media (e.g., an interview concerning a public figure) and would protect the media if the information supplied by a third-party collector was obtained by unlawful means.[325]

Current privacy law effectively recognizes all these "carve-outs." For instance, under both constitutional and tort law, media are immune from liability[326] for unauthorized use of personal identity as long as the identity bears a reasonable relation to the news.[327] The term "news" has been interpreted broadly to include all media presentations of information on public issues.[328] Thus, current law affords adequate protection for information that should be disseminated on the basis of its newsworthiness.

In a nutshell, the suggested legal regime would give individuals property rights in their personal information. They would own this information during their lifetime, subject to a (i) non-exclusive automatic inalienable license to the original collector and (ii) limited non-exclusive automatic license to the general public. This way, friends of, say, Robert Bork would be free to talk, and newspapers free to write, about movies he watches or books he reads, but a video- or bookstore would not be free to reveal his customer record even in the heat of his nomination campaign.

---

[325] *See* Bartnicki v. Vopper, 532 U.S. 514, 535 (2001) (reasoning that right to privacy fails when weighed against media's right to publish matters of public interest despite private nature, and illegal acquisition, of information).

[326] Eastwood v. Super. Ct. of Los Angeles County, 149 Cal. App. 3d 409, 421 (Cal. Ct. App. 1983) ("Publication of matters in the public interest, which rests on the right of the public to know, and the freedom of the press to tell it, cannot ordinarily be actionable.").

[327] *See, e.g.*, Barrows v. Rozansky, 489 N.Y.S.2d 481, 485 (N.Y. 1985) (holding that "to be privileged such use must be legitimately related to the informational value of the publication and may not be a mere disguised commercialization of a person's personality").

[328] Paulsen v. Personality Posters, Inc., 299 N.Y.S.2d 501, 506 (N.Y. 1968). The court in *Paulsen* explained:

> The scope of the subject matter which may be considered of "public interest" or "newsworthy" has been defined in most liberal and far reaching terms. The privilege of enlightening the public is by no means limited to the dissemination of news in the sense of current events but extends far beyond to include all types of factual, educational and historical data, or even entertainment and amusement, concerning interesting phases of human activity in general.

Id.

VII. PROPERTY RIGHTS IN PERSONAL INFORMATION: SOME PRACTICAL ISSUES

The proposed law should be codified in federal legislation with certain fact-specific issues left to judicial interpretation. The federal nature of the legislation would ensure consistency of citizens' rights all over the country and bring American law into accord with evolving international privacy standards. Under that legislation, throughout their lifetimes, individuals would have an option to keep their personal information private, or conversely, sell, pledge, or license it.[329] Since the interest owned is only a life estate, property rights in personal information would not be devisable and would not pass by intestate succession.

Naturally, any personal information published by individuals themselves would enter the public domain.[330] One could argue that by simply making our information visible we "publish" it and thus give up our property right to it. This argument is flawed. It focuses on the outdated privacy rationale of secrecy instead of the more relevant rationale of control.[331] The difference between an affirmative decision to publish certain information about oneself and information inadvertently revealed through, say, browsing the Internet may be analogized to the difference between abandoned and lost or stolen property. In the first case, the owner relinquishes her property rights while in the second case she does not. I do not give up my property right in my ring just because I make it visible to others. I do not give up my property right even if I "misplace" my ring by leaving it on a bathroom sink, "lose" it by dropping it on the floor, or fail to guard it well enough from a thief. In

---

[329] At least one attempt by an individual to sell personal information has been recorded. *See* Diane Anderson, *Woman Auctions Personal Info Online* (June 15, 2000), *available at* http://www.pcworld.com/resource/printable/article/0,aid,17199,00.asp. In June 2000, Tracy Coyle tried to auction off information about herself. *Id.* She answered 378 questions commonly asked by marketers regarding her financial status, health, and religious beliefs, but no one made a bid. *Id.* A year later Coyle started a website company, www.Itsmyprofile.com, which aspires to make it possible for consumers to sell their personal data directly to advertisers. *See* Julia Scheers, *My Shoe Size? It'll Cost You* (June 11, 2001), *available at* http://www.wired.com/news/print/0,1294,44278,00.html. "Your information is just that — yours," says Coyle. *Id.* "If someone else benefits from that information, you deserve compensation for its use." *Id.* Coyle's current goal is to attract 20,000 members to make her member profiles marketable. *Id.* She plans to charge advertisers 14 cents to access each member's 1,300-question profiles and 25 cents to send members e-mails, which are routed through her site to avoid their resale. *Id.*

[330] *See* NIMMER, *supra* note 98, ¶ 16.08, at 16-24 (analogizing privacy law to trade secrecy and suggesting that intimate details of life disclosed in autobiography are not private and any property interest in respect thereto is waived).

[331] *See* discussion *supra* notes 101-04, 186-87 and accompanying text.

other words, I do not lose a property right unless I make an affirmative decision to relinquish control over it. By the same token, I do not publish personal information just because I make bits and pieces of it visible to others, or because someone manages to collect or steal it.

Recognizing the special nature of personal information, the law should protect it from involuntary transfers such as a judgment lien, although a voluntary pledge should be enforceable.[332] The pledgee should be able to perfect their security interest in personal information, just like in any other intangible, by filing a financing statement in the domicile of the pledgor — the same way security interests in customer lists are perfected now.[333] In bankruptcy, the law should provide for an exclusion of personal information from the estate of the individual, analogously to how state insolvency laws currently exclude certain personal possessions.[334]

The law should vest in the individual certain inalienable rights such as the right to obtain one's records, to demand correction of errors, and to block or erase any incomplete or inaccurate information[335] even after all other rights to it have been transferred. Similar approaches may be seen, for instance, in European legislation[336] protecting "moral rights"[337] of

---

[332] For a similar treatment of certain property, see Uniform Exemptions Act, UNIF. EXEMPTIONS ACT § 8(a)(3), 13 U.L.A. 298 (2002) (exempting from an application of judicial lien, among other things, family portraits and heirlooms of particular sentimental value to the individual).

[333] *See* U.C.C. § 9-301(1) (1998) (listing requirements for perfection of security interest in intangibles).

[334] For a similar treatment of certain property in bankruptcy, see BANKR. CODE, 11 U.S.C. § 522(b) (2000) (providing individual debtor with choice between exemptions authorized by Bankruptcy Code, other federal law, and state law); BANKR. CODE, 11 U.S.C. § 522(d)(3) & (4) (authorizing exemptions of various property that is held "primarily for the personal, family or household use of the debtor"). For an example of state debtor-creditor law exemptions, see New York C.P.L.R. § 5205(a) (exempting from application of judicial lien, among other things, family bible, family pictures, seat or pew in place of worship, various household items, wedding ring, watch, etc., all subject to value limitations).

[335] The European Union Data Protection Directive includes a similar principle. *See* Data Protection Directive, *supra* note 2, art. 12 (investing data subject with right to obtain records, correct errors, and block or erase any incomplete or inaccurate information).

[336] *See* Samuelson, *supra* note 300, at 1147 (noting that many countries protect moral rights, but two most commonly discussed are France and Germany, and providing examples of protection of moral rights in these two countries); *see also Law on the Intellectual Property Code*, No. 92-597 of July 1, 1992, *in* WORLD INTELLECTUAL PROPERTY ORG., COPYRIGHT AND NEIGHBORING RIGHTS, LAWS AND TREATIES (1996) [hereinafter French Act]; Urheberrechtgesetz (UrhG) § IV.2, arts. 12-14, *available at* http://iecl.iuscomp.org/gla/statutes/UrhG.htm [hereinafter German Act].

[337] Samuelson, *supra* note 300, at 1147 (listing such commonly recognized moral rights as right of attribution (i.e., right to be identified as author of work); right of integrity (i.e., right to protect work from alterations that would be harmful to author's reputation; right of

authors even after copyright has been sold. The moral rights regime is based on the idea that artistic and literary creations are more than just a commodity; rather, they are "emanations of the author's personality in which he can and should retain an interest even after copies of the work have entered the stream of commerce."[338] Some countries consider moral rights sufficiently important and vulnerable to make them inalienable.[339]

The inalienability regime is justified in this case by the dual nature of privacy (it is both a personal right and a social value) and by the legitimate interest of society in the accuracy of publicized information. Under the Calabresi-Melamed rules,[340] inalienability is warranted when people seek to avoid non-monetary externalities and impose on themselves a restriction, so that "they will be prevented from yielding to momentary temptations which they deem harmful to themselves."[341] If a significant number of people chose, for instance, to waive the rights described above in exchange for coupons, the society as a whole would be hurt. Making rights inalienable is particularly justified in circumstances involving information asymmetry and collective action problems (which is currently the case in the area of information privacy),[342] because those systemic problems increase the risk of irrational decisionmaking by individuals.[343]

"divulgation" (i.e., right to decide when and under what circumstances to divulge work); and, recognized in some jurisdictions, right of withdrawal (i.e., right to withdraw all published copies of work if work no longer represents author's views or otherwise would be detrimental to author's reputation). For examples of French law, see French Act, *supra* note 336, art. L. 121-1 (codifying rights of attribution and integrity), art. L. 121-2 (codifying right of divulgation), and art. L. 121-4 (codifying right of withdrawal). For examples of German law, see German Act, *supra* note 336, art. 13 (codifying right of attribution), art. 14 (codifying right of integrity), and art. 12 (codifying right of divulgation).

[338] Samuelson, *supra* note 300, at 1146.

[339] *See id.* (discussing France as example of jurisdiction that made moral rights inalienable to protect them against unfair contractual overrides). For a general discussion of the actual inalienability of moral rights in Europe see Neil Netanel, *Alienability Restrictions and the Enhancement of Author Autonomy in United States and Continental Copyright Law*, 12 CARDOZO ARTS & ENT. L.J. 1, 7, 48 n.254-305 (1994) (arguing that essential moral rights are properly considered to be inalienable under Continental law).

[340] Calabresi & Melamed, *supra* note 195, at 1111-13; *see also* Radin, *Market-Inalienability*, *supra* note 266, at 1903-36 (arguing that, in name of human flourishing, certain personal interests should remain inalienable).

[341] *Id.* at 1113. One example of such restriction would be a law prohibiting selling oneself into slavery. *Id.* at 1112.

[342] *See, e.g.*, Schwartz, *supra* note 106, at 822 (pointing out that there are significant information asymmetries and collective action problem regarding privacy on Internet).

[343] To address the same concern, the law should also impose implied warranties (e.g., accuracy and transferability) on any transferor of personal information with the individual being a third party beneficiary of those warranties. *See* Mell, *supra* note 16, at 79

Other rights in personal information should be freely transferable upon individual consent. That consent may take different forms. It could be an outright sale, in which case both the original and the secondary collector would be free to transfer the personal information to whomever they want. Alternatively, the consent may be in the form of a transferee-, industry- or purpose-specific license, either free of any restrictions or subject to certain limitations on future transfers. That license, for instance, could completely block dissemination of some of the provided information and allow sharing of other information only with entities of a particular type (e.g., located in the United States or having a similar privacy protection policy). Presumably, the price would reflect the difference in the scope of the transferred rights. That way, individuals could control the type of information a business may transfer into the secondary market. For instance, if the licensee failed to follow the terms of the transaction, the individual could revoke the license or petition a court for an injunction.[344]

Others have suggested that individual consent should be required not only for transfers of personal information but also for its collection and internal use by a company.[345] In my view, such requirement is excessively harsh on businesses and unnecessary. As long as collected information is used for product development, research, and general marketing strategies, individual privacy does not suffer. Any communications with customers or potential customers certainly must be consensual — but that is true even in the absence of any direct relationship between a business and an individual. Telemarketers' calls

---

(suggesting that "[t]he privilege of the holder to use and disclose the persona [should] carry a double warranty: a warranty of authority to disclose and a warranty of accuracy."). That would protect interests of both the individual and society, especially if the current trend of accumulation of personal information by commercial enterprises continues and certain enterprises start specializing in assembling and selling individual personal profiles.

[344] *See* Basho, *supra* note 32, at 1525 (promoting license agreements as means to regulate use and transfer of personal information). A proposed licensing agreement might provide:

> I grant Company X the right to distribute my name only to third parties with privacy policies equal to Company X's until 1/1/02 and I will receive $2.00 each time my name is transferred to such a third party. After 1/1/02, Company X must cease all use of this information and will no longer have any rights or interest in it.

Id.

[345] *Id.* A licensing agreement proposed by Basho includes the following language: "Company X is authorized to collect my name, address, income, and online buying habits. It may use this information to determine what products I will be most interested in buying, to make decisions about its own product development, and to send me emails about changes to this product." *Id.*

in the middle of a dinner are no less annoying because the caller obtained your phone number from local "white pages," rather than directly from you.

Irrespective of the chosen form of a transaction, the consent of the individual should be affirmative (based on the "opt-in" model) and informed, in writing and conspicuous on its face. In addition, the law should prohibit a collector to condition doing business with an individual on obtaining such consent.[346] This last requirement poses some interesting questions.

The first general question is how to justify this restriction? Normally, if an individual is free to sell, pledge, or otherwise transfer her property, a counterparty is equally free to demand a transfer of that property in consideration for entering into a transaction. Why forbid a collector (e.g., Yahoo!) from requiring that individuals provide their personal information as a consideration for gaining access to Yahoo! databases? The reasons for that restriction are in the inequality of bargaining positions of an individual and a service provider like Yahoo!, and in the risk of injury to individuals' privacy inherent in that inequality.

Similar considerations stand behind the doctrines of "unconscionability" and "adhesion," which permit courts to refuse enforcement of coerced agreements. The doctrine of unconscionability has been applied most frequently in areas where there is an inequality of bargaining power "to protect those who cannot protect themselves."[347] An agreement may be held unconscionable if it takes away some important rights of a consumer, including a waiver of defense clause,[348] a disclaimer of some or all warranties,[349] or consent to repossession of an item sold on credit if a seller "deems itself insecure."[350] A forced consent

---

[346] Today, many websites do not allow access to Internet users unless they provide their personal information. *See, e.g.*, Schober et al., *supra* note 45, at 721 (referring to *New York Times* website, which effectively provides that "if you will not sign in and disgorge personal information, then you can't read the paper online.").

[347] Hertz Corp. v. Attorney Gen. of New York, 518 N.Y.S.2d 704, 707-08 (N.Y. 1987); *see also* Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 449 (D.C. Cir. 1965) ("Unconscionability has generally been recognized to include an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favorable to the other party.").

[348] *See* Chem. Bank v. Rinden Prof'l Ass'n, 498 A.2d 706, 714 (N.H. 1985) (holding that "neither the waiver itself, nor the manner in which it was executed, was unconscionable").

[349] *See* Rottinghaus v. Howell, 666 P.2d 899, 903-05 (Wash. Ct. App. 1983) (holding disclaimer of warranties unconscionable where disclaimer provisions were overbroad, not bargained for, and not specifically agreed upon).

[350] JAMES J. WHITE & ROBERT S. SUMMERS, UNIFORM COMMERCIAL CODE 163 (5th ed. 2000) (listing examples of substantive unconscionability).

to the transfer of personal information takes away an equally important right of consumers — their right to privacy — and should be seen as equally unconscionable.

An adhesion contract is typically a standardized form "offered to consumers of goods and services on essentially a 'take it or leave it' basis without affording the consumer a realistic opportunity to bargain and under such conditions that the consumer cannot obtain the desired product or services except by acquiescing in the form contract."[351] The distinctive feature of a contract of adhesion is that "the weaker party has no realistic choice as to its terms."[352] A requirement that, in order to receive goods or services, a consumer must sign a standard, non-negotiable consent form permitting the collector to transfer the consumer's personal information squarely fits under the definition of an adhesion contract.

The same public policy that makes courts interfere with adhesion contracts (to avoid systematic unfair advantage by a more sophisticated party with overwhelmingly stronger bargaining opportunities) should be followed to protect individuals from collectors who may require their customers to consent to the transfer of their personal information as a condition of doing business. A consent obtained by such an ultimatum should be considered unconscionable and a contract of adhesion. That agreement should be null and void *ab initio*; any further transfer pursuant to that agreement should be deemed unauthorized and thus actionable against the collector and anyone who has obtained consumer information from it.

What if the original collector does not explicitly refuse to transact with an individual but instead offers different prices for its goods or services. For example, you can have this book for $5 if you consent to any further transfer of your personal information but, without such consent, it will cost you $15. At which point does this price differential become punitive and in fact block the transaction? Perhaps, this issue should be left for courts to decide — they are experienced in reviewing similar disputes when deciding, for instance, whether liquidated damages provided for

---

[351] Wheeler v. St. Joseph Hosp., 63 Cal. App. 3d 345, 356 (Cal. Ct. App. 1976); *see also* Burkons v. Ticor Title Ins. Co. of Cal., 798 P.2d 1308, 1320 (Ariz. Ct. App. 1989), *rev'd on other grounds*, 813 P.2d 710 (Ariz. 1991) (explaining that essence of adhesion contract is that it is offered to consumers on essentially "take it or leave it" basis).

[352] *Wheeler*, 63 Cal. App. 3d at 356; *see also* Friedrich Kessler, *Contracts of Adhesion — Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629, 632 (1943) (concluding that essence of adhesion contract is that bargaining position and leverage enable one party to select and control risks assumed under contract).

in an agreement are reasonable[353] or whether a foreclosure sale was at fair market value.[354] The determination of substantive unconscionability pursuant to section 2-302 of the U.C.C.[355] often turns on the question of whether a contractual price was excessive.[356] A court may find a price excessive because "it returns too great a profit to the seller, or because it yields too great a return on the seller's invested capital, or because it is a substantially higher price than other merchants similarly or unsimilarly situated charge for like items."[357] Analogous criteria may be applied by a court to determine whether the price attached to the individual's personal information is commercially reasonable or excessive and, therefore, punitive and impermissible.

The original collector in the proposed legal structure would be able to freely use any personal information collected by it in the course of selling goods or services to its customers, but only internally. In the modern corporate world full of corporate giants, mergers and acquisitions, the meaning of "internal use" would need to be defined. I would suggest that affiliates and subsidiaries be allowed to enjoy the same kind of automatic license as the original collector itself, but only affiliates and

---

[353] *See, e.g.*, John Deere Leasing Co. v. Blubaugh, 636 F. Supp. 1569, 1574-75 (D. Kan. 1986) (concluding that liquidated damages clause on purchase option price before option matured was punitive and not enforceable); Northwest Acceptance Corp. v. Hesco Constr., Inc. 614 P.2d 1302, 1306-07 (Wash. Ct. App. 1980) (opining that fair damages formula was not penalty).

[354] *See, e.g., In re* Lindsay, 59 F.3d 942, 949 (9th Cir. 1995) (deciding whether foreclosure sale was conducted legally and fairly); Resolution Trust Corp. v. Maplewood Invs., 31 F.3d 1276, 1278-79 (4th Cir. 1994) (reversing trial court's decision to bar creditor-purchaser from obtaining deficiency judgment because property sale was improper due to conflict of interest on part of trustee and officers); OMP v. Sec. Pac. Bus. Fin., Inc., 716 F. Supp. 251, 254 (N.D. Miss. 1989) (holding foreclosure sale was conducted in equitable manner because there was no improper conduct even though lender bid amount was substantially below amount of indebtedness).

[355] *See* U.C.C. § 2-302 (1998), which states:

> If the court as a matter of law finds the contract or any clause of the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract, or it may enforce the remainder of the contract without the unconscionable clause, or it may so limit the application of any unconscionable clause as to avoid any unconscionable result.

[356] *See, e.g.*, WHITE & SUMMERS, *supra* note 350, at 158 (noting that one of two groups of cases where courts most often find clauses to be unconscionable is excessive-price cases).

[357] *Id.* at 161; *see also* Am. Home Improvement, Inc. v. MacIver, 201 A.2d 886, 888 (N.H. 1964) (finding price excessive because mark-up was too high); State *ex rel.* Lefkowitz v. ITM, Inc., 275 N.Y.S.2d 303, 321-22 (N.Y. Sup. Ct. 1966) (finding price excessive because it was significantly higher than price charged by other merchants for same or similar goods).

wholly-owned subsidiaries in the same line of business.[358] For other affiliates and subsidiaries, consent of the individual should be required, just as for any other transfer of personal information from an original collector to the secondary market.[359]

VIII. ENFORCEMENT OF INDIVIDUAL'S PROPERTY RIGHT IN PERSONAL INFORMATION

Finally, a few words regarding the enforcement of these rights. The proposed statute should provide for a private cause of action, legal fees (which may be denied in case of a frivolous lawsuit), injunctive relief, and damages. The damages should be the higher of actual damages and a certain statutory amount. This amount may be a fixed sum or may be calculated for each day of violation, analogously to the Electronic Communications Privacy Act, which provides for the higher of $10,000 or $100 per each day of violation.[360] In the case of an unauthorized transfer of personal information, a fixed amount would be more appropriate, whereas in a situation where the defendant refuses to correct inaccurate personal information, a *per diem* amount would probably make more sense. In addition, criminal penalties, similar to those provided by the Fair Credit Reporting Act, should be available to penalize any officer or employee of a company who knowingly and

---

[358] *See, e.g.*, Peter P. Swire, *Modern Studies in Privacy Law: Notice, Autonomy and Enforcement of Data Privacy Legislation*, 86 MINN. L. REV. 1263, 1311 (2002) (advocating limiting inter-affiliate sharing of information to affiliates in same line of business).

[359] The Gramm-Leach-Bliley Act, for example, has been widely criticized for allowing inter-affiliate sharing of personal information. *See, e.g.*, Ralph Nader, *Banking Jackpot*, WASH. POST, Nov. 5, 1999, at A33 ("The affiliates of the conglomerates and their telemarketers will be free to share many intimate details of an individual's buying habits, investing patterns, health records, entertainment choices, employment data and other aspects of one's existence"); *see also* Cuaresma, *supra* note 66, at 512. Cuaresma explains:

> Even though Congress explicitly directs each financial institution to "respect the privacy of its customers," customers cannot opt-out of information sharing between affiliates. Allowing a single company to engage in banking, securities, and insurance activities increases the secondary uses of such information. For example, once a banking division obtains nonpublic personal information, there is no legal roadblock to prevent it from sharing that information with its insurance and securities divisions.

Cuaresma, *supra* note 66, at 512.

[360] *See* Electronic Communications Privacy Act, Pub. L. No. 99-508, § 252(c)(2), 100 Stat. 1848 (1986) (providing for recovery of greater of (A) sum of actual damages suffered by plaintiff and any profits made by violator as result of violation, or (B) greater of $100 day for each day of violation and $ 10,000); *see also* Mell, *supra* note 16, at 79 (advocating similar penalties for unauthorized dissemination of personal information).

willfully supplies information concerning an individual from the company's files to a person not authorized to receive that information.[361]

Legislation based on such principles would adequately protect respective interests of American businesses and consumers and would bring U.S. law into accord with the developing body of international law regarding treatment of personal information.

CONCLUSION

As I was finishing this Article, my eleven-year-old daughter received a junk-mail letter with some Internet-related advertisements in it. The letter was addressed to a Sue Grong (a fictitious name my daughter has used a few times on various websites), but our home address was absolutely correct. "Why did you give them our real address?" I asked. "But I did not," she replied, "I gave them a non-existing address in New York City." "So how did they get our address?" I started to say, and then I stopped. . . .

By the way, Peter Steiner's cartoon had a sequel.[362]

[361] *See* United States Fair Credit Reporting Act, Pub. L. No. 91-508 (1970), as amended by Pub. L. 104-208 § 620, 110 Stat. 3009 (1996) (providing for maximum two-year imprisonment for "[a]ny officer or employee of consumer reporting agency who knowingly and willfully supplies information concerning an individual from the agency's files to a person not authorized to receive that information"); *see also* Mell, *supra* note 16, at 79 (suggesting similar penalty for unauthorized willful disclosures).

[362] *Anonymizer*, *at* http://web.archive.org/web/19970403034059/www.anonymizer.com/cartoon.html (last visited Mar. 1, 2003) (the website's motto is: "Because on today's Internet, people *do* know you're a dog").

***