

Article

***633 OUR DATA, OURSELVES: PRIVACY, PROPERTIZATION, AND
GENDER [FN1]**

Ann Bartow [FN1]

Copyright © 2000 University of San Francisco School of Law; Ann Bartow

CYBERSPACE BRIEFLY HELD a lot of promise for women. [FN2] It was the closest we could expect to come to being "brains in . . . boxes." [FN3] In cyberspace, we would not be judged by our bodies. No one would know when we were having bad hair days. We would not ever have to wear make-up and high heels. We could even be "men" without hormones or expensive surgery. Then we began shopping and chatting over the Internet. Shortly thereafter, we learned that anyone in cyberspace could ascertain our gender, ages, incomes, education levels, marital status, sizes, consumer purchase proclivities, aspects of our health, and employment histories, and the number, ages, and genders of our children, and that this information could be used to sell us *634 goods and services. [FN4] Now, instead of brains in boxes, we are "eyeballs with credit cards." [FN5]

Cyberspace has become fertile ground for the harvesting of consumer data, and consumers have very little ability to keep their personal information private, especially online. Yet, we are unlikely to see any sector of government launch comprehensive, enforceable online privacy initiatives based on the precept that privacy is a good unto itself. [FN6] At the same time, copyright, trademark, and patent protections obtained by companies for words, thoughts, ideas, and symbols are expansive and seemingly grow broader on a daily basis. [FN7]

This article considers the possibility that one evil can be remedied by another. Perhaps the current corporate-friendly intellectual property framework, so effective at turning the information superhighway into a toll road, can be co-opted to enable individuals to "own" and control our own personal information, giving us the tools to "gatekeep" our own informational privacy. [FN8] Perhaps we should have the same property rights in our names and personal information that corporations have in their names and data. At a minimum, we should have the same property rights that corporations have in our names and personal information. Perhaps, if nothing else, an attempt to secure property rights in our personal information will draw attention to the ongoing corporate propertization of everything.

I. A Disproportionate E-Impact on Women

The data collection issue is of singular importance to "web swimming" women. [FN9] Women do most of the shopping in real space and will inevitably do the same in cyberspace, where we are appearing in *635 ever increasing numbers. [FN10] Women control 80 to 85% of all personal and household goods spending and are reportedly the fastest-growing audience on the web, a market "expected to grow to 65 million in 2002 from 45 million today." [FN11] Internet analysts agree that "anybody who wants to make money on the Internet cannot afford to ignore [women]." [FN12]

In cyberspace, women are inherently desirable, but only because things of value, data, and ultimately money, can be taken from us. In the abstract, many of us may be concerned about personal privacy, but when we are out swimming the web, this concern may be overshadowed *636 by a desire to participate fully in online life. [FN13] We are lured to special "women- oriented" web sites that efficiently facilitate the extraction of our personal information assets and our nummular currency. [FN14] Attracted to interesting, high quality content and the promise of supportive, dynamic online communities, we are easily persuaded to actively share personal information with site owners and advertisers. [FN15] Simultaneously, and often unthinkingly, we also passively share information about ourselves through the articles that we select to read, the topics that we elect to post about, and the sites and advertisers that we choose to visit. [FN16] Docilely, we allow corporate entities to monitor our online efforts to educate and inform ourselves, support each other, and purchase goods and services for our families and ourselves. [FN17] This data is then used to more efficiently separate us from our money. [FN18] *637 The fact that we give web sites information of greater value than the content we receive is obfuscated by our sense of gratitude that we are no longer ignored in cyberspace; that typing the keyword "woman" into a search engine now produces something besides pornography sites; that we finally have cyber-rooms of our own. Indeed, web analysts postulate that some women actually form emotional bonds with certain sites, using cyber fora to create social networks for themselves. [FN19] Electronic entities then attempt to exploit this sharing and networking for commercial gain. [FN20]

Online data collection should be a serious concern to everyone who ventures into cyberspace, regardless of gender. This phenomenon is particularly problematic for women because, as explained above, women do most of the hunting and gathering for themselves and their families, and are therefore becoming the primary targets of marketers in cyberspace. [FN21] The admittedly problematic (and perhaps appallingly cynical) solution proposed, however, applies equally well to men. If all individuals are awarded the same broad property rights *638 in their personal data that business interests successfully assert in words, ideas, and information, people can control how much online privacy they have and, correspondingly, the levels of targeted marketing to which they are subjected.

II. The Online Data-Collecting Flypaper

In cyberspace women are the quarry, and we are "targeted" by web sites that are "aimed at us." Online companies create content that will lure women to their web sites. Touted by the New York Times as a "place for serious sisterhood," iVillage [FN22] has immense corporate backers, including General Electric, America Online,

Intel, Tele-Communications, Ralston Purina, Kimberly-Clark, AT&T, Ford, and Amazon.com. [FN23] An iVillage spokesman stated, "We're very focused on the fact that the Web is one of the best mass- marketing opportunities ever." [FN24] The company offers a plethora of online shopping opportunities and "targets" affluent women between the ages of 25 and 49, a "highly valued demographic." [FN25] One tactic that iVillage uses is blending content and commerce as seamlessly as possible. Candice Carpenter, the primary architect of iVillage "pioneered the use of 'integrated sponsorships,' where advertisers participate in the creation of content, the information, articles, and services that appear on the company's Web sites." [FN26] For example, Ralston Purina sponsors a pet channel, which offers chat rooms, message boards, and access to a pet expert. The pet expert also happens, completely uncoincidentally, to be a Ralston Purina employee, who *639 can refer web swimmers to products available at an accompanying online pet store. [FN27] Similarly, "[i]n what it called a breakthrough partnership with the milk industry, iVillage established a 'behavior modification program' of 'weekly chats, E-mail reminders, and lively message boards' to encourage 'the habit of drinking three glasses of milk per day.'" [FN28] One will not find any information challenging the purported benefits of milk present at this site, so there is no need to worry our pretty little heads about conflicting data regarding the health benefits or utility of high levels of milk consumption. iVillage also maintains a network of many web sites and claims millions of registered members. [FN29] It seeks to build a community of women on the Internet around issues such as divorce, miscarriage, breast cancer, child discipline, job stress and "unfortunate taste in boyfriends," and then "monetize" the community by profitably selling products and advertising. [FN30] One example is found at the iVillage site Parent Soup, [FN31] where "a pregnant woman can enter her due date and receive a calendar showing day by day what's likely to be happening inside her body." [FN32] Women with overlapping calendars are directed to a "Pregnancy Circle," an online support group where they can trade advice and concerns and are simultaneously prompted to purchase items such as books from Amazon.com, [FN33] baby goods from iVillage's iBaby, [FN34] and maternity clothes from iVillage's iMaternity. [FN35]

Another alleged "place for serious sisterhood" is Microsoft's online magazine, insipidly named Underwire [FN36] and ostensibly "more serious and sedate" than iVillage. [FN37] Microsoft also maintains WomenCentral, [FN38] a web site/Internet channel of the Microsoft Network. [FN39] WomenCentral features content from Women.com, [FN40] another *640 online publisher of "women's material," as well as content from Underwire and other original material. [FN41]

Oxygen Media, backed in part by Oprah Winfrey, has also constructed online flypaper for female consumers, and runs three "women-oriented" sites it bought from America Online in the fall of 1998: Electra, [FN42] ThriveOnline, [FN43] and Moms Online. [FN44] Its main site [FN45] appeared in late May of 1999. [FN46] The concept of Oxygen is to fuse the television, the Internet, and the telephone, creating a strongly tight-knit, multimedia community of women. [FN47] Aspects of Oxygen Media's mission were imbued with an aura of public interest legitimacy when Markle Foundation President Zoe Baird announced a joint venture between Oxygen Media and the charitable Markle Foundation. [FN48] The venture involves \$8.5 million

dollars worth of research, \$4.5 million of which the Markle Foundation is providing, on "the information needs of women." [FN49] According to Baird, The Oxygen/Markle Pulse will develop baseline ongoing research, day in and day out, to find out what women want, what they are concerned about, and how they feel about the world around them. All of this will be made public so that other companies can use it. We hope it will influence public perception and women's perception about their influence. [FN50]

Thus, while the information generated by this research may somehow give women more political power, as Baird seems to intend, in part, it will also, by design, assist companies seeking to identify, understand *641 and target female consumers. [FN51] This approach seems to reflect a fundamental assumption that meeting the needs of women requires the efficient sales and marketing of goods and services to women. In other words, our need to shop is so powerful that a charitable foundation will, in the name of the public good, spend millions of dollars assisting for-profit companies with efforts to more sensitively and responsively take our money.

Other gateway pages are bawdier, such as Estroclick, [FN52] which bills itself as "an estrogen powered web network." [FN53] This site promises "broad-based content" (get it?) at "girl sites that don't fake it" and features links to special interest sites like hipMama, [FN54] Wench, [FN55] Bust, [FN56] and Hissyfit. [FN57] Still other sites do not bother offering much in the way of content at all, instead pitching their sites as time and money savers that research products and services on our behalves. [FN58]

III. Buy This 16-Year-Old and Get All Her Friends Absolutely Free [FN59]

Like women, "teenagers" are also seen as a lucrative emerging e-market. [FN60] Many companies especially want to collect data from teenage*642 women, a highly coveted audience. [FN61] In addition to their purchasing power at present, they are "proto-consumers whose purchasing habits and brand identification are still soft enough to shape" and "at the very beginning of their lifetime value as a customer [sic]." [FN62] Data is collected first to measure, and then ultimately to influence the popularity of consumer goods aimed at young women. Ironically, one site designed to ensnare teenagers for market research purposes, SmartGirl Internette, [FN63] has the (apparently) trademarked, non-ironic slogan "smart girls decide for themselves." [FN64] At the "Speak Out" section of the SmartGirl site, [FN65] "girls answer multiple-choice questions and opine to their hearts' content in open response areas. Their teenage sentiments are collected, cross-referenced and sold to SmartGirl clients or sent out in press releases for promotional purposes." [FN66] SmartGirl uses the data it collects to perform customized research and surveys. [FN67] It then publishes a line of subscription reports, including the Celebrity Report, which appears six times per year and costs \$10,000 annually, and the shorter monthly Trend Report, which costs \$2,000 per year. [FN68] SmartGirl framed this market research as a service to its teenaged readers, as a way to keep the site free of advertising, and as a mechanism for determining "what girls want so companies can make better stuff for you and really meet your needs." [FN69]

Empirically, teenagers are willing not only to provide data about themselves, but also to divulge information about their friends and *643 other family members. [FN70] A recent study conducted by the Annenberg School of Communications at the University

of Pennsylvania determined that while teenagers expressed a general nervousness about privacy on the Internet, most would provide personal information about themselves and their families, especially in exchange for a free gift. [FN71] Teenaged girls are also likely to engage in very personal online dialogues. [FN72]

IV. Now That They've Come, What Can We Sell Them?: Data Collection and Targeted

Marketing [FN73]

What sets so-called "women-centric" sites apart from traditional real space, hard copy women's magazines is that, in addition to providing content and subjecting readers to advertisements, these sites can record which articles we read and which ads catch our eyes, collecting reams of intimate personal data from each person who accesses the site. [FN74] Computers can gather, store, sort, retrieve, and *644 disperse previously incomprehensible quantities of data. [FN75] As one observer stated:

It's not just that technology collates existing information like public records in new and ways. It also creates new kinds of information. One of the most interesting is "clickstream" monitoring, a page-by-page tracking of people as they wander through the Web. Your clickstream reveals your interests and tastes with unnerving precision. (Did you go from slate.com to a Volvo dealer's Web site? Did you then buy some brie from peapod.com, the online grocery? You may be one of those limousine liberals we've been hearing about.) And when Web merchants combine clickstream analysis with another new software technique known as "collaborative filtering," which makes educated inferences about your likes and dislikes based on comparing your user profile with others in the database, they have a marketing tool of high potential not only for customer satisfaction but also for abuse. [FN76]

One Internet security consultant demonstrated that a data miner could easily collect our names, street addresses, e-mail addresses, birthdays, transactional information, and insight about products that interest us after we had visited fewer than ten web sites. [FN77] The collection and assessment of "clickstream" [FN78] data enables delivery of precisely directed, sometimes personalized, advertisements. These advertisements are rabidly sought after by advertisers, so that "targeting" *645 can be as accurately calibrated as possible. [FN79] After an advertisement draws us to a site, the customization continues.

[What e-commerce companies term] the utopian vision of true "one-to-one marketing" . . . is predicated on gleaning as much information as possible about a customer and building a storefront tailored to that particular individual. After gathering personal data and tracking a shopper's movements within the site, Internet retailers can display products to suit that customer's tastes and price range, or list customized specials and sales. [FN80]

As a result, "an Internet user who looks up tourist information about England on a travel site . . . might be fed ads for airlines flying into Heathrow Airport and for hotels in London as he checks sports scores." [FN81] Marketing analysis of a "women's site" web swimmer might therefore transpire as follows: [FN82]

She's reading the articles on weight loss. Cross-reference this with her shopping records, which indicate she purchases clothing in rather large sizes. Her income level looks like it could support medication, prepackaged food, a diet center, and/or a health

club, or perhaps we could entice her with a rich line of desserts and designer chocolates. Her medical records bespeak a family history of hypertension and heart disease. She has articulated a desire to shed pounds and increase her level of physical fitness in an online discussion. She's also *646 worried that she would have trouble maintaining a healthy diet if she were to become pregnant. Let's send some select banner ads her way, and some precisely targeted, personalized e-mail advertisements as well, because effective marketing is the true purpose of this web site, and marketing in the guise of sisterhood, friendship, and support is the most potent of all. [FN83] Online merchants will not voluntarily forgo these opportunities: The concept of online privacy "is directly at odds with one of the most attractive aspects of doing business online--the Net's capacity for helping target marketing and advertising efforts directly at specific users." [FN84] Gerry Laybourne, the self-described Chairman, CEO, and Founder of Oxygen Media, has boasted:

70% of women cannot stand the way America advertises to them. It's insulting. It's demeaning. It doesn't understand what motivates them. And they don't want to be sold. They want to buy, they want information, and they want to be talked to as real human beings. And I know this from what we did with Nickelodeon, where the same stereotypes were held for kids. And it is amazing what you can do when you like your audience, you're an advocate for your audience and you're on their side. [FN85]

Oxygen Media and its competitors may indeed do "amazing" things for its corporate clients, after we freely provide the tools--copious amounts of our personal data. Once the data is disgorged and tabulated, we are placed squarely in vendors' sights, with our cyber-bull's eyes clearly e-outlined, ready to be aimed at. We are simply prey. The chief executive of Women.com, after describing techniques for luring women to and through a web site with quality content, enthused, "For advertisers, it's fantastic because you're catching a consumer right in flight." [FN86] Targeted marketing techniques can significantly increase the response to an advertisement and web sites can correspondingly charge a premium for delivering ads aimed at certain users.

[FN87] One company has even patented a "[m]ethod and apparatus *647 for determining [the] behavioral profile of a computer user." [FN88] This method "provides targeting of appropriate audience based on psychographic or behavioral profiles of end users" that are formed by "recording computer activity and viewing habits" for the purpose of "continually auto-target[ing] and customiz[ing] ads for the optimal end user audience." [FN89] Targeted advertising has been called the "Holy Grail" of the online advertising industry because it allows publishers to charge higher rates based on a perception of enhanced efficacy. [FN90]

Women's sites with compelling content will certainly make their owners wealthy. As one commentator observed, "The Internet has changed the characteristics of information. It used to be that a bank robber would go to a bank to steal money. Now the information about customers is almost as valuable as the financial assets themselves." [FN91] Another opined, "The Internet is an absolute gold mine" of exploitable personal information. [FN92] Still others stated, "The digital deposits of . . . [online] transactional details are so deep that the practice of exploiting their commercial value is called 'data-mining,' evoking the intensive, subterranean, and highly lucrative labors of an earlier age." [FN93] At least one commercial web site illustrated just how valuable it considered consumer data when it downgraded

customers' ability to evaluate its products by cutting a zoom feature in order to free up bandwidth--so it could "employ a sophisticated database that can track inventory as a user enters the site and can serve registered customers *648 images of items they might like." [FN94] Further evidence of the value of personal information is provided by the actions of Free-PC.com. [FN95] This company gave away 10,000 computers to individuals who were willing to provide extensive demographic data and accept a constant stream of advertisements, and a host of other companies providing ostensibly "free" goods and services over the Internet. [FN96]

Meanwhile, web sites encourage web swimmers to "shop naked." [FN97] Presumably, the intended meaning is that we can e-shop as we are, without toting children, hiring babysitters, applying make-up, or even bothering to dress. A second denotation is more ominous--shop naked because we are figuratively nude. Netscape and its clients know everything about us, our personal flaws and most intimate attributes have been stripped from us and are known to all. We are e-naked while we e-shop on the Internet. The more we shop, the more exposed we become. As two observers articulated, "Imagine walking through a mall where every store, unbeknownst to you, placed a sign on your back. The sign tells every other store you visit exactly where you have been, what you looked at, and what you purchased. Something very close to this is possible on the Internet." [FN98] It is not only our online transactions that will define us in cyberspace. Some Internet marketers, in an effort to be fully comprehensive, will "[combine] information gathered from people online with vast stores of data on *649 these same people kept by companies that compile traditional mailing lists." [FN99] Indeed, "[a] series of initiatives . . . are converging to transform the browse-and-surf Internet into a giant information exchange, one that features a tug-of-war between consumers and Web sites for everything from e-mail addresses to shoe sizes." [FN100] Paul Schwartz has described this as "the privacy horror show currently existing in cyberspace." [FN101] In the future, even our home appliances may contribute information to our marketing profiles. [FN102]

Sometimes data collected on us will be used to deny, rather than sell us material things. [FN103] A newly formed debit credit bureau "will combine data from full credit reports with demographics and other information 'mined' from various computer sources. A computer-generated credit score will [then] determine whether a store should accept an individual's debit card." [FN104] Related practices, involving use of a person's banking, insurance, credit card, brokerage transactions records (and, conceivably, cyber-indicia of race, age or religion) to determine whether she is too risky a candidate to receive a loan or line of credit, have been christened "digital redlining." [FN105] In other instances, data derived from a collective us will be used to maximize certain types of popular content and minimize or eliminate features that are less frequently accessed, thereby denying desired content to individuals with less mainstream interests. [FN106]

*650 Commercial entities track which advertisements lure particular web swimmers without warning us that in the process of learning about a product or service, we are also educating merchants and advertisers about ourselves. In "real space," consumers who might answer surveys or participate in focus groups could hardly do so without some awareness that they were giving information or being observed. Sitting alone in a room in our homes, with a computer we have purchased, swimming the web on time

we are paying for, is not an activity we would expect to have extensively monitored. We might expect our online purchases to register and of course they do. But, individual Internet services amass detailed records of who uses their sites, how the sites are used, and can then cooperatively pool data "into a central database containing digital dossiers on potentially every person who surfs the Web." [FN107] In fact, even the act of placing objects in online "shopping carts," but later declining to purchase them, is closely observed.

Using this information, online merchants can then devise ways to convert browsers to buyers, such as by giving shoppers fewer opportunities to abandon purchases to maximize impulse spending. [FN108] Borrowing (and trampling) a cliché familiar to lawyers everywhere, this has been characterized as "'mak [ing] a consumer's purchase decision as slippery a slope as possible." ' [FN109] One online department store actually pursues shoppers who abandon large purchases, calling or e-mailing them to try to close the sale, identifying them with information knowingly or unknowingly provided. [FN110]

There is a snowball effect too. The more information an entity has about us, the more they are able to collect. Information from credit card purveyors documents not only our creditworthiness, but also our travels by recording airline or train tickets, rental cars, gasoline purchases, and hotel charges. Information from food markets gives big clues about our consumption of fat, sugar, red meat, cigarettes, and alcohol, as well as how many servings of fruits and vegetables *651 we are likely imbibing. Simply paying for a purchase by credit card may also provide the vendor with our social security numbers. [FN111]

V. Manufacturing Demand

Web merchants lure women to putatively supportive sites, learn about our frailties and desires in the context of the articles we read, the discussion groups we post to, the chat rooms we visit (and what we say when we are there). In the guises of helpfulness and sisterhood, they then use this information to sell us products and services, free of targeted intervention, for which we have not expressed or entertained desires or needs. [FN112] As Jerry Kang observed:

After all, personal information is what the spying business calls "intelligence," and such "intelligence" helps shift the balance of power in favor of the party who wields it. . . . [A]nother's control of our personal information can make us susceptible to a whole range of ungenerous practices. It could subject us to influence that crosses the line between persuasion and undue influence. Sophisticated advertisers, for example, do not merely track consumer demand; they manufacture it outright. Detailed knowledge of who we are and what we consume makes the job of preference fabrication that much easier. [FN113]

The insidious effectiveness with which a marketer can infiltrate and co-opt a discreet subculture is exemplified by Nike's successful campaign to market shoes to skateboarders. [FN114] After discerning that skateboarders felt victimized by intolerant police officers and local government officials, Nike produced an ad that humorously asked what it would look like if other athletes were harassed and fined the way skateboarders apparently routinely are. [FN115] By acknowledging and harnessing feelings of persecution, Nike calculatedly transformed itself from an

enemy into a sympathizer, bringing the skaters "into the brand's fold." [FN116] The one-to-one marketing possible over the Internet will give Nike and other companies the power to ascertain, collect, monitor, and manipulate not only the emotions and perceptions of subcultures, but also of individuals.

*652 Data mining, data aggregation, and data distribution in cyberspace also perpetuate targeted "direct marketing" in real space. By acquiring and compiling information about individuals, direct mailers can eschew mass mailings in favor of customized pitches and marketing niches, improving their bottom lines. [FN117] No trees are saved in the process, though. "Junk mailings" actually increased in 1998 and appear to be stoked, rather than usurped, by the Internet and the information it provides. [FN118]

It should be noted that some of the people deriving wealth from women accessing these and other women-directed sites are in fact other women. While the folks making millions from hardware and software are radically disproportionately male, the consumer service and marketing aspects of e-commerce have brought cognizable numbers of women into the web e-economy. [FN119] Some argue that simply bringing more women into the design, application, and evaluation of new technologies will integrate women into cyberspace in a healthy, productive way. [FN120] We might reasonably anticipate that just as the involvement *653 of smart, talented women in enterprises such as Oxygen Media will result in better online content, the involvement of women in developing technology will inevitably lead to better technology. However, in both cases, the end result will be attempts to sell more goods and services to women--either by advertising the goods and services on high quality women oriented sites or through inventions embodying technology developed by women. The assumption that being enticed to buy more things benefits women is bolstered, rather than questioned. [FN121]

VI. Data Collection and the Meaning of "Female" in Cyberspace

Datum by datum, woman by woman, the cyber-definition of "female" is being constructed. One observer remarked that reading about the behavioral studies and statistical sum-ups that advertisers create made her feel like "a discarded lump of target-audience Spam." [FN122] Compilers of her information will decide what she means in cyberspace. [FN123] Derivative e- stereotypes, braced by a plenitude of personal *654 information, will appear scientific and incontrovertible. [FN124] Aggregations of data will certify to entities engaged in commerce:

This is what older cyber-women want to wear, that is what younger cyber-women want to read, these are the toys that appeal to middle class cyber-women with children, those are the hats and wigs likely to be purchased by cyber-women undergoing chemotherapy.

Data collectors thus position themselves as interpreters of the popular will. Women.com deserves special mention for proclaiming that it had conducted research demonstrating that all women fall into one of six categories, or "psychographic segments" for net marketing purposes: Pillars, Movers, Trendsetters, Believers, Breadwinners, and Explorers. [FN125] Meanwhile, an advertising agency, with many online clients, subdivides mothers into a mere four assemblages: June Cleaver: The Sequel, Tug of War, Strong Shoulders, and Mothers of Invention. [FN126]

Additionally, online activities may also be monitored for social science research purposes that may or may not have a direct relationship to commerce, making web swimmers unwitting subjects of research without their consent. [FN127] Chat rooms and "clickstreams" are tools that can be utilized for example, either by anthropologists in academia or "industrial anthropologists" who are employed by companies to study consumer behavior. [FN128] The advertising firm Ogilvy & Mather overtly recruits "anthropology Ph.Ds who have 'no ideological or moral objections to consumption/materialism.'" ' [FN129] Behavioral *655 scientists are also employed to observe consumers and, ultimately, to persuade them to make certain purchasing decisions. [FN130]

It has been argued that extensive, nonconsensual observation is in tension with human dignity, in part because it interferes with exercises of choice and leads inexorably to self-censorship. [FN131] Such observation can also sell a lot of sneakers. Nike marketers embarked on "an ethnographic fact finding tour" of high school girls' basketball in meet space, and based on its findings, the company invented a replica girls' high school basketball team, which was "made the subject of intentionally low-budget-looking commercials that document the team's arduous, unsung road to a fictitious state championship." [FN132] Consumers found the faux authenticity very convincing. [FN133] The ability to cheaply and efficiently collect reams of data in cyberspace will enable much smaller, less wealthy companies to fabricate its own targeted marketing campaigns.

Ironically, while we may be targeted individually for marketing purposes, the only content that may ultimately be available to us is what is demonstrably popular to the masses (via "clickstream" accretion), which we may find bland and unoriginal, or even patently offensive. One journalist observed, "The more we learn about exactly how much and why you like us, the less excuse we'll have to rely on our own judgment." [FN134] He further noted:

In print publications, certain departments depend on an at best fragile feeling of editorial obligation to keep them running; rare is the magazine that can justify a book review section--not to mention, *656 say, dance or visual arts coverage--on readership alone. Glamour magazine couldn't even justify continuing the only women-in-politics column in a major women's mag, killing it last fall. Improved metrics could only worsen this tendency. The online-media business is already founded on mealy-mouthed rationalizations about how editorial/business compromises--commerce links next to articles, selling placements within search-engine results--are really just foresighted, win-win strategies to empower users and give them what they want. As we [journalists] get better and better at giving readers exactly what they want, what will be the percentage in trying to give readers what we think they need? [FN135] Desirable, online content may still be unavailable if we do not wish to provide personal information. [FN136] Even when we are willing to capitulate, we may still be denied access if we do not have a large enough income or fit other demographic criteria. [FN137] According to at least one webtrepreneur, "[t]he Web of the future will be all about 'coach, business and first class.'" ' [FN138] Consumers may be categorized by variables such as income and purchasing habits. [FN139] Content would be made available to them based on whether they occupied "basic, gold, [or] platinum tiers." [FN140] Digital redlining can be "employed to determine who gets--

and who is excluded from--all kinds of opportunities like jobs, housing and education." [FN141]

The use of e-data for e-stereotyping will not be limited to women. Dispersal and collection of personal data online has comparable ramifications for cognizable demographic groups such as racial minorities. [FN142] At present, companies are more interested in "women" than they are in "minorities" per se because women do most of the *657 shopping across racial lines. [FN143] As more racial minority members gain Internet access, race specific sites will undoubtedly develop apace. [FN144] These sites will likely feature quality content intended to draw the targeted group to the site, where data will be collected and reactions to specific content offerings will be measured and evaluated. [FN145] Site visitors will be exposed to advertisements tailored by racial expectations and stereotypes, which in turn may be "verified" or "fine-tuned" by data that is reaped. [FN146]

VII. Owning Our Data

One could argue that the right to privacy is a platform from which to wrest control of our personal information. Certainly, a privacy-based approach would be doctrinally preferable to those aghast and appalled at the prospect of expanding the scope of intellectual property protection in the manner discussed below. However, it is not *658 likely to be successful. [FN147] We certainly do not have personal information privacy at the moment. We are not like Europeans, who are protected by "strict and broad data privacy laws that protect personal information, like where a citizen lives, what [s]he buys, and how much money [s]he makes." [FN148] The only recent data protection law enacted in the United States protects only children.

A. The Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act [FN149] ("COPPA" or "Act") was passed in October of 1998. This Act requires a "website or online service directed to children" to obtain verifiable "parental consent" prior to collecting individually identifiable personal information from children under the age of thirteen. [FN150] Parents are also to be provided access to personal information collected about their children and the opportunity to prevent further use or collection of this personal information. [FN151] Commercial web site operators are further required to "establish and maintain reasonable procedures to protect the confidentiality, security, accuracy, and integrity of personal information collected from children." [FN152] The Federal Trade Commission ("FTC") is the agency charged with promulgating regulations to implement COPPA. On October 20, 1999, the FTC issued the Children's Online Privacy Protection Rule [FN153] *659 ("Rule"), which went into effect on April 21, 2000. The Rule requires certain commercial web sites to obtain parental consent before "collecting, using, or disclosing" personal information from children under thirteen. FTC Chairman Robert Pitofsky asserted, "The rule meets the mandates of the statute. It puts parents in control over the information collected from their children online, and is flexible enough to accommodate the many business practices and technological changes occurring on the Internet." [FN154] COPPA's implementation was driven partly by a March 1998 survey of 212 commercial children's web sites, which found that "while 89 percent of the sites collected personal

information from children, only 24 percent posted privacy policies, and only one percent required parental consent [for] the collection or disclosure of children's information." [FN155]

COPPA applies to commercial web sites and online services "directed to children that collect[] personal information from children or . . . that ha [ve] actual knowledge that [they are] collecting personal information from . . . child[ren]" under thirteen. [FN156] These sites will be required to provide site-based notice about their policies with respect to the collection, use, and disclosure of children's personal information, and (with certain statutory exceptions) to obtain "verifiable parental consent" before collecting, using or disclosing personal information from children. COPPA defines "verifiable parental consent" as "any reasonable effort (taking into consideration available technology) . . . to ensure that a parent of a child . . . authorizes the collection, use, and disclosure" of a child's personal information. [FN157]

The Rule "temporarily adopts a 'sliding scale' approach that [enables] Web sites to vary their consent methods based on the intended use[] of the child's information." [FN158]

For a two-year period, use of the more reliable methods of consent [, such as] print-and-send via postal mail or facsimile, use of a credit card or toll-free telephone number, digital signature, or e-mail accompanied by a PIN or password[,] will be required only for those activities that pose the greatest risks to the safety and privacy of children--i.e., disclosing personal information to third parties or making it publicly available through chatrooms or other interactive activities. [FN159]

***660** "For internal uses of information, such as an operator's marketing back to a child based on the child's personal information, operators will be permitted to use e-mail, as long as additional steps are taken to ensure that the parent is providing consent." [FN160] The Rule requires operators to "give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties." [FN161]

However, the Rule also "sets forth several exceptions to the requirement of prior parental consent that permit operators to collect a child's e-mail address for certain purposes." [FN162] "For example, no consent is required to respond to a one-time request by a child for 'homework help' or other information." [FN163] "In addition, an operator can enter a child into a contest or send a child an online newsletter as long as the parent is given notice of these practices and an opportunity to prevent further use of the child's information." [FN164] "The Federal Register notice accompanying the [R]ule makes clear that [it] covers only information submitted online, . . . not information requested online but submitted offline." [FN165] This exception creates a potentially large loophole through which companies can circumvent COPPA strictures. [FN166] Moreover, the "personal information" referenced in ***661** COPPA is defined as "individually identifiable information about an individual collected online." [FN167] Asking a child about her age, gender, height, weight, grade in school, interests, habits, hobbies, pets, friends, zip code, even her first name (only) and then recording her preferences and movements online would not be susceptible to COPPA regulations as long as her first and last name, address, phone number, or other contact information was not solicited. [FN168]

Additionally, the Rule makes clear that schools can act as parents' agents, or as

intermediaries, between web sites and parents in the notice and consent process. [FN169] In an age of advertisements, corporate sponsorships, product placements, and Channel One in schools, this loophole is potentially cause for concern. [FN170] Companies may seek to trade cash for student access and data, and schools are empirically likely to acquiesce. [FN171] America Online ("AOL") has offered free service to schools nationwide, purportedly to build brand loyalty and create *662 a generation of future AOL customers. [FN172] AOL claims that no marketing information will be gathered on students because they will use only a first name and a password to access the service in school. [FN173] However, while it is possible that personally identifiable information will not be collected, it defies credulity that AOL will pass up a golden opportunity to collect aggregate marketing information about school children utilizing this "free" access. While few web marketers wanted to openly oppose the viscerally appealing concept of protecting children online, most argued that COPPA should impose the least restrictive consent requirements possible, and successfully opposed parental control of data after consent has been obtained. [FN174]

B. The European Union's Data Protection Directive

Ultimately, in terms of protecting the privacy of personal information, COPPA compares unfavorably to the European Union's Data Protection Directive ("Directive"). The Directive requires entities collecting data to inform citizens what their data will be used for, provide citizens free access to data about themselves, the ability to correct false information, and notice and opportunity to "opt out" of data transfers to third parties. [FN175] European citizens have the specifically enumerated right:

*663 [To] object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

[FN176]

The Directive is premised on "the fundamental idea that 'my' personal information is none of 'your' business." [FN177] It "treats privacy as a basic human right and seeks to protect individuals against violations of the right . . . and says to other countries that it is none of their business to intrude on the privacy rights of persons in the European Union." [FN178] By contrast, "the United States does not have a single, comprehensive privacy law or agency charged with administering such laws," [FN179] reflecting a nation more concerned with commerce and less with individual rights. [FN180] The Directive gives more data privacy protection to European adults than COPPA gives to American children. Possible explanations for the differences between the data privacy regulatory cultures in the United States and Europe include hypotheses that Americans are more trusting of the private sector; that Americans believe the mass media will expose market sector privacy abuses; that Americans believe technology can solve the problem; and that *664 Americans are more wary of government regulation. [FN181] Europeans, it is posited, prefer to err on the side of overprotection of personal data because they view informational privacy as a

fundamental right of citizens. [FN182] Americans, on the other hand, "are more likely to cherish the principles embodied in the First Amendment--which favors a free flow of information--as fundamental human rights." [FN183]

The European Union's Data Protection Directive is intensely disliked by American companies that do not want to comply with it when engaging in e-commerce overseas. [FN184] They are specifically concerned about provisions that give individuals and private organizations the right to sue companies that do not provide adequate privacy protections. [FN185] United States' commercial interests are pushing for the ability to have access to European data, while agreeing only to self-regulation, and to have "safe harbor" status for certain business practices. [FN186] These discordant views of privacy oversight are currently the subject of international negotiation. [FN187] Even if the safe harbor approach is adopted, as appears likely, Americans will not get the same privacy protections as Europeans, rendering us, from a privacy standpoint, "second-class citizens in [our] own country." [FN188]

***665 C. The United States' Approach to Privacy Protection**

The United States' legislative approach to informational privacy is best described as piecemeal. By way of illustration, cable subscription records and video rental records have statutory privacy protections, but medical records do not. [FN189] As a result of the gaping holes in privacy protection, information about us circulates widely without our control, or even our awareness:

Finding out what agencies have information on you is tricky--if not impossible. The number of bureaus that have the potential to get information on you has soared amid technological advances that have made data processing cheaper and faster than ever. The spread of personal information is also facilitated by so-called information brokers, who make it worth the major credit bureaus' while to sell data. These brokers buy data in bulk and then sell it in smaller, more affordable portions to other agencies. Smaller agencies have also been empowered by information-sharing with their clients. If you bounce a check at Macy's, for example, the department store will share that fact with a monitoring service. That service, in turn, will warn Bloomingdale's when you try and write a check there. [FN190]

Players in the information industry, who profitably buy, collect, and sell huge data banks of personal information about Americans, have successfully lobbied against government regulation of most of their practices. [FN191] The Clinton administration asserted that "U.S. companies should not be forced to give people access to personal information about themselves" and actively opposed the adoption of broad privacy safeguards. [FN192] When President Clinton spoke in favor of consumer *666 privacy, his focus was primarily on individual financial information and medical records, rather than general personal data. [FN193] While he has, on occasion, spoken in favor of expanding general consumer privacy, he has not backed his words with actions. [FN194] Quite the contrary, his administration recently declined to support a proposal by the Federal Trade Commission for Internet consumer privacy legislation. [FN195]

Members of Congress who express concern about data privacy seem primarily focused on potential privacy violations by the government and do not seem troubled by intrusions by commercial entities. *667 [FN196] Congress has promulgated statutory

restraints upon law enforcement's ability to collect data related to phone records, [FN197] cable subscriber records, [FN198] video rental records, [FN199] credit reports, [FN200] and medical records. [FN201] It also enacted the Driver's Privacy Protection Act, [FN202] which prohibits state motor vehicle registration agencies from disclosing personal information about its drivers without their express *668 consent. [FN203] These are all prohibitions on the "jackbooted thugs" of government and largely do not affect the jackboot-selling agents of commerce, except to the extent private entities acquire data from government sources. The Privacy Act of 1974, [FN204] the United States' most comprehensive privacy law to date, addresses the automation of records held on individuals by the federal and state governments, but not those gathered by private entities. [FN205]

1. Self-Regulation

In July of 1999, the FTC released a report entitled "Self-Regulation and Privacy Online: A Report to Congress." [FN206] The FTC concluded that "legislation to address online privacy is not appropriate at this time" because "self-regulation is the least intrusive and most efficient means to ensure fair information practices [online], given the rapidly evolving nature of the Internet and computer technology." [FN207] By May of 2000, however, the FTC appeared less enamored of self-regulation, and voted to ask Congress for new regulatory powers over collection and use of consumer information on the Internet. [FN208] The FTC actually floated a proposal for legislation to protect consumer privacy on the Internet, but it was rejected by both the Republican-*669 controlled Congress and the Clinton administration. [FN209] The FTC's newfound interest in consumer privacy originated not out of an independent concern for individual informational integrity, but as a result of trepidation that privacy concerns hamper the growth of online retail sales. [FN210] Private sector efforts at self-regulation have emerged, including "seal" programs such as those administered by TRUSTe, [FN211] the Better Business Bureau's Online Privacy Program [FN212] ("BBBOnLine"), and the Online Privacy Alliance. [FN213] Commercial web sites that carry an online "seal," a unique logo, purport to subscribe to a corresponding set of privacy principles articulated by the organization providing the seal. [FN214] Use of such seals is not particularly widespread at present. [FN215] *670 Moreover, purveyors of seals may be paid by sites to post their symbol, which presents an inherent conflict of interest. Giving a web site a poor privacy rating may lower consumer participation and the site's revenues. [FN216] In addition, the efficacy of TRUSTe in particular appears dubious. A security expert discovered that TRUSTe licensee RealNetworks [FN217] was secretly collecting personally identifiable information on what users were playing and recording from consumers using its RealJukebox software. [FN218] RealNetworks did not disclose its extensive information gathering practices in the long privacy policy posted on its web site, nor in the licensing agreement users approved when installing the RealJukebox program. [FN219] TRUSTe distinguished the RealJukebox software from the RealNetworks site where the software was downloaded. [FN220] TRUSTe maintained that the web site was what had earned the TRUSTe seal and the software available at the site was outside of the seal's purview. [FN221] TRUSTe's CEO has publicly conceded that even a site that collects consumers' e-mail addresses and then sells them to a direct-

marketing company could *671 "earn" the TRUSTe seal. [FN222] He also conceded that TRUSTe has never removed its seal from a site for bad behavior and that very few sites get rejected from the seal program. [FN223]

The pressure on privacy seal companies to keep their privacy requirements mild and corporate friendly is illustrated by an exchange between BBBOnline and eBay, [FN224] the online auction company. [FN225] After BBBOnline investigated a consumer complaint against eBay, it rendered a decision criticizing eBay for not informing eBay users what purposes their personal information was being used for in some contexts. [FN226] The decision concluded that eBay needed to take corrective action to conform to BBBOnline privacy policies. [FN227] In response, eBay stated that it believed that BBBOnline had "erroneously accepted" the consumer complaint, had "subsequently mishandled resolution of the complaint," and had "demonstrated its complete lack of understanding of both the Internet and software." [FN228] After pointing out that it far preferred the resolution of this issue proffered by TRUSTe, eBay concluded its diatribe against BBBOnline by announcing "[I]t is with great regret that eBay announces that it will withdraw from the BBBOnline program, should this matter not be satisfactorily resolved." [FN229] If other BBBOnline participants take criticism as poorly as eBay, BBBOnline will have to choose between maintaining a credible seal with fewer subscribers, or watering down its privacy policies and enforcement practices. Overall, there is little reason to hope that seal programs, as currently constituted, will advance informational privacy very far. [FN230]

***672 2. Asking Big Brother for Assistance**

Opinion polls have indicated the public's desire for government regulation of online data collection. [FN231] However, even if the government could be persuaded to protect consumer data, it is uncertain what the scope and nature of that protection would ultimately be. [FN232] Not everyone is comfortable having the government make decisions about who gets access to our personal information. As one commentator noted:

It's ironic that Americans are asking for privacy protection from the same government that has in the last few years expanded electronic surveillance beyond Richard Nixon's wildest dreams--always with an appeal to public fear and mistrust. Federal agencies are creating centralized databases to track every new job hire in the country (to catch illegal immigrants and deadbeat dads), to make sure that welfare recipients don't overstay their five years by changing states and to provide instant "terrorist" profiling to airport security agents. The country has not hesitated in the last few years to wipe out the civil liberties of whole swaths of the population in futile gropes for greater public security that's never attained. [FN233]

In the name of curbing crimes such as terrorism, identity theft, and retail fraud, the government actively thwarts sales and development of technology that would improve privacy in electronic communications. [FN234] The government often seems as eager as commercial *673 entities to collect information about citizens. [FN235] For example, it was recently reported that a company that built a national database of driver's license photographs received extensive financial support from Congress and technical assistance from the United States Secret Service. [FN236] In the closing

days of the 105th Congress, the Clinton Administration proposed that the federal government's "New Hires" database, ostensibly authorized to track down parents who were failing to pay child support, be made available to the Department of Education for tracking down defaulting student loan holders. [FN237] Personal information is as attractive to the government as it is to the private sector. [FN238] As one observer noted, "Now that financial data are compiled and stored digitally, it is cheap, easy, and tempting for the government to cast a wider and wider financial dragnet to build increasingly intrusive computer profiles of citizens." [FN239]

3. Bartering Information for Access

Along with asserting that collecting our data helps commercial interests serve us better and perpetuates "female empowerment," [FN240] web site merchants also argue that if consumers accept an offer for free content in exchange for personal information, there is an information exchange that does not infringe upon privacy interests. [FN241] This would be a reasonable position if the terms of the exchange are mutually understood and agreed upon, and if the freely conferred information is not subsequently divulged to others, nor used for any unintended, undisclosed purposes. However, as Jerry Kang noted, "For numerous reasons, such as transaction costs, individuals and information collectors do not generally negotiate and conclude express privacy contracts before engaging in each and every cyberspace transaction." [FN242] In a related vein, Paul Schwartz has pointed out that that the cyberspace use of personal data "helps set the terms under which we *674 participate in social and political life and the meaning that we attribute to information- control." [FN243] By this, he means that "consenting" to the terms and conditions of web site access or an Internet transaction superficially appears to represent an informed "exercise of self-reliant choice." [FN244] However, these terms and conditions are offered on a take-it-or-leave-it basis, which severely constrains consumer choice, and "locks in" a low level of privacy. [FN245]

Even if consumers were able and willing to bargain over collection and disclosure of their personal information in an intelligent and informed fashion, data collectors may, for efficacy and utility reasons, be disinclined toward negotiating with consumers in a transparent and straightforward manner. [FN246] American data merchants are generally loathe to rely exclusively on voluntary "information exchanges." This dislike is based on empirical evidence that when individuals are directly and openly confronted with a request for information, they are unwilling to part with it without compensation and may not agree to divulge it at all. [FN247] For example, people resist filling out online registration forms, which seem invasive, and do not have a real space counterpart. [FN248] As one commentator noted, "Imagine going to a 7- Eleven to buy a can of Coke, and having to fill out a registration form that asks you about marital status." [FN249]

Jerry Kang has persuasively argued that individuals do not generally have enough information to know the value of their personal data. [FN250] Perhaps we do not feel "robbed" when it is taken, but many people do feel invaded at some level. Recent studies have indicated that "Internet users are increasingly uncomfortable with the amount of personal data gathered by online companies . . . as online companies [are] becom[ing] more aggressive about collecting that information." *675 [FN251] One

study found that 87% of people online want "complete control" over their personal data. [FN252] Jerry Berman and Deirdre Mulligan recounted:

[S]everal recent incidents involving the sale and disclosure of what many perceive as less sensitive information indicate a rising of privacy concerns among the public. In recent years, a number of corporations . . . have learned the hard way that consumers are prepared to protest against services that appear to infringe on their privacy. In 1996, public criticism forced Lexis-Nexis to withdraw a service known as P-Trak, which granted easy online access to a database of millions of individuals' Social Security numbers. Also in 1996, Yahoo faced a public outcry over its People Search service. The service, jointly run with a marketing list vendor, would have allowed Net searchers to put an instant finger on 175 million people, all culled from commercial mailing lists. After hearing the complaints, Yahoo decided to delete 85 million records containing unlisted home addresses. During August of 1997, American Online ("AOL") announced plans to disclose its subscribers' telephone numbers to business partners for telemarketing. AOL heard loud objections from subscribers and advocates opposed to this unilateral change in the "terms of service agreement" covering the use and disclosure of personal information. In response, AOL decided not to follow through with its proposal. [FN253]

Moreover, an April 2000 study by a market research firm determined that "[a] notable 92% of online households agree or agree strongly with the statement, 'I don't trust companies to keep personal information about me confidential, no matter what they promise.'" [FN254] This mistrust is not misplaced. By way of illustration, "Gizmoz" is a technology that "uses consumers to pass along marketing messages and content embedded in email to develop a 'viral network.'" [FN255] "Viral *676 marketing" is a technique used to spread information from person to person like a virus, so that consumers are provided with incentives to effectively become part of a company's sales force, and pass marketing messages to their friends and acquaintances. [FN256] Gizmoz's technology then leaves an electronic trail that marketers can follow to see where content and promotions go. [FN257] A major Gizmoz investor publicly asserted that "privacy is a key concern of Gizmoz and the company does not request nor pass on private information about individuals." [FN258] Gizmoz's terms-of-service agreement tells a very different story, stating that users "should not have an expectation of privacy in (their) account." [FN259]

Allowing a user to opt in to a data collections scheme puts a web swimmer on notice that she is being watched and followed, and gives her the opportunity to obfuscate or to say no to such practices. However, if she accedes to a site's practices, knowing that her "clickstream" is being observed and recorded will cause her to self-censor, compromising the data collected. [FN260] Passive, sub rosa data collection techniques are therefore preferred by database assemblers to straightforward requests for personal information, as they do not cost anything, nor draw attention to the nature or scope of the data mining that is occurring. Passive collection may also prove more accurate, as "[s]urvey after survey has indicated that online users resent being asked for personal information, don't trust companies that do ask for such information and often--as much as 25 percent of the time--enter false information when prompted for personal details." [FN261]

Ironically, the commercial enterprises so eager to collect or take advantage of

consumer data collections hypocritically object when data is collected by others about their consumer bases or commercial activities. In some instances, web publishers and advertising agencies quarrel with each other concerning exclusive ownership of our *677 data. [FN262] Once companies have assembled databases, many would like to impose criminal penalties on others that steal "their" information. [FN263] Of course, even though corporations may not be able to protect their data by invoking a right to privacy, they are able to do so using contract, tort, and intellectual property law.

[FN264] As Jerry Kang has pointed out:

[A] potent array of unfair competition, trade secret, patent, trademark, and copyright law, in addition to confidentiality agreements, support an institution's ability to control various types of information identifiable to itself. In addition, collective entities often have the wherewithal to employ self-help security measures so that information in their control flows only in ways they choose. [FN265]

The possibility of giving individuals similar tools to control our personal information is explored at the end of this article.

VIII. The Propertization of Privacy: Privacy As a Marketable Good

A. Ad-Blocking Software

Web software to block advertising is already available and attractive to some web swimmers. In addition to keeping advertisements off their screens, "ad- blocking software can mean faster performance. Files that contain ads laden with graphics and animation take far longer to load than files with text." [FN266] Ad-blocking utility programs sometimes include firewalls intended to prevent intrusions by hackers and other features that limit or prevent web sites from collecting "clickstream" data through cookie files. [FN267]

Not surprisingly, most web site operators and advertisers generally both fear and oppose ad-blocking software, maintaining that it will "clog their revenue stream, and challenge the fundamental structure of the emerging Internet industry." [FN268] Use of such software is characterized not only as unfair but practically bigoted. As one webtrepreneur *678 stated, "The audience already allows overt advertising in mainstream media, so they must be tolerant in the context of the online model as well." [FN269] Another maligns the desire for privacy as deviant and dishonest, analogizing ad-blocking to shoplifting, and asserts that his site uses "software code that prevents anyone using an ad blocker from even logging onto the company's site." [FN270] Ad- blocking software poses very high risks for some companies. For example, when CDNow's marketing budget was divided by the number of people who make purchases from the site, the result indicated that the company was spending \$45 in advertising to attract each paying customer. [FN271] Some data collection techniques are kept intentionally surreptitious, so that web swimmers seeking data privacy will not even know what to avoid. For example, one simple animated mouse pointer has been secretly tracking its users' web travels on behalf of companies such as Yahoo, Lycos, theglobe.com, Warner Bros., Universal Studios, RealNetworks, MindSpring, M&M/Mars, MSNBC, Energizer, CNET, Comedy Central, United Media, and Universal Press Syndicate. [FN272] As is sadly typical with many electronic data collection techniques, this practice was exposed, rather than disclosed.

If an independent software analyst had not figured out that Comet Systems was using its cursor software for web tracking purposes, the public would still be unaware that this was occurring. [FN273]

B. Cookie Disablement

"Cookies" in the cyber context are data files created on our own computer hard drives when we visit a web site. [FN274] Cookie files contain unique tracking numbers that can be read by the web site, and advertising servers, tracking us as we swim from one web page to another. [FN275] The technologically proficient can set our Internet browsers to refuse *679 cookies, but sites that use cookie files, which includes almost all commercial sites, will then refuse us access. [FN276]

C. Consequences of Self Help in Protecting Our Privacy

Average web swimmers are aware of some technological solutions to data collection techniques, such as ad-blocking software and cookie disablement. These solutions theoretically exist for people who like to look at advertisements, but do not want their movements through commercial cyberspace tracked and recorded, as well as for those who prefer to avoid advertisements altogether. However, such "self help" is easily thwarted by web site operators who will simply refuse access to web swimmers who will not submit to banner ads and cookie files. [FN277] Unless web sites are required to accept visitors who block ads and/or refuse cookies, technology will not effectively or consistently protect consumer privacy without effecting access. Given the opposition to regulating the Internet, which flows from so many quarters, imposition of such requirements seem highly unlikely. Similarly, use of "anonymizers," [FN278] to the extent they are even held to be legal, could be blocked by web sites. [FN279] Web sites can require confirmation of identity before allowing access if they so choose. Some types of cyberspace transactions make anonymity impractical anyway. For example, when we purchase goods and services, we have to pay for them and provide an address for delivery. This requirement could be avoided through extensive pre-planning, but most people are not likely to be prepared to shoulder the burdens of losing access to some sites, navigating the *680 complexities of an anonymous payment system such as digital cash, and obtaining real space "mail drops" for delivery of tangible goods, in order to avoid disclosing personal data online. As Paul Schwartz observed:

For the current online industry . . . personal information largely has the quality of nonrivalrous consumption, which means that one firm's utilization of it does not leave any less for any other company. As a result, almost all major Internet enterprises and computer companies benefit from developing standards, including new technology, that preserve the current status quo of maximum information disclosure. [FN280] Data collections will lock in low levels of privacy through collaborative standard setting, forcing consumers to choose between informational privacy and the Internet. [FN281]

D. Buying Back Our Privacy

Another technological solution involves companies called "infomediaries." These companies will, for a price, provide security mechanisms that help consumers "regain

control" over who purchases their personal data and for what purpose. [FN282] This service takes the quixotic experience of having to pay extra to have a phone company not publish your telephone number to new extremes. It would require us to buy back control of our personal data and means that we would have to make decisions about how much information privacy we can afford. It would also force us to trust a commercial entity to manage our personal information for us and to forgo the enticing profits that exploitation of our data would offer.

Moreover, relying upon technology or technological changes to prevent the distribution of personal data is likely to provide more information privacy for wealthier, better educated web swimmers, and less for poorer, less computer savvy members of the population. Some "privacy rating" services are available to consumers for free, but are either beholden to the sites that they rate for income, which creates a conflict of interest, or they subject users to advertising and give marketers *681 access to user lists. [FN283] As Peter Swire and Robert Litan have noted:

It can be daunting for an individual consumer to bargain with a distant Internet merchant or a telephone company about the desired level of privacy. To be successful, bargaining might take time, effort, and considerable expertise in privacy issues. Even then, the company might not change its practices. Even worse, a bargain once reached might be violated by the company, which knows that violations will be hard for the customer to detect. [FN284]

E. Opting Out of Data Collection

Another purported solution to protect privacy compromised by data collection is allowing a web swimmer to "opt out" by filling out a form (online or on paper) asking web entities not to disseminate personal information. [FN285] This option places the burden on consumers to be constantly vigilant and possibly fill out a form for every web site visited, which could quickly get onerous. [FN286] Compounding the arduousness of any attempt at uniform and consistent opting out is the fact that some sites for services may require consumers to assert "privacy preferences" more than once. [FN287] For example, AOL requires subscribers desiring personal information privacy to fill out an opt out form once a year. [FN288] If they do not submit timely annual renewal forms, their privacy preferences "expire" and information collected from their AOL usage may be sold to marketers and other interested parties. [FN289] Additionally, large-scale data compiler DoubleClick's opt out system was recently determined to be "ineffective" with certain versions *682 of the Netscape Communications web browser. [FN290] Preferences for high security were reverting back to low security without notice to the user. [FN291] People who had affirmatively opted out of data collection schemes were secretly, and involuntarily, opted back in to them. [FN292]

Additionally, opting out of a data collection and distribution framework may fence the privacy-seeking web swimmer off from content or other perquisites of a site. The iWon website's so-called privacy policy aptly illustrates this capability. [FN293] One may access the website without providing personally identifiable information, but failing to provide such information renders one ineligible for the "free" daily, weekly, monthly, and yearly drawings and prize giveaways, the only reason most people would access the site in the first place. [FN294] The iWon Privacy Policy site touts its

TRUSTe seal and then states in pertinent part:

During registration, iWon collects personal information including your name, address, email address, birth date, gender, zip code and phone number. After providing iWon with this information, you are no longer anonymous. You do not have to provide any personal information to use the iWon service. However, if you choose to withhold requested information, you will not be registered and you will not earn entries into the iWon Sweepstakes when using iWon. In addition, we may not be able to provide you with some of the other services dependent upon the collection of such information, such as a personalized home page. [FN295]

The entire policy is rather lengthy and discloses that iWon will do just about anything it pleases with our data, including matching it with personally identifiable consumer data collected by other entities and selling it. [FN296] The company is therefore unlikely to jeopardize its TRUSTe seal by not complying with its stated privacy policy, as it would be virtually impossible for iWon to do anything that ran afoul of its stunningly broad self proscribed privacy mandate. Just in case iWon changes its mind, it reserves the right to modify its privacy policy at *683 any time. [FN297] The only way site users will learn of the change is by constantly monitoring the policy and comparing it to earlier versions. [FN298]

F. Opting In

The mirror image of "opt out" is "opt in," which puts the burden on a data collector to get an individual's approval of the data harvesting. Mandatory opt in is one approach to privacy promoted by some online privacy advocates. However, when and how it could be implemented is unclear. A federal appeals court recently concluded that an FCC regulation requiring phone companies to secure opt in style consent from customers before using their personal information for commercial purposes violated the phone companies First Amendment free speech rights. [FN299] Moreover, an opt in scenario would be efficacious only if full disclosures of the nature and scope of the data collection were made, with the ability to opt out of any objectionable portions of whatever plans a web site has for the data.

If sites can exclude web swimmers unwilling to fully opt in to data collection schemes, this approach will not solve anything. We will be required to opt in before we can access content and fully utilize desirable aspects of the Internet. Any freedom of choice associated with opting in will be illusory. Moreover, an opt in approach does not solve the problems posed by our inability to value our own data. [FN300] It also raises legitimate concerns for data collectors about the accuracy of data that is permissively and transparently obtained. [FN301]

IX. Machiavelli in Cyberspace: The Possibility That Another Wrong Can Make Things Right

Politicians and judges who may be unwilling to safeguard personal privacy are downright enthusiastic about protecting intellectual *684 property. This enthusiasm, if appropriately channeled, could allow the intellectual property framework to provide structural support for personal information privacy. The definition and scope of intellectual property is expanding at a rapid rate. In addition to the apocryphal "better mousetrap," patents now "protect" plants, animals, and even business methods.

[FN302] Copyrights accrue to minimally original expressive works at the moment of creation, usually lasting 70 years from the deaths of their creators. [FN303] Copyrights are increasingly treated as ordinary chattel. [FN304] Both patents and copyrights can be bought, sold, or licensed like tangible goods. [FN305] Trademarks have evolved into intangible commercial property that can be defended not only against infringement, but also against trespasses such as "blurring" and "tarnishment." [FN306] Product packaging and the not-particularly-original layouts and design schemes of stores and restaurants are protectable as "trade dress." [FN307] Ideas, methods, inventions, processes, and even vendor and customer lists that are not eligible for formal intellectual property protection can still be proprietary as "trade secrets." [FN308] Initiatives to more rigorously protect data collections, which are already partially covered by copyrights, have been unsuccessful, but are still ongoing. [FN309]

This expansion of the scope of proprietary intellectual property is detrimental to society, and fundamentally wrong. However, the tide seems irreversible. Jessica Litman observed that:

Commodification is the preeminent engine of progress. Transforming ephemeral figments into saleable property is a patriotic act, and the fact, without more, that an offer to sell something will *685 find customers is reason enough to sanction its appropriation from the commons. There has been inexorable pressure to recognize as an axiom the principle that if something appears to have substantial value to someone, the law must and should protect it as property. [FN310]

If the rigid commodification of information is indeed inevitable, perhaps it is time for individuals to appropriate the intellectual property framework so eagerly constructed by corporate interests, and to seek control of the data we generate and a share of the proceeds this information produces. We must assert proprietary interests in ourselves and hoist consumer data merchants by their own cyber-petards. We must definitively establish that consumer information is intellectual property that belongs to the consumers themselves. Rosemary Coombe has trenchantly observed that:

To read a book, listen to a song, scan an encyclopedia, pass along a newspaper article to a friend, exchange recipes and furniture-finishing instructions with a neighbor--these were communicational activities encouraged within liberal democracies with an Enlightenment faith in the progress of arts and sciences. The same activities may well be deemed forms of theft--illegal trespassing upon private property--in the digital environment. [FN311]

If the expanding scope of intellectual property will burden our ability to share with each other in cyberspace, then we should not freely share our information with business enterprises that drive this expansion of intellectual property rights in cyberspace and then claim our data as their intellectual property, simply by virtue of their having collected it from us. Our rights to our own personal information can be deemed to flow from an amalgam of the law of copyrights, trademarks, and the right of publicity. When Congress inevitably passes a sui generis data protection scheme, ideally we will have a specific, legislatively enacted ability to reap the financial rewards of our personae. [FN312]

A. Rewarding the Sweat of the Wrong Brows

Legislation under consideration seeks to establish the rights to our data, not in ourselves, but in the first corporate entity to gather it. The legislation would prevent the commercial extraction of use of quantitatively or qualitatively substantial parts of a collection of information,*686 gathered or maintained by another, so as to harm the actual or potential market for a product or service containing that collection of information. [FN313] In other words, this data protection legislation would give the first entity to collect our personal information a cause of action against a second entity that "extracted it" from the collection without permission. Our collected personal data would therefore transmogrify into the first entity's property. These property rights would putatively arise as compensation for the "sweat of the brow" generating labor that the first entity engaged in while collecting our data. [FN314] Data merchants assert that they own our data by virtue of their investment in building and developing "information assets." [FN315] Jessica Litman stated:

Data mining--the collection, extraction, correlation, categorization, and sale of identifying personal data--claims to be a new engine of breathtaking economic growth. The miners are seeking intellectual property protection for their collections of information about whose eyeballs are valuable to whom. It is no wonder that advertisers feel proprietary about our eyeballs. From their viewpoint, those are their eyeballs. They paid for them. [FN316]

But what about the perspiration generating efforts we exude while "creating" our data, living our lives? We must work to create employment records, visit (and remunerate) physicians to produce medical records, register for Social Security numbers, pay to obtain and maintain phone numbers and e-mail accounts. A single real space visit to the Department of Motor Vehicles to obtain a Driver's License or register a car requires a lot more time and effort than compiling thousands of cookie file results. Why should collecting data about the arrival of a new baby give birth to a property right in the information, if 24 hours of excruciating labor does not? Why, when we ask a company*687 where it obtained personal information about us, should we accept answers like "it's proprietary" or "we won't tell you" ? [FN317]

B. Turning a Wrong Into a "Right"

Simply put, if information about us is to be bought and sold, the initial purchase should be from us, since we are the ultimate content providers. If intangible property rights are rewards for the effort expended in creating the thing to be protected, we are entitled to ownership of our personal information. [FN318] As owners, we should get royalties every time our data is used or transferred for commercial purposes, and these transactions should transpire only with our affirmative consent. Like companies protecting their intellectual property, we ought to be further entitled to veto power over use of our names and attendant information. [FN319] With this power, we can prevent our names from being used by companies that annoy or offend us because "the unauthorized use of an individual's persona potentially poses the maximum harm to [that individual] when the persona is being appropriated in an objectionable context or for an objectionable purpose." [FN320] Europeans may have the precept of privacy to defend themselves against direct marketers, but here in the United States, apparently only property rights get respected and protected. For this reason, we need to assert and

defend property rights in ourselves. While ***688** the common law tort-based misappropriation doctrine might be of some use to protect our data, if corporate intellectual property owners can seek recourse in the federal courts, then we should be able to also. [\[FN321\]](#) The legal and social mores that create an information subsidy in favor of data collectors should end.

Several economists have proposed "granting individuals property rights in their personal information as a way of resolving the data privacy controversy." [\[FN322\]](#) In discussing this proposal, Pamela Samuelson observed:

Given the fact that the market in personal information is already very substantial and personal data are commercially valuable, the idea of granting individuals property rights in their personal information is perhaps not as radical as it might initially seem. Propertizing personal information would merely extend this market and give members of the public some control, which they currently lack, over the traffic in personal data. [\[FN323\]](#)

Samuelson has also articulated some of the difficulties she sees in recognizing property rights in personal data, including the need for a complex bureaucratic infrastructure to enable efficient market transactions in data, and doctrinal conflicts with rights-based conceptions of privacy. [\[FN324\]](#) She has expressed particular concern that a property rights approach to personal data protection would establish a new form of intellectual property right in information which would be at odds with fundamental intellectual property principles (promotion of ***689** science and the useful arts), further straining the already fragmenting coherence of intellectual property law. [\[FN325\]](#)

Instead, she favors consideration of alternatives for promoting information privacy such as promulgation of modified trade secrecy default rules. [\[FN326\]](#) She has asserted that, "The general rule of trade secrecy licensing law is that if the licensor has provided data to another for a particular purpose, the data cannot be used for other purposes without obtaining permission for the new uses." [\[FN327\]](#) Licensing law, she has argued, generally accommodates the reasonable expectations of the parties, allows reasonable enforcement of implicit limitations on use where appropriate, and permits revocation for material breach of terms. [\[FN328\]](#)

Along similar lines, Eugene Volokh has expressed a preference for a contract-based approach to information privacy, at least as an alternative to the propertization of personal data. [\[FN329\]](#) Volokh's particular concern is the detrimental effect on free speech that ownership of information can have. [\[FN330\]](#) Volokh has noted that promises not to reveal information in the form of contracts not to speak are enforceable, and do not conflict with First Amendment free speech protections, even when such contracts are implicit. [\[FN331\]](#) He also asserted that statutory default rules could clarify obligations concerning the use and disclosure of data, and are preferable to leaving the courts to guess about what was assumed or expected with respect to personal information. [\[FN332\]](#) Volokh concluded that the great free speech advantage of the contract model of information privacy does not endorse any right to stop people from speaking about each other. [\[FN333\]](#) Instead, he argued, it simply endorses a right to stop people from violating their promises. [\[FN334\]](#) He noted that there are two limitations to this approach: people can restrict use and disclosure of information ("speech") only ***690** by parties with whom they have a contract to do so; and parties

can waive (or compel waiver) of speech-restricting contract terms. [FN335] While both Samuelson and Volokh raise important concerns about propertizing data, it is not clear that a contract or licensing based approach can truly avoid the pitfalls they describe. One cannot usually bargain over the sale or lease of something without conceptualizing it at some level as a good or service. To the extent personal data is treated as a good in licensing or contract negotiations, it will assume the characteristics of intangible personal property. As a result, courts addressing personal information contract or licensing disputes may then import both personal property law and intellectual property constructs in an attempt to define and circumscribe the subject of the contract and the meaning of its terms. While a straight property based approach is not without drawbacks, at least a governing body of law already exists, incoherent as it may sometimes be.

Until database (or other) legislation provides us property rights in our own personal information, or an equity-minded court recognizes that we had them all along, we can assert the right to overlapping intellectual property protection classifications currently available. Fortuitously for these purposes, corporate interests have so widened (and some would say corrupted) the scope of intellectual property categories that personal information requires little doctrinal stretch for protection. [FN336]

Donna Rawlinson MacLean, a poet and waitress, recently applied for a patent in the United Kingdom on an invention she created and called "Myself," explaining, "[I]t has taken thirty years of hard labor for me to discover and invent myself, and now I wish to protect my invention from unauthorized exploitation, genetic or otherwise."

[FN337] While she may very well be novel, useful, and nonobvious, patents are the mode of intellectual property that are least adaptable to personal information. [FN338] Other forms, discussed below, seem to have the potential for being far more accommodating.

***691 X. Legal Underpinnings: Copyrights, Trademarks, and the Right of Publicity**

A. Copyrights: Rights in Our Personal Data Compilations

Whether or not we traditionally view ourselves as the expression of ideas, our existences are at least minimally creative and original. [FN339] We are in every sense the "author" of our personal biographical data, and so should automatically own our personally identifiable, personally generated information. [FN340] It is bedrock copyright doctrine that discrete bits of factual information are not in and of themselves copyrightable. [FN341] However, when factual information is incorporated into an original compilation, it acquires copyright protection. [FN342] Compilations are defined as a collection and assembly of preexisting materials or of data that are selected, coordinated, or arranged so that the resulting product constitutes an original work of authorship. [FN343] The compilation copyright construct is broad enough to embrace mail order catalogues, yellow pages data in phone books, and a guidebook of used car values, so there is no doctrinal impediment preventing the construct from encompassing personal data compilations. [FN344]

While our individual "facts" may not be copyrightable, they are not independently valuable either. [FN345] No entity can effectively exploit our income ranges without

e-mail addresses to "spam," or real space addresses to target with catalogs. Most would prefer to know our gender and a host of other variables. Each component of our personhood may be singularly unprotectable, but we select, coordinate, and arrange our lives at great effort and expense, and our investments *692 should be preserved. [FN346] We therefore deserve protection as compilations. [FN347] Individual data compilations do not, as a policy matter, appear to require the lengthy term assured to ordinary copyright. Few compilations will have value after the compiler--the person living the life that is reflected in the data--expires, severely limiting her earning and spending capacities and making her data irrelevant. However, all copyrights receive a lengthy term of protection regardless of the social or economic value of the underlying work. In the event that post mortem personal data proves valuable, for research purposes or otherwise, we ought to be able to devise ownership of our information to our heirs, rather than allowing companies to reap a free "public domain" data windfall. If unlicensed use of personal data occurs, especially if it leads to unsolicited commercial contacts, statutory damages could be an efficient remedy, so long as awards are sufficiently large to serve as an effective deterrent. Large-scale, intentional, non-permissive use of personal data could, like other copyright infringements, be criminally sanctioned. [FN348]

B. Trademarks: Rights in Our Personmarks

As one commentator has observed:

Companies have successfully claimed trademark rights in the decor of a restaurant, an artistic style of painting, the design of a golf course, the shape of a faucet handle, the diamond shape of a lollipop, the unique registration process of a toy fair, the shape of a mixer, and the design of personal organizers [FN349]

It is hardly hyperbole to suggest that, against a backdrop of word and symbol ownership, one ought to be able to assert independent Lanham Act [FN350] rights in her name, phone number, and "snail" and e-mail addresses. They are as unique and perform as much of a distinguishing, source-identifying function in commerce as do trademarks, servicemarks, and trade dress. Famous people have already used the Lanham Act to protect "personas" in the context of the "right of publicity," which has roots in both privacy and property doctrines. [FN351] *693 Courts have recently "relied on trademark-like rubrics to uphold claims to exclusive rights in names, faces, voices, gestures, phrases, artistic style, marketing concepts, locations, and references." [FN352]

The intangible property right in the personal information of celebrities and non-celebrities alike could, for clarity's sake, be called "personmarks." Trademarks are protectable for as long as they continue to be used in commerce. [FN353]

Personmarks should therefore receive protection for as long as the data is "in use," meaning accurately reflecting a sentient being who is immersed to some degree in the stream of commerce, which is to say, alive.

When unlicensed use is made of a personmark, infringement awards could reflect the varying worth of personal data compilations. If we indulge in indiscriminate licensing, this would reduce our damages, because if we have agreed to receive solicitations from a wide array of companies, a few unlicensed mark-infringing solicitations would be less injurious to us than to a person who inflates the value of her data by restricting

access to it.

Persuasive arguments have been made against the propertization of trademarks. For example, Mark Lemley has written:

[P]ropertizing trademarks comes at a rather significant cost to society. Sometimes that cost takes the form of lost opportunities: Important political and social commentary and works of art may be suppressed entirely. It may also take the form of higher prices: When we protect the design of products as trademarks, we prevent competition in the sale of those products, and the price goes up accordingly. Other social costs are more diffuse, but no less real: Our language and our culture are impoverished when we cannot use the most familiar words to discuss--or make fun of, or criticize--the products and companies that are the basis of our economy. At the very least, it becomes inconvenient to do so. And perhaps most important, trademark licensing is expensive. The more we propertize, the more transaction costs we impose on everyone. Companies and individuals will have to hire more lawyers, delay introducing their products, and spend money in merchandising fees to acquire the rights to use words, logos, or product configurations. Because trademarks so often overlap, propertization may also reduce certainty, making trademark searching and clearance more difficult and leading to more litigation. [FN354]

Lemley is absolutely correct. A personmark scenario might impose costs upon society quite similar to those he described. However, it would also bring benefits, such as promoting broad personal information *694 privacy and conferring upon individuals the same ability to own and control information that companies have. Given that the data at issue is already propertized to a substantial extent, personmark protections might not significantly exacerbate an already burgeoning propertization trend. They would certainly fragment and complicate the ownership picture, increasing commercial transaction costs. However, if society can tolerate ownership of information by companies, there is no compelling reason not to accord analogous property rights to individuals. To the extent that any resulting commercial friction results in a general, broad-based reconsideration of the trend toward the propertization of trademarks, society will benefit.

C. Publicity Rights for Pre-celebrities

Celebrities have state law based control over their personas [FN355] and a federal right to publicity may be established in the future. The right of publicity is an increasingly robust doctrine, wafting from the otherwise withering privacy penumbra. [FN356] It ostensibly protects individuals from misappropriation of their names and likenesses and has been judicially extended to nicknames, signatures, physical poses, characterizations, singing style, performance style, vocal characteristics, frequently used phrases, mannerisms and gestures, and body parts, if found to be distinctive and publicly identified with the pertinent individual. [FN357] "Personal attributes are . . . treated just like business attributes." [FN358] If famous people can claim and profit from a right of publicity, then this right should be available to everyone. [FN359] We are all in some sense "pre-celebrities." [FN360] Our data can be deemed unequivocally distinctive and publicly identified with us as individuals. In fact, the unauthorized use of a private person's photograph impelled *695 the right of privacy decisions almost one hundred years ago that are now viewed as the origin of the right

of publicity doctrine. [FN361]

Attorneys for celebrities who assert property rights in themselves characterize those who utilize or reference some audio or visual aspect of the celebrity without permission as "pirates who rob famous people of their own chances to market themselves and control how they are depicted." [FN362] This characterization of personal characteristics as wealth that can be "robbed" by "pirates" helps illustrate the degree to which the right of publicity is propertized. There is no reason that the right of publicity cannot apply to all individuals, celebrity or not, who want to prevent unwanted commercial exploitation and protect against usurpation of the investment that they have in their own individual characteristics. [FN363] As celebrities successfully seek to prevent commercial exploitation of their individual persona, we should also have the ability to prevent unlicensed, commercial exploitation of our own individual attributes. As Alice Haemmerli articulated:

As to whether a person should be able to claim a property right in the use of her objectified identity, there is no logical reason why she should not and every reason why she should: 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? [FN364]

The right of publicity has been resoundingly criticized on several grounds. The argument against the right of publicity that most resonates with this author is the manner in which publicity rights facilitate ownership, censorship, control of popular culture, and the making of social meaning. [FN365] Michael Madow provides the following (lengthy but worthwhile) example:

A few years ago, a bill was introduced in the New York Legislature to create a broad and descendible right of publicity. During hearings on the bill, some of the testimony referred to a greeting card, said to be sold chiefly in gay bookstores. The card bears a picture of John Wayne, wearing cowboy hat and bright red lipstick, above the caption, "It's such a bitch being butch." Wayne's children, *696 among others, objected to the card not only on the ground that its sellers were making money from The Duke's image--money that should go to them, or, in this case, to the charity of their choosing. They objected also, indeed primarily, because in their view the card was "tasteless" and demeaned their father's (hard-earned) conservative macho image. To his children, as to most of his fans, "John Wayne" epitomizes traditional America's mythic and idealized view of itself, its history, and its national character. What Wayne stands for--what his image means in the mainstream cultural grammar--is rugged individualism, can-do confidence, physical courage, and untroubled masculinity. That is the "preferred meaning" of "John Wayne." It was on this preferred meaning that [then] President Bush drew easily and effectively in communicating his military plans in the [Persian] Gulf. It is on that meaning, too, that Wayne Enterprises drew when it licensed the Franklin Mint to sell (for \$395) a "serially numbered, non-firing" replica of the .45-caliber automatic pistol that Wayne "carried in so many great military films." Nevertheless, against-the-grain readings of John Wayne are also possible. For instance, in a course on how to survive as a prisoner of war, the U.S. Navy uses the term "John Wayning it" to mean trying foolishly to hold out against brutal torture. The particular greeting card that Wayne's children and others objected to so strenuously represents an even more subversive inflection of Wayne's image. The card uses his

image to interrogate and challenge mainstream conceptions of masculinity and heterosexuality. It recodes Wayne's image so as to make it carry a cultural meaning that presumably works for gay men, among others, but which Wayne's children (and no doubt many of his fans) find deeply offensive. If the New York Legislature were to make John Wayne's right of publicity descendible, however, it would confer on Wayne Enterprises the power to determine that this particular appropriation of the John Wayne image is "illegitimate," and to enforce that determination by denying a license to the greeting card maker. Wayne Enterprises would henceforth have the power to fix, or at least try to fix, the meaning that "John Wayne" has in our culture; his meaning for us. [FN366]

Jessica Litman similarly observed that "'Mickey Mouse,' 'Twinkies,' 'Star Wars,' and 'Spam' are trade symbols, but they are also now metaphors with meanings their proprietors would not have chosen. They got that way in spite of any advertising campaigns because the general public invested them with meaning." [FN367] Because society broadly constructs and adopts these metaphors, the owners of the pertinent trademarks cannot readily appeal to the courts to enjoin their use. However, as is illustrated in Madow's John Wayne anecdote, attempts are sometimes made to use right of publicity-based litigation *697 to control the meaning of societal icons. The possibility that such efforts could succeed is disturbing.

However, self-ownership of personal information poses few risks in this regard. Sheldon Halpern has argued that protection of the right of publicity is not a balancing "between the rights of the public at large and a fortuitously placed individual; the choice is between the individual to whom that associative value attaches and a stranger to the process who would make money out of it." [FN368] This "associative value" is derived from fame, and celebrity is exploited differently than the personal information of ordinary individuals. Celebrity generates economic value in three central ways: sales of information about the lives and activities of celebrities (news stories, biographies, interviews, etc.), sales of merchandise bearing the names and identifiable characteristics of celebrities (clothing, posters, toys etc.), and celebrity advertising and endorsements directed at selling collateral products. [FN369] In other words, celebrity is used to sell goods and services to us, the non-famous. Our personal information is collected for the exact opposite end, to persuade us to spend our money in particular ways. Unless aggregated, it is not likely to have broad meaning or to serve as the basis for far-reaching meaning making. Once compiled, however, the analysis changes because aggregate data about even non-famous individuals is very meaningful and important to the creation and alteration of meaning. To the extent that corporate entities usurp the meaning derived from this data for commerce purposes, perhaps we lose only our ability to be targeted so precisely.

It is possible that power over our own personal "publicity" may also prevent us from organizing, identifying others with similar interest, and speaking with unified voices. However, as Jerry Kang has pointed out:

The commerce argument [against information privacy], presumes that privacy necessarily entails information blockage. But this is not so. If individuals will truly benefit by releasing their personal data . . . they will rationally choose to do so.

Information privacy does not mandate informational quarantine; it merely requires that the individual exercise control within reasonable constraints over whether, and

what type of, quarantine should exist. [FN370]

*698 We will, therefore, have to trust ourselves to freely and willingly disseminate our data enough to keep our social and political connections.

Ironically, in some respects, the right of publicity does offer ordinary folks some protections it does not provide celebrities. The "newsworthiness privilege" [FN371] underpinning "celebrity journalism" and so-called tabloid television effectively negates a celebrity's right to personal privacy. Whereas, the rest of us, when acting in non-newsworthy fashion, do have a cognizable, if unsubstantial, right to be free from public disclosure of our most intimate affairs. [FN372]

Using the right of publicity as a mechanism for gaining control over our personal information has not yet met with success in the courts. In one case that generated a fair amount of press, one individual attempted to assert a property-like right in his personal information using state privacy law and a right of publicity theory. [FN373] In 1995, Ram Avrahami unsuccessfully tried to recover actual and punitive damages from U.S. News & World Report after it sold his name and address to two publishing companies. [FN374] He argued that his name was his personal property because the Virginia General Assembly "established and protected a person's property right in his own name" when it promulgated a state Privacy Act. [FN375] The Act states (in pertinent part):

Any person whose name, portrait or picture is used without having first obtained the written consent of such person . . . for advertising purposes or for the purposes of trade, such persons may maintain a suit in equity against such person, firm or corporation so using such person's name, portrait or picture to prevent and restrain the use thereof. [FN376]

*699 He also cited Virginia Supreme Court cases that stated that this statute creates a property right in one's name and likeness. [FN377] His claims were primarily privacy based, but ultimately unpersuasive to a court that viewed his injuries as trivial. [FN378]

Nor are we likely to be accorded privacy rights in our likenesses. When South Carolina Attorney General Charles M. Condon sued a company that was compiling a database of driver's license pictures comprise of 3.5 million digital photographs, a state judge ruled that the photo database was "no more intrusive on the privacy of an individual than showing the driver's license itself." [FN379]

More ominously, the Federal Trade Commission tried to protect consumer privacy, promulgating rules that prevented telephone companies from using customer information (such as phone numbers called and phone services subscribed to) without consumer consent. [FN380] The Tenth Circuit Court of Appeals held that these regulations violated the First Amendment by interfering with the phone companies' ability to engage in commercial speech with customers. [FN381]

XI. The Impact on Free Speech

Eugene Volokh recently wrote an interesting article about the burdens information privacy laws can place upon the exercise of free speech. [FN382] In pertinent part, Volokh addressed the idea of assigning people a property right in their personal information, and expressed concern that this would inhibit the beneficial flow of information *700 through society. [FN383] Though acknowledging that the Supreme

Court has found that the speech restrictions imposed by intellectual property rights are constitutional, he asserted that the Court has stressed that intellectual property owners do not have the power to suppress facts. [FN384] He argued that this is a critical distinction, because, in his view, granting individual property rights in personal information would bestow upon them the undesirable and unconstitutional capacity to suppress facts. [FN385]

Volokh supported his argument that First Amendment jurisprudence does not allow intellectual property owners to suppress facts by citing Supreme Court cases that seem to stand for this proposition. [FN386] In the copyright context, Volokh relied upon *Harper & Row v. Nation Enterprises*, [FN387] which certainly contains strong language about the Copyright Act's differentiation between copyrightable expression and uncopyrightable facts and ideas. What the case does not do, however, is offer any meaningful guidance about distilling one from the other. The *Harper & Row* case concerned a "purloined" copy of former President Gerald Ford's memoirs, which *The Nation* described and reviewed in a published article, without authorization, prior to planned publication of an excerpt of the memoir in *Time* magazine. [FN388] *Harper & Row*, which owned the memoir copyright, successfully brought a copyright infringement claim, despite *The Nation's* argument that all it took from the memoir was factual information, most of which was paraphrased, interspersed with a few short quotations. [FN389] The Supreme Court concluded that, for example, Ford's quoted narrative about the Nixon pardon was protectable expression, even though it was fact based and discussed historical events that Ford witnessed and participated in. [FN390] Even the act of paraphrasing Ford's recounting of an historical event did not divorce fact from expression sufficiently to avoid copyright infringement, according to the Court. [FN391] The decision in *Harper & Row* demonstrates that copyright allows the suppression of facts quite handily.

**701* With respect to trademarks, Volokh asserted that trademark law does not prohibit noncommercial speech that communicates facts or opinions about a product. [FN392] As a doctrinal matter, he is essentially correct. As a practical matter, though, trademark law impacts free speech tremendously. If one writes a novel in which the protagonist attributes tooth decay to drinking too much of a name brand cola, or makes disparaging remarks about the taste of a certain brand of soda, and her publisher actually allows her to use the trademarked name in print (which is unlikely), then the carbonated beverage company may bring suit, and at least one of the claims would likely be trademark based. The author would in all probability then agree to remove the trademarked name from future editions of the novel to settle the suit as expeditiously and inexpensively as possible.

Even seemingly benign uses of trademarks will provoke letters from lawyers. If one writes a novel in which a character "xeroxes" something, she may very well receive a letter from the Xerox company asking her to kindly substitute the word "photocopy" for their trademark in the future (so that their trademark does not commit genericide). [FN393] If she writes about "kitty litter," which is also a trademark, and it comes to the trademark owner's attention, she will get a similar letter asking her to eschew the "kitty litter" trademark in favor of the generic term "cat box filler." [FN394] If she moves away from fiction into the world of fact, and constructs a web site critical of a company or product, trademark law will be used in an attempt to shut down her site

and shut her up: First Amendment values might ultimately triumph over trademark, but only after expensive, potentially protracted litigation. [FN395]

*702 Volokh may be correct that an absolute property right in personal information could have a deleterious effect on free speech. However, to the extent personal information is treated like a copyrighted database or a trademark, and bound by the same First Amendment jurisprudence, concerns about free speech should be no greater for personal data than for informational components of intellectual property. Individuals would have a level of information control tied to that enjoyed by commercial entities, and subject to the same restrictions. If this stimulated a broad reevaluation of the interplay between intellectual property and the First Amendment, that would surely represent a positive development.

XII. Fair Use--Non-permissive Data Uses for the Societal Good

"Fair use" is the doctrine that allows one to use another's intellectual property for (usually) limited purposes without the owner's consent, or in some situations, even contrary to the owner's wishes. Fair use has been called an equitable rule of reason with no real definition. [FN396] Most clearly delineated in the copyrights context, fair use doctrine embodies the policy against freighting ideas and information with proprietary claims. [FN397] Intangible (or "intellectual") property is vested with a public interest and intended to achieve an "important public purpose." [FN398] There is a societal bargain implicit in the legal protections accorded intellectual property. Owners are given tools in the form of exclusive rights which they can use to financially exploit creative endeavors. However, this gift is conditioned upon an understanding that the ultimate goal of the legal framework is to maximize *703 the number of creative works available to the public, not to benefit individual intellectual property owners. [FN399] Fair use, therefore, represents ample control withheld from an intellectual property owner when a grant is made, rather than a right or privilege owners earn or acquire that is subsequently "taken."

Courts have held that the scope of copyright fair use is inversely related to ease of licensing. [FN400] If contracting for our data is fast and efficient, there will not be a need for any non-permissive fair use as corporate interests currently construe the doctrine. [FN401] Only descriptive, noncommercial uses of our data without a license would likely be fair under a Lanham Act analysis, so our personmarks could only be fairly used without our consent within a limited range of contexts. To the extent our data is protected by our rights of publicity, it may not be susceptible to fair use at all because fair use is not a defense in that context. [FN402]

We therefore have little to fear from fair use, in terms of losing power or exclusivity, thanks to the industrious efforts of commercial content owners. We can accrue the benefits of information exchange when we voluntarily disclose our personal information and permit uses of our data. Non-permissive fair uses are unlikely to be significant enough to impact our privacy, given the current narrow scope of fair use generally. [FN403]

***704 Conclusion**

If every woman gains control over her own personal information, commercial expectations could be kept off balance. Corporations will not know whether someone has allowed her personal information to be purchased because she is interested in a product, or interested in obtaining a royalty. They will know only what we allow them to know, not the other way around, and may at times be forced to rely on their own judgments.

Corporations will, however, be freed from the web of conflicting privacy laws they have railed and lobbied against. [FN404] Rather than varying privacy standards for different jurisdictions, these companies will simply have to come to terms with uniform, consistent, predictable, straightforward, universal property rights, to the extent the legislative and judicial bodies of government can proscribe them.

Once I own my own data, I personally look forward to formulating a reverse "click-wrap" license, whereby any enterprise that wants me to visit its web site will have to agree to MY list of terms and conditions, which may look something like this:

By inviting me into your site, you, the web entity, agree to the following:

You will not leave any cookie files without my express authorization, and even with my express authorization will leave the least invasive cookie file possible, the purpose and goals of which will be clearly communicated to me, along with instructions for removing the cookie file if and when I desire to. You will not record any aspect of my clickstream without express authorization from me, and even with authorization will not record it in conjunction with information that identifies me. You will not use any information I permit you to collect to generate personalized advertisements or direct them at me. If you violate any of the terms of this agreement, you agree to pay me \$10,000 per occurrence, plus reimburse any legal fees I incur.

[FN1]. See Boston Women's Health Collective, *Our Bodies, Ourselves: A Book By and For Women* (2d ed. 1976). The title of this article references this seminal work that enabled women to learn about and gain control over their bodies and health. Use of the third person plural is also in homage to this groundbreaking book.

[FN1a]. Assistant Professor of Law, University of South Carolina School of Law. Many thanks to Llew Gibbons, Vernellia Randall, Andrea Seielstad, and Molly O'Brien for sharing their thoughts and comments about early drafts of this article. This article is dedicated to Casey Bartow- McKenney.

[FN2]. Where are women in cyberspace? After watching Bob Cringely's PBS documentary "Nerds 2.0.1: A Brief History of the Internet," one could readily conclude that women spend most of their online time appearing on porn sites, batting their cursors and looking for cyber-dates, or e-shopping. See *Nerds 2.0.1* (visited May 28, 2000) <<http://www.pbs.org/opb/nerds2.0.1/>>. With few exceptions (most notably, Sandy Lerner, co-founder of Cisco Systems, who was subsequently ousted from the company and currently runs Urban Decay, a successful cosmetics company that she founded), women did not seem to have much of a role in founding the Internet, which like so many modern marvels has moved smoothly from creation as an instrument of military communication to civilian application as an implement of commerce. See *Nerds 2.0.1- Cast of Characters* (visited July 19, 2000) <<http://www.pbs.org/opb/nerds2.0.1/cast/>> (listing the names of people responsible for the development of the Internet).

[FN3]. Tama Janowitz, *Slaves of New York* 59 (1986).

[FN4]. See discussion *infra* Parts II, III, IV. See generally Leslie A. Kurtz, *The Invisible Becomes Manifest: Information Privacy in a Digital Age*, 38 *Washburn L.J.* 151, 165-66 (1998) (explaining how personal information is collected via cyberspace).

[FN5]. Net marketers often describe visitors to web sites as "a pair of eyeballs." See Erik Larson, *Free Money*, *New Yorker*, Oct. 11, 1999, at 76, 78.

[FN6]. See discussion *infra* Part VII.

[FN7]. See discussion *infra* Part IX.

[FN8]. "Information privacy" references the ability to control the dissemination of personal information, data that is identifiable to an individual. See Information Infrastructure Task Force: *Privacy and the National Information Infrastructure* (June 6, 1995) <http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html>.

[FN9]. The author uses the more gender-neutral "web swimming" rather than "web surfing," since most surfers are male. It also is more apropos, since using the Internet is more like plunging in and thrashing around than gracefully skimming a surface.

[FN10]. See Lindsey Arent, *How Women Buy, and Why* (Nov. 17, 1999) <<http://www.wired.com/news/print/0,1294,32483,00.html>> (discussing a joint study conducted by Harris Interactive, Procter & Gamble and Women.com Networks entitled *The Online Woman: How to Tap Into Her Buying Power*, which determined that women handle 75% of the family finances and control roughly 80% of family purchasing decisions); Laurie J. Flynn, *Microsoft is Starting Web Site Aimed at Women* (Feb. 8, 1999) <<http://www.nytimes.com/library/tech/99/02/biztech/articles/08net.html>> (citing Michael Goff, MSN's director of programming); John Frederick Moore, *iVillage IPO Takes Off* (Mar. 19, 1999) <<http://cnnfn.cnn.com/1999/03/19/technology/ivillage/index.htm>>; see also Martha Slud, *Web Targets Women Users: From iVillage to Oprah.com, the Net is Making a Play for the Female Market* (Apr. 2, 1999) <<http://cnnfn.cnn.com/1999/04/02/technology/women2/index.htm>> ("By 2002, women are projected to comprise 51 percent of all Internet users.... [W]omen wield huge control over household spending and are expected to be the catalysts if and when major growth in online shopping takes place."); Bob Tedeschi, *Online Retailers Applaud Increase in Women Shoppers* (July 12, 1999) <<http://www.nytimes.com/library/tech/99/07/cyber/commerce/12commerce.html>>. [T]he percentage of World Wide Web Shoppers who are women has jumped the last 12 months, to 38 percent from 29 percent, according to a Commercenet/Nielsen Media Research study.... "The early part of the e-commerce revolution was a revolution of rich white males," said Katherine Borsecnik, senior vice president for strategic business at America Online. "That's changing. And with 80 to 85 percent of household spending controlled by women, the total retail dollars involved in that change is very high." Id. But see Jim Frederick, *\$6 Billion in Online Holiday Sales by the End of This Month! \$24 Billion in Internet Ads by 2003! 2.3 Trillion E-Biz Predictions by 2010!* (Dec. 19, 1999) <<http://www.nytimes.com/library/magazine/home/19991219mag-frederick9.html>> (casting doubt on the reliability of predictions about e-commerce).

[FN11]. Flynn, *supra* note 10. See Lisa Moskowitz, *What Kind of Mother Are You?* (Feb. 28, 2000) <<http://www.salon.com/mwt/feature/2000/02/28/marketing/print.html>> ("According to *Sales and Marketing Management* magazine, women in the United States control 80 percent of all household buying decisions."); cf. Mark Boal, *Women Are Easy* (June 2-8, 1999) <<http://www.villagevoice.com/features/9922/boal.shtml>> ("[W]hen it comes to spending--the litmus test for advertisers--women match men in dollar power, and in some areas outspend them. Total monthly credit card expenditures by women 18 to 34 exceed male spending by 2 percent, according to MediaMark, a top New York consumer research firm.").

[FN12]. Slud, *supra* note 10 (quoting Susan Williams Defife, President and CEO of Womenconnect.com).

[FN13]. See, e.g., Denise Caruso, *Exploiting--and Protecting--Personal Information*

(Mar. 1, 1999) <<http://www.nytimes.com/library/tech/99/03/biztech/articles/01digi.html>>; Peter McGrath Privacy, Please (Apr. 15, 1999) <http://www.newsweek.com/nw-srv/tnw/today/cs/cs02we_1.htm>.

[FN14]. See discussion *infra* Part II.

[FN15]. But see Lakshmi Chaudhry, *Breath Oxygen, Be Free* (Mar. 3, 2000) <<http://www.wired.com/news/print/0,1294,34264,00.html>> (quoting Emily Hancock, editor of *Moxie*, a feminist e-zine, for the proposition that the need to sell produces insipid content, and quoting Lisa Jervis, editor of *Bitch* magazine, for the proposition that despite their use of feminist rhetoric, sites like *iVillage*, *Women.com*, and *Oxygen Media* "merely recycle the traditional women's magazine formula of health-beauty-sex" and sadly circumscribe women's interests to be only about makeup because advertisers do not trust women to want interesting content).

[FN16]. See Peter McGrath, *Knowing You All Too Well* (Mar. 25, 1999) <http://www.newsweek.com/nw-srv/printed/us/st/ty0113_1.htm>, <http://www.newsweek.com/nw-srv/printed/us/st/ty0113_2.htm>, <http://www.newsweek.com/nw-srv/printed/us/st/ty0113_3.htm>.

[FN17]. Women do not seem to be doing much hacking, so cyber-women would not appear to be online troublemakers. Hacking is a "boy culture," predominantly white, suburban, male, and premised on the formation of masculinity. See, e.g., Ellen Messmer, *Security Expert Explains New York Times Site Break In* (Sept. 18, 1998) <<http://cnn.com/TECH/computing/9809/18/nythack.idg/index.html>> (discussing the group that hacked New York Times site and called itself "Hackers for Girlies." It was apparent from context that the "Girlies" reference was not intended to be complimentary, and did not describe the individuals who had entered and altered the site.).

[FN18]. See Bob Tedeschi, *Can Merchants Buy Loyal Customers?* (Sept. 19, 1999) <<http://www.nytimes.com/library/tech/99/07/cyber/commerce/19commerce.html>>. To join, [Mypoints customer rewards program] members must also ante up something of value: they have to fill out a form detailing their interests and shopping preferences. Once they do so--on the condition that Mypoints will not reveal their identity to marketers, or sell personal information without the customers' permission--Mypoints sends them an e-mail with "targeted, relevant offers" daily or every other day, said Steve Markowitz, Mypoints' chief executive. Merchant partners, meanwhile, pay on average 25 cents for every e-mail message that Mypoints sends on their behalf. Since Mypoints collects detailed demographic data from its users, those e-mails can produce strong results. For example, in a promotion conducted for *Egghead.com* earlier this year, Mypoints sent an e-mail offer to 20,000 of its members. Even though this campaign was much smaller than *Egghead's* typical direct marketing effort, James Kimball, a marketing analyst for *Egghead*, said it was a "tremendous success."

"Our customer list is well over 2 million, which we send e-mails to once or twice a week. But since Mypoints has such amazing information on their customers, we could target a very specific demographic, and we got a click-through rate on that mailing that was eight times our normal e-mail response, and a conversion rate that was about three times our normal rate," Kimball said, referring to the rate at which companies turn browsers into buyers."

Id. See generally Kurtz, *supra* note 4, at 159-61 (discussing monitoring techniques).

[FN19]. See Slud, *supra* note 10; Paul Schwartz, Privacy and Democracy in Cyberspace, 52 Vand. L. Rev 1609, 1647-50 (1999). The Internet "has the potential to emerge as an essential focal point for communal activities and political participation...forming new links between people and marshalling these connections to increase collaboration in democratic life." Id. at 1648. See generally Jeffrey Rosen, The Eroded Self (Apr. 30, 2000) <<http://www.nytimes.com/library/magazine/home/20000430mag-internetprivacy.html>>. The sociologist George Simmel observed nearly 100 years ago that people are often more comfortable confiding in strangers than in friends, colleagues or neighbors. Confessions to strangers are cost-free because strangers move on; you never expect to see them again, so you are not inhibited by embarrassment or shame. In many ways the Internet is a technological manifestation of the phenomenon of the stranger. Id.

[FN20]. See, e.g., Bob Tedeschi, Now That They've Come, What Can We Sell Them?, N.Y. Times, Mar. 29, 2000, at 9 (discussing how initially the Internet "assumed a quaint identity as a place where people offered information freely"; then came e-commerce, tremendous interest in making money from the large number of people who frequent a site, and profound changes for community sites).

[FN21]. See *supra* notes 9-12 and accompanying text.

[FN22]. iVillage.com (visited June 4, 2000) <<http://www.ivillage.com/>>.

[FN23]. See Nina Teicholz, Places for Serious Sisterhood (Oct. 22, 1998) <<http://www.nytimes.com/library/tech/98/10/circuits/library/22ivil.html>>; iVillage Offering is Priced Higher (Mar. 17, 1999) <<http://www.nytimes.com/library/tech/99/03/biztech/articles/17village.html>>; Larson, *supra* note 5, at 78-79.

[FN24]. Teicholz, *supra* note 23 (quoting Jason Stell, "an iVillage spokesman").

[FN25]. Moore, *supra* note 10. Do not expect iVillage to employ a lot of women, though; instead it relies on the labor of over a thousand presumably grateful volunteers. See Lisa Napoli, America Online is Facing Challenge Over Free Labor (Apr. 14, 1999) <<http://www.nytimes.com/library/tech/99/04/biztech/articles/14aol.html>> ("For instance, iVillage [sic], an online women's network, uses more than 1,000 volunteers to manage

message boards and chat communities."). Web entities are happy to sell products to women consumers, but perhaps less eager to hire them. Jesse Jackson has labeled this "one-way trading." See Matt Richtel, Jackson Says Silicon Valley Companies Discriminate (Mar. 1, 1999) <<http://www.nytimes.com/library/tech/99/03/cyber/articles/01jackson.html>>; see also Diana Lynch, If Women Made Computers... (Feb. 23, 1999) <<http://abcnews.go.com/sections/tech/WiredWomen/wiredwoman990223.html>> ("[T]he brave new digital world is no democracy, and strength in numbers isn't buying [women] influence on the Web or employment in the corporate offices of the high-tech firms that increasingly control it.").

[FN26]. Larson, *supra* note 5, at 76.

[FN27]. See *id.* at 78.

[FN28]. *Id.* at 85.

[FN29]. See *id.* at 78-79.

[FN30]. *Id.* at 78.

[FN31]. Parent Soup (visited June 17, 2000) <<http://www.parentsoup.com>>.

[FN32]. Larson, *supra* note 5, at 78.

[FN33]. Amazon.com (visited June 17, 2000) <<http://www.amazon.com>>.

[FN34]. iBaby.com (visited June 17, 2000) <<http://www.ibaby.com>>.

[FN35]. iMaternity.com (visited June 17, 2000) <<http://www.imaternity.com>>. See Larson, *supra* note 5, at 78.

[FN36]. Underwire (visited June 17, 2000) <<http://www.underwire.msn.com>>.

[FN37]. Flynn, *supra* note 10.

[FN38]. WomenCentral (visited June 17, 2000) <<http://womencentral.msn.com/>>.

[FN39]. The Microsoft Network (visited June 17, 2000) <<http://www.msn.com/>>. See Flynn, *supra* note 10.

[FN40]. Women.com (visited June 17, 2000) <<http://women.com/>>.

[FN41]. See Flynn, *supra* note 10.

[FN42]. Electra (visited June 17, 2000) <<http://www.electra.com/>>.

[FN43]. ThriveOnline (visited June 17, 2000) <<http://www.thriveonline.oxygen.com>>.

[FN44]. Moms Online (visited June 17, 2000) <<http://momsonline.oxygen.com/>>.

[FN45]. Oxygen (visited June 17, 2000) <<http://www.oxygen.com/>>.

[FN46]. See Slud, *supra* note 10.

[FN47]. See James Poniewozik, Will Women Take a Breath of Oxygen? (Jan. 31, 2000) <<http://www.time.com/time/magazine/articles/0,3266,38042,00.html>>, <<http://www.time.com/time/magazine/articles/0,3266,38042-2,00.html>>; Courtney Macavinta, Oxygen: Lipstick and Recipes or a Media Revolution? (Oct. 25, 1999) <<http://news.cnet.com/news/0-1014-201-920020-0.html>>.

[FN48]. See James Ledbetter, Net Investing for the Good of Mankind (Aug. 9, 1999) <<http://www.thestandard.com/article/display/0,1151,5756,00.html>> ("Many of Markle's Internet investments have the aura of do-gooder high-mindedness associated with traditional foundation grants."); The Markle Foundation (visited June 4, 2000) <<http://www.markle.org/index.html>> (displaying the homepage for the private not-for-profit Markle Foundation).

[FN49]. Courtney Macavinta, U.S. Official Directs Net Funding, Puts Consumers First (Nov. 15, 1999) <<http://news.cnet.com/news/0-1005-200-1438333.html>> (interviewing Zoe Baird). See also Amy Harmon, For Zoe Baird, a New Opportunity for Public Service (July 26, 1999) <<http://www.nytimes.com/library/tech/99/07/biztech/articles/26zoe.html>>.

[FN50]. Macavinta, *supra* note 49.

[FN51]. Zoe Baird has urged readers to use the Internet to focus on "unmet markets" and "unmet needs":

For example, there also may be large, untapped markets in low-income areas. A recent study found that inner-city consumers wield \$85 billion in annual spending power, yet are under served by traditional retail services. We need to understand the needs and attitudes of these populations better so businesses have the information to tap these new markets.

Zoe Baird, Use Web for More Than Shopping (Dec. 9, 1999) <<http://www.markle.org/news/Clipping.199912091055.1172.html>>. See also Ledbetter, *supra* note 48 ("Geraldine Laybourne acknowledges that the Markle project amounts to doing market research for her competitors, an arrangement she calls 'highly unusual.'").

[FN52]. Estroclick (visited June 17, 2000) <<http://estroclick.chickclick.com/>>.

[FN53]. Id.

[FN54]. hipMama (visited June 17, 2000) <<http://www.hipmama.com/>>.

[FN55]. Wench (visited June 17, 2000) <<http://www.wench.com/>>.

[FN56]. Bust (visited June 17, 2000) <<http://www.bust.com/>>.

[FN57]. Hissyfit (visited June 17, 2000) <<http://www.hissyfit.com/>>. See Chickclick Press Releases (visited July 19, 2000) <<http://www.chickclick.com/faq/press.html>>; Elizabeth Weise, Oxygenating the Women's Market (Feb. 3, 2000) <<http://www.usatoday.com/life/cyber/tech/net001.htm>>.

[FN58]. See, e.g., iWon Women's Consumer Center (visited July 19, 2000) <http://www.iwon.com/home/shopping/womens_center_overview/0,13826,,00.html> ("Start saving time and money today. Leave the comparison shopping and haggling to us!").

[FN59]. See Jean Kilbourne, *Deadly Persuasion: Why Women and Girls Must Fight the Addictive Power of Advertising* 33 (1999) (referring to the title of Chapter One, "Buy This 24-Year-Old and Get All His Friends Absolutely Free").

[FN60]. See, e.g., Bob Tedeschi, E-Commerce Sites Target Next Generation of Buyers (Mar. 29, 1999) <<http://www.nytimes.com/library/tech/99/03/cyber/commerce/29commerce.html>> ("According to industry executives and analysts, Internet commerce companies are recognizing the natural confluence of e-commerce and the 18-and-under set, and are positioning themselves more aggressively at that intersection.").

[FN61]. See Janelle Brown, Cool Hunters Hit the Web Jungle (May 13, 1999) <<http://www.salonmagazine.com/tech/feature/1999/05/13/smartgirl/index.html>>, <<http://www.salonmagazine.com/tech/feature/1999/05/13/smartgirl/index1.html>>.

[FN62]. Id. (quoting Kevin Mabley, director of research at online market research firm Cyber Dialogue).

[FN63]. SmartGirl Internette (visited June 4, 2000) <<http://www.smartgirl.com/>> (displaying the homepage for coyly named website, highlighting the phrase "Smart girls decide for themselves," followed by a prominent "TM").

[FN64]. Id.

[FN65]. Speak Out (visited July 8, 2000) <<http://www.smartgirl.com/pages/speak.html>>.

[FN66]. Brown, *supra* note 61.

[FN67]. See id.

[FN68]. See id.

[FN69]. Speak Out (visited July 8, 2000) <<http://www.smartgirl.com/pages/speak.html>>. Although SmartGirl at one time did not accept advertising, that is no longer their policy. "Because of economic demands, SmartGirl now includes some advertising. All advertising is clearly marked as advertising." Id.

[FN70]. See Joseph Turow & Lilach Nir, *The Internet and the Family 2000, The View From Parents, The View From Kids*, Report Series No. 33 (May 2000) <http://www.appcpenn.org/finalrepor_fam.pdf> (displaying report done by the Annenberg Public Policy Center on the differing points of view regarding the importance of Internet privacy).

[FN71]. See id.

[FN72]. See Janelle Brown, *Girl Talk* (July 28, 1999) <http://www.salonmagazine.com/tech/feature/1999/07/28/girl_talk/index.html>.

[FN73]. See Bob Tedeschi, *supra* note 20, at 9. This section title refers to the title of this article.

[FN74]. See Jerry Berman & Deirdre Mulligan, Privacy in the Digital Age: Work in Progress, 23 *Nova L. Rev.* 551, 554 (1999).

The Internet accelerates the trend toward increased information collection, which is already evident in our offline world. The data trail, known as transactional data, left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. Transactional data, click stream data, or "mouse droppings," as it is alternatively called, can include the Internet protocol address ("IP address") of the individual's computer, the browser in use, the computer type, and what the individual did on previous visits to the Web site, or perhaps even other Web sites. This data, which may or may not be enough to identify a specific individual, is captured at various points in the network and available for reuse and disclosure. Some of the data generated is essential to the operation of the network, like the phone number that connects a calling party to the intended recipient, the IP address is necessary, for without it the network cannot function. However, other pieces of data may serve purposes beyond network operation. Along with information intentionally revealed through purchasing or registration activities, this transactional data can provide a "profile" of an individual's activities. When aggregated, these digital fingerprints reveal the blueprint of an individual's life. This increasingly detailed information is bought and sold as a commodity by a growing assortment of players. Id. at 554. See also Jerry Kang, Information Privacy in Cyberspace Transactions, 50 *Stan. L. Rev.* 1193, 1223-30 (1998) (discussing the information exchanged in a typical

e-commerce transaction).

[FN75]. See Schwartz, *supra* note 19, at 1623-26.

[FN76]. McGrath, *supra* note 16.

[FN77]. See D. Ian Hopper, *New Tool Offers Privacy Without Crippling Browsing Habits* (Mar. 21, 2000) <<http://www.cnn.com/2000/TECH/computing/03/21/idcide/index.html>>.

If the networks are allowed to track, they can record all sorts of information about your habits. Security consultant and privacy watchdog Richard M. Smith showed how DoubleClick can mine personal data from a user's habits on such popular Web sites as AltaVista, Travelocity, DrKoop.com, Buy.com and the Internet Movie Database. By visiting less than 10 sites, the network had his name, street address, e-mail address and birthday. The ad company also saved transactional information such as the route of a plane trip, what search terms he used in a search engine, and what products he browsed on e-commerce sites.

Id.

[FN78]. For a discussion of the meaning of "clickstream," see Hiawatha Bray, *They're Watching You*, *Boston Globe*, Feb. 11, 1999, at G6.

Here's how it works: Many commercial Web sites feature banner ads linked to the DoubleClick network. When someone visits one of these sites, his or her computer gets a cookie that notes the particular ad being displayed. The cookie continues to track the user, noting every visit to a site featuring DoubleClick ads. The cookie tracks which ads the user clicks on for more information, and which ads he or she ignores.

Id.

[FN79]. See Saul Hansell, *Big Web Sites to Track Steps of Their Users*, *N.Y. Times*, Aug. 16, 1998, at A1. See generally Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (2000) (criticizing the proliferation of technologies used by businesses, the government and others to invade personal privacy). For a broader, more detailed explanation of how "finely granulated personal data" can be harvested via computer, see Schwartz, *supra* note 19, at 1621-31.

[FN80]. Bob Tedeschi, *Targeted Marketing Confronts Privacy Concerns* (May 10, 1999) <<http://www.nytimes.com/library/tech/99/05/cyber/commerce/10commerce.html>>.

See also Schwartz, *supra* note 19, at 1641.

[FN81]. Hansell, *supra* note 79, at A1.

[FN82]. See McGrath, *supra* note 16. The Web has evolved into a marketplace, and in the process transformed privacy from a right to a commodity. High-speed networking and powerful database technologies have made it possible for businesses to amass, quickly and at low cost, a wealth of personal information on nearly 200 million

Americans, especially the 40 or so million who cruise the Web. You want a list of people in the wealthy Westchester County suburbs of New York, sorted by household income and "lifestyle interests" ? No problem. Go to myprospects.com, which will charge you as little as 16 cents a name, no questions asked. You want to know if a potential business partner has a history of bad credit or fraud? Hundreds of investigative sites, such as discreetresearch.com, will oblige. You want to buy the executive travel records of your competitor, so you can figure out not only where they're going but whom they're meeting with? Companies that do "competitive intelligence" can mine the database, as the giant accounting firm PricewaterhouseCoopers recently found out to its chagrin.
Id.

[FN83]. See, e.g., Andrew Leonard, *Your Profile, Please* (June 26, 1997) <<http://www.salonmagazine.com/june97/21st/article970626.html>> ("Says Ted Kamionek, Firefly's director of communications: 'If an advertiser comes to us and says, I want to reach males who live in the Midwest who like athletic activities and R.E.M. and want to buy T-shirts, we can manage that relationship.' "). See also Hansell, *supra* note 79, at A1, A24.

[FN84]. Leonard, *supra* note 83. But see Denise Caruso, *A New Model for the Internet: Fees for Services* (July 19, 1999) <<http://www.nytimes.com/library/tech/99/07/biztech/articles/19digi.html>> (discussing how Internet-centered businesses are moving away from the ad-supported business model and toward the transaction model).

[FN85]. From the *Speeches of Gerry Laybourne* (visited May 1, 1999) <http://www.oxygen.com/html/ox_vi_spch.htm>. This web page is no longer accessible.

[FN86]. Tedeschi, *supra* note 10.

[FN87]. See Hansell, *supra* note 79, at A1.

[FN88]. Freedom of Information, Inc., U.S. Patent No. 5848396 (Dec. 8, 1998) (Thomas A. Gerace, Inventor).

[FN89]. USPTO Entry of U.S. Patent No. 5848396 (visited June 17, 2000) <<http://164.195.100.11/netacgi/nph-Parser?Sect=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netahtml/srchnum.htm&r=1&f=G&l=50&s1='5848396'.WKU.&OS=PN/5848396&RS=PN/5848396>> (displaying the abstract and claims of the patent). See *Patently Personal* (Dec. 18, 1998) <http://www.privacytimes.com/index_ecom.htm>.

Be Free Inc., a small start-up in Marlborough, Mass., expects to receive a patent for a method of passively collecting behavioral profiles and psychographic data (attitudes and life styles) in individual computer users, storing this information in a huge database and then using it to decide which consumers should see which ads.

Id.

[FN90]. See Marius Meland, *The Other Online Profiler* (Feb. 25, 2000) <<http://www.forbes.com/tool/html/00/Feb/0225/mu2.htm>>.

[FN91]. Tedeschi, *supra* note 80 (quoting Julie Williams, chief counsel of the Comptroller of the Currency, a federal agency that oversees banking activities). See also Tedeschi, *supra* note 18.

[FN92]. Leonard, *supra* note 83 (quoting Jerry Kang, a law professor at UCLA).

[FN93]. Berman & Mulligan, *supra* note 74, at 571-72.

[FN94]. Bob Tedeschi, *Seeking Ways to Cut the Web-Page Wait* (June 14, 1999) <<http://www.nytimes.com/library/tech/99/06/cyber/commerce/14commerce.html>> (quoting Jonathan Morris, executive vice president of Bluefly, a discount apparel retailer).

[FN95]. See Debra Aho Williamson, *The Information Exchange Economy* (Apr. 30, 1999) <<http://www.cnn.com/TECH/computing/9904/30/infoexchange.idg/>>.

[FN96]. See Saul Hansell, *In a Wired World, Much is Free at Click of a Mouse* (Oct. 14, 1999) <<http://www.nytimes.com/library/tech/99/10/biztech/articles/14free.html>>; see, e.g., Michelle Finley, *Want Free DSL? You'll Pay For It* (Mar. 27, 2000) <<http://www.wired.com/news/print/0,1294,35104,00.html>>.

[FN97]. See Taylor & Jerome, *Offend Your Mother* (Dec. 1999) <<http://www.zdnet.com/pccomp/stories/all/0,6605,2386401,00.html>>; *How to Shop Online* (visited July 12, 2000) <<http://www.netguide.com/special/primers/shopping/home.html>>.

[FN98]. Berman & Mulligan, *supra* note 74, at 558. See also Michael Stroud, *You Are What You Ware* (Sept. 28, 1999) <<http://www.wired.com/news/print/0,1294,31529,00.html>> ("You're walking around some huge computer show wearing a cracker-sized sliver of silicon that was part of your conference registration package. Your stylish 'infocharm' comes with a tiny infrared transceiver that automatically captures which booth you visited, whom you talked to, and how long you spent there."); *Beyond 2000--Supermarkets Check You Out* (Mar. 8, 2000) <http://www.beyond2000.com/news/story_475.html>. See, e.g., James Glave, *Levi's Brave New World* (Aug. 16, 1999) <http://www.wired.com/news/print_version/business/story/21268.html> (discussing something close to this is actually available in real space at Levi's San Francisco store, which uses biometrics, including fingerprinting, to track and learn about customers).

[FN99]. Hansell, *supra* note 79, at A24 (Adforce Inc., of Cupertino, California, is "seeking to persuade Internet service providers to give [it] the name and address of each visitor as he or she surfs. Adforce would then instantly retrieve demographic and

buying-habit data kept by Metromail about that person and use it to display advertisements aimed at him or her.").

[FN100]. Williamson, *supra* note 95.

[FN101]. Schwartz, *supra* note 19, at 1612.

[FN102]. See Steve Lohr, Online Industry Seizes the Initiative on Privacy (Oct. 11, 1999) <<http://www.nytimes.com/library/tech/99/10/biztech/articles/11priv.html>>. The spread of Internet technology will result in a data collection network of previously unimagined reach as telephones, televisions, cars and appliances-- not just personal computers--are connected to the global digital network before long. And the rapidly developing fields of data-mining and profiling software will enable corporations to increasingly slice and search through this ocean of data to identify personal patterns of buying and behavior--and make inferences, accurate or not, about a person's likely behavior.

Id.

[FN103]. See Who Watches Your Credit? (June 2, 1999) <http://cnnfn.com/1999/06/02/life/q_creditaccess/> (discussing how various agencies gather and use people's credit information).

[FN104]. Id.

[FN105]. Jeri Clausing, Revised Banking Legislation Raises Concerns About Privacy (Oct. 25, 1999) <<http://www.nytimes.com/library/tech/99/10/biztech/articles/25priv.html>>.

[FN106]. See discussion *infra* Part VI.

[FN107]. Hansell, *supra* note 79, at A1.

[FN108]. See Bob Tedeschi, Internet Retailers Work to Turn Shoppers Into Buyers (Mar. 8, 1999) <<http://www.nytimes.com/library/tech/99/03/cyber/commerce/08commerce.html>>.

[FN109]. Id. (quoting Andy Halliday, vice president for Excite's commerce division).

[FN110]. See id. (stating "[a]bout 15 percent of the customers the company pursues ultimately complete the sale").

[FN111]. See, e.g., Peter H. Lewis, Forget Big Brother, N.Y. Times, Mar. 8, 1998, at G1 (expressing consternation that the Holiday Inn chain used his Social Security number as his hotel membership number, apparently after obtaining it on its own initiative).

[FN112]. See Tedeschi, *supra* note 80 ("Internet retailers are... hoping customers view their [one-to-one marketing] efforts as helpful, not intrusive.").

[FN113]. Kang, *supra* note 74, at 1215-16 (footnotes omitted).

[FN114]. See Thomas Frank, *Brand You, Better Selling through Anthropology*, *Harper's Magazine*, July 1999, at 74, 78.

[FN115]. See *id.*

[FN116]. *Id.*

[FN117]. See Stuart Elliot, *Despite the Internet, Direct-Mail Pitches Multiply* (Oct. 25, 1999) <<http://www.nytimes.com/library/tech/99/10/biztech/articles/25adco.html>>.

[FN118]. See *id.* ("[D]irect mail... is proliferating faster than it did before the Internet, climbing to 44 percent of all pieces of mail handled last year by the post office from 41 percent a decade ago and 32 percent in 1978.").

[FN119]. See Marci McDonald, *A Start-Up of Her Own* (May 15, 2000) <<http://www.usnews.com/usnews/issue/000515/women.htm>>; Sue Zeidler, *Net Shatters Not-So-Sacred Gender Myths* (Mar. 8, 2000) <<http://www.zdnet.com/zdnn/stories/news/0,4586,2457975,00.html>> ("The roaring new economy is a genderless frontier with equal opportunity for men and women.").

[FN120]. For example, the Institute for Women and Technology has asserted: The application of technology to the lives of women has often been either an afterthought or based on stereotypical assumptions about the roles and needs of women and without the input or participation of those women. The situation has improved when it has been recognized that the difference in men's and women's situations, whether physiological or environmental, warrant different tools, techniques or solutions, and when design is based on women's real needs and desires. This enlightenment most often occurs when women are involved as creators and when their input as users/subjects is actively sought and used. It is no accident that as women entered medicine in large numbers, medicine began to question the application to women of research results from studies using only male subjects. Nor is it an accident that serious development of non-stereotypical computer tools and games appealing to girls is being initiated by women who listen to girls. Just as every invention reflects the values, perspectives, background and needs of the inventor, the variety and impact of new technologies will depend on the degree to which women are involved and the degree to which women's needs are taken into account.

Involving women actively in technology policy, design, development and deployment will create a better world for everyone. Both studies and evaluations of the real world indicate that when resources are given to women they are likely to be used for the betterment of the entire community. This is true whether the resources are education or money. We posit that the same will be true if the resource is information

technology. We believe that there has been no other time in history when the possibility for transformation towards equity is more possible, nor when it is more dangerous if we do not step up to the challenge.

The Institute for Women and Technology: Background (visited July 13, 2000) <<http://www.parc.xerox.com/oct/projects/iwt.org/background.html>>.

[FN121]. Professor Jessica Litman has made a related observation in a different context, noting:

Ralph [Brown] argued [in his 1948 article] Advertising and the Public Interest that just because people paid more for products did not mean there had been any actual increase in productivity and welfare--rather, we had let ourselves be talked into paying more money for the same stuff. That, he insisted, was obviously in the interest of the producers whose advertising had persuaded the public to pay a higher price, but was wasteful for the public at large. Today, that once self-evident point is controversial. Productivity seems to be measured less by what people make than by what people are inclined to buy. What consumers are willing to pay has become synonymous with value.

Jessica Litman, Breakfast With Batman: The Public Interest in the Advertising Age, 108 Yale L.J. 1717, 1725 (1999).

[FN122]. Jenn Shreve, Advertising Stole My Humanity (June 4, 1999) <<http://www.salonmagazine.com/media/col/shre/1999/06/04/ad/index.html>>.

[FN123]. Cf. Niva Elkin-Koren, Cyberlaw and Social Change: A Democratic Approach to Copyright Law in Cyberspace, 14 Cardozo Arts & Ent. L.J. 215, 238 (1996) (discussing how compilers of information necessarily must categorize that information, "perpetuat[ing] meanings assumed by the compilers").

[FN124]. See, e.g., Rosen, *supra* note 19.

[FN125]. See Arent, *supra* note 10.

[FN126]. See Moskowitz, *supra* note 11 (quoting Denise Fedewa of the Leo Burnett advertising firm).

[FN127]. See Florence Olsen, On-Line Research With Human Subjects Deserves More Scrutiny, Scientists Say (June 13, 1999) <<http://www.chronicle.com/free/99/06/99061501t.htm>>; see also CASRO: Code of Standards and Ethics for Survey Records (visited May 28, 2000) <<http://www.casro.org/casro.htm>> (displaying the homepage for the Council of American Survey Research Organizations, claiming to be "the national trade association of commercial survey research companies located in the United States"). CASRO requires its 170 members to subscribe to the CASRO Code of Standards and Ethics for Survey Research, which prohibits (with some qualifications) directing individual marketing efforts toward survey respondents "beyond those actions taken toward the entire database population group" simply because of participation in a survey. *Id.*

[FN128]. See Katie Hafner, *Coming of Age in Palo Alto* (June 10, 1999) <<http://www.nytimes.com/library/tech/99/06/circuits/articles/10anth.html>>.

[FN129]. Frank, *supra* note 114, at 79.

[FN130]. See Ruth Shalit, *The Return of the Hidden Persuaders* (Sept. 27, 1999) <<http://www.salon.com/media/col/shal/1999/09/27/persuaders/index.html>>; Lynn Burke, *Fiddling with Human Behavior* (Mar. 6, 2000) <<http://www.wired.com/news/print/0,1294,34526,00.html>>; Arthur Allen, *Shrinks and Con Men* (Feb. 28, 2000) <<http://www.salon.com/mwt/feature/2000/02/28/shrinks/print.html>> (Langebourne Rust has a Ph.D. in developmental psychology from Columbia University, and uses his skill "to convert knowledge of kids and their families into messages that sell."); Kilbourne, *supra* note 59, at 9 ("Many companies these days are hiring anthropologists and psychologists to examine consumers' product choices, verbal responses, even body language for deeper meanings.").

[FN131]. See Kang, *supra* note 74, at 1260; Schwartz, *supra* note 19, at 1656- 58; Kurtz, *supra* note 4, at 167.

[FN132]. Frank, *supra* note 114, at 79.

[FN133]. See *id.*

[FN134]. James Poniewozik, *We are All Page-View Whores Now* (visited May 28, 2000) <<http://www.salon.com/media/col/poni/1999/05/06/msnbc/index.html>>, <<http://www.salon.com/media/col/poni/1999/05/06/msnbc/index1.html>>. See also Felicity Barringer, *As Data About Readers Grows, Newspapers Ask: Now What?* (Dec. 20, 1999) <<http://www.nytimes.com/library/tech/99/12/biztech/articles/122099outlook-medi.html>> (discussing how online periodical publishers use data collected on their visitors).

[FN135]. Poniewozik, *supra* note 134.

[FN136]. See Williamson, *supra* note 95.

[FN137]. See *id.*

[FN138]. *Id.* (quoting Rich LeFurgy, chairman of the Internet Advertising Bureau and a consultant to venture-capital firm Walden International Investment Group).

[FN139]. See *id.*

[FN140]. *Id.*

[FN141]. Lohr, *supra* note 102. See also Martha M. Hamilton, *Web Retailer Kozmo Accused of Redlining* (Apr. 14, 2000) <<http://www.washingtonpost.com/wp-dyn/articles/A9719-2000Apr13.html>> (discussing the accusations against Kozmo for violating civil rights laws by denying Internet service to predominantly African-American neighborhoods in Washington, D.C.).

[FN142]. For example, at the moment the Hispanic market may not appear lucrative. See Bob Tedeschi, *Bringing Technology to the Barrio* (Sept. 23, 1998) <<http://www12.nytimes.com/library/tech/98/09/cyber/articles/23barrio.html>> (quoting Anthony Wilhelm, author of a Tomas Rivera Policy Institute report and speaker at a Silicon Barrio conference: "Companies like IBM and Microsoft don't have a strategy that exploits Hispanic markets.... They're never quite candid about why, but basically I think they don't want to spend a whole lot of resources going after an unproven market.").

[FN143]. See *id.*

[FN144]. See Janet Stites, *Black Entrepreneurs Spread the Word About "Digital Freedom"* (Feb. 22, 1999) <<http://www.nytimes.com/library/tech/99/02/biztech/articles/22pros.html>> ("According to [Forrester Research of Boston] 2.7 million African-American households (out of about 11 million) have access to the Internet....").

[FN145]. See Kilbourne, *supra* note 59, at 3. "At \$446 billion, African American buying power is more than the GNP of Switzerland," says an ad in *Advertising Age*. Another, for a "Black-owned agency," implies it can "get you inside the soul of the African American consumer." "Are You Skirting a Major Market?" asks an ad for a local Florida television station picturing a Latina in a very short skirt. It concludes, "Channel 23. Because South Florida spends a lot of dinero!" An ad for a Latina magazine says "She's Latina. She spends more." And the Hispanic Network tells advertisers that "Hispanic families are more responsive to advertising. And ads in Spanish are 5 times more persuasive." *Id.*

[FN146]. For discussions of the impacts of racial stereotyping, see Keith Aoki, "Foreign-ness" and Asian American Identities: Yellowface, World War II Propaganda, and Bifurcated Racial Stereotypes, 4 *U.C.L.A. Asian Pac. Am. L.J.* 1 (1996) and Alice Abreu, Lessons From LatCrit: Insiders and Outsiders, All At The Same Time, 53 *U. Miami L. Rev.* 787 (1999). See also Kang, *supra* note 74, at 1210. Under one interpretation of the privacy definition, because... information is directly about [a] group and not the individuals that constitute the group, the data are not personal and stand outside privacy's realm. But this seems formalistic. A more functional approach would recognize that groups, even those recognized as legal persons, function only through the actions of the human individuals who are its members. Accordingly, information concerning a group concerns also those individuals that constitute the group. What we ultimately label as "personal" should

thus depend on context, such as the size of the group and the degree of focus the information places on some subset of that group.
Id.

[FN147]. See discussion *infra* Part VII.C.

[FN148]. Carl S. Kaplan, *Strict European Privacy Law Puts Pressure on U.S.* (Oct. 9, 1998) <[http:// www.nytimes.com/library/tech/98/10/cyber/cyberlaw/09law.html](http://www.nytimes.com/library/tech/98/10/cyber/cyberlaw/09law.html)>. See also Karlin Lillington, *Hands Off that Data--I'm European!* (July 7, 1998) <[http:// www.salonmagazine.com/21st/feature/1998/07/07feature.html](http://www.salonmagazine.com/21st/feature/1998/07/07feature.html)>.

[Because I am European, i]f I return a product registration card, I know that the personal information I offer cannot be sold to others as part of a sales database unless my permission has been obtained. I am never asked, except by the government department that issued it, to identify myself by a nationally assigned number. And any organization that holds any information about me-- banks, medical offices, telephone companies, the supermarket whose loyalty program I belong to, my gym, the videorental shop or the place where I returned a product registration card--must, at my request, supply me with full details of its computer records bearing my name.
Id.

[FN149]. 15 U.S.C. §§ 6501-6506 (2000).

[FN150]. Id. § 6502(b)(1)(A).

[FN151]. See id. § 6502(2)(b)(1)(B).

[FN152]. Id. § 6502(b)(1)(D).

[FN153]. 16 C.F.R. pt. 312 (2000). On October 20, 1999, the FTC announced issuance of its "final rule" with a press release, noting that the Rule would be published shortly in the Federal Register. See *New Rule Will Protect Privacy of Children Online* (Oct. 20, 1999) <[http:// www.ftc.gov/opa/1999/9910/childfinal.htm](http://www.ftc.gov/opa/1999/9910/childfinal.htm)> [hereinafter *FTC Press Release*].

[FN154]. FTC Press Release, *supra* note 153.

[FN155]. Id.

[FN156]. 15 U.S.C. § 6502(b)(1)(A).

[FN157]. Id. § 6501(9).

[FN158]. FTC Press Release, *supra* note 153; 16 C.F.R. § 312.5(b)(2) (2000).

[FN159]. FTC Press Release, *supra* note 153. The press release also states:
The notice must state the name and contact information of all operators, the types of

personal information collected from children, how such personal information is used, and whether personal information is disclosed to third parties.

The notice also must state that the operator is prohibited from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary. In addition, the notice must state that the parent can review and have deleted the child's personal information, and refuse to permit further collection or use of the child's information.

Id.

[FN160]. Id. The press release also states:

Such steps could include sending a confirmatory e-mail to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. The "sliding scale" will sunset two years after the effective date of the rule, at which time the more reliable methods would be required for all uses of information, unless the Commission determines more secure electronic methods of consent are not widely available.

Id.

[FN161]. Id.

[FN162]. Id. See also 16 C.F.R. § 312.5(c) (2000) (setting forth one such exception to parental consent).

[FN163]. FTC Press Release, *supra* note 153.

[FN164]. Id.

[FN165]. Id.

[FN166]. The press release states:

The statute also includes a "safe harbor" program for industry groups or others who wish to create self-regulatory programs to govern participants' compliance. Commission-approved safe harbors will provide Web site operators with the opportunity to tailor compliance obligations to their business models with the assurance that if they follow the safe harbor they will be in compliance with the rule. Sites participating in such Commission-approved programs will be subject to the review and disciplinary procedures provided in those guidelines in lieu of formal Commission action.

Id.

[FN167]. 15 U.S.C. § 6501(8) (2000).

[FN168]. See *id.* § 6502(a)(1); see also Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,892 (1999) (codified at 16 C.F.R. pt. 312 (2000)).

One commenter [sic] asked the Commission to clarify that operators are not required to provide parental notice or seek parental consent for collection of non-individually

identifiable information that is not and will not be associated with an identifier. The Commission believes that this is clear in both the Act and the Rule.
Id.

[FN169]. See FTC Press Release, *supra* note 153. ("The Federal Register notice accompanying the rule makes clear that schools can act as parents' agents or as intermediaries between Web sites and parents in the notice and consent process.").

[FN170]. See Daniel Golden, *Is ZapMe Collecting Data on School Kids?* (Jan. 19, 2000) <<http://www.zdnet.com/filters/printerfriendly/0,6061,2423767-2,00.html>> (discussing firm that brings online advertising into schools, allegedly helping advertisers collect the names and addresses of minors for marketing purposes without parental consent using equipment installed in 1,300 schools with a total of more than a million students). Channel One is a company that provides schools with "free" televisions and educational programming, but also broadcasts advertisements to students while they are in school and during school hours. Legislators seem to have taken notice of this practice. See Rebecca S. Weiner, *Parents Should Know Cost of Free Computers, Legislators Say* (July 12, 2000) <<http://www.nytimes.com/library/tech/00/07/cyber/education/12education.html>>.

[FN171]. See Paul Tolme, *AOL Offers Free Service To Schools* (May 17, 2000) <<http://www.cnn.com/2000/TECH/computing/05/17/aol.in.school.ap/index.html>>.

[FN172]. See *id.*

[FN173]. See *id.*

[FN174]. But see, e.g., Comments of the Direct Marketing Association, Inc. on the Children's Online Privacy Protection Rule (June 11, 1999) <<http://www.ftc.gov/privacy/comments/dma.htm>>.

[The Direct Markers Association] urge[s] the Commission in its final rules to: (1) endorse easy-to-use e-mail-based consent mechanisms that will not chill the availability of interactive sites for children; (2) reject parental "rights" to pick and choose between practices set forth in the operator's privacy notice, rather than accepting or refusing to consent to the operator's practices as a whole; (3) clarify certain exceptions to parental consent; (4) reject a parental "right" to alter data an operator has collected; (5) simplify significantly the rules' lengthy notice requirements; (6) modify the safe harbor provision so that it is less prescriptive, provides greater incentives for operators to join self-regulatory efforts, and leaves room for true self-regulation to resolve compliance problems; (7) make clear that the rules do not apply retroactively to information collected before the statute's effective date; (8) modify the definition of "collection" so that it does not apply to material submitted to an operator through other media or to inadvertent collection of information; (9) clarify that the statute does not impose strict or vicarious liability for the conduct of third-party contractors where contractors agree to follow the requirements of the statute; and (10) clarify the Commentary's discussion of security

measures.

Id.

[FN175]. See European Community Directive On Data Protection: Articles 11, 12, & 14 (visited July 13, 2000) <<http://www.acs.ohio-state.edu/units/law/swire1/psecdir.htm>>; see also Joel R. Reidenberg, Restoring Americans' Privacy in Electronic Commerce, 14 *Berkeley Tech. L.J.* 771, 781-85 (1999).

[FN176]. European Community Directive On Data Protection: Article 14(b) (visited June 17, 2000) <<http://www.acs.ohio-state.edu/units/law/swire1/psecdir.htm>>. It should be noted that as of this writing, several European countries have not yet passed national laws to carry out the European Union's Data Protection Directive. See Edmund L. Andrews, U.S.-European Union Talks On Privacy Are Sputtering, *N.Y. Times*, May 27, 1999, at C6.

[FN177]. Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive 3* (1998).

[FN178]. Id.

[FN179]. Kaplan, *supra* note 148 (quoting Ohio State University law professor Peter Swire).

[FN180]. See Bob Tedeschi, European Union Advances E-Commerce Policies (Apr. 26, 1999) <<http://www.nytimes.com/library/tech/99/04/cyber/commerce/26commerce.html>> (quoting Laura Starita, analyst with the Gartner Group, a Stamford, Connecticut based Internet research firm, "Europe is much more aggressive than the U.S. when it comes to legislating these things.... Culturally, we have a much more aggressive economic environment that's less concerned about individual rights"); see also Edmund L. Andrews, European Law Aims to Protect Privacy of Personal Data (Oct. 26, 1998) <<http://www.nytimes.com/library/tech/98/10/biztech/articles/26privacy.html>> ("For years, European nations have been far tougher than the United States about protecting privacy. Many countries essentially ban telephone marketing to people's homes, and that prohibition is now being applied to unsolicited sales approaches by fax and e-mail."); Kaplan, *supra* note 148 (quoting Peter Swire, "[Europe's data law sets a] standard of legal rights for individuals in Europe that go far beyond the legal rights of Americans.").

[FN181]. See Pamela Samuelson, Book Review: A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy, 87 *Calif. L. Rev.* 751, 756-57 (1999) (reviewing Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (1996) and Swire & Litan, *supra* note 177). For a more comprehensive discussion of the differences between the United States and European approaches, see Domingo R. Tan, Comment, Personal Privacy in the

Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union, 21 Loy. L.A. Int'l & Comp. L.J. 661 (1999).

[FN182]. See Samuelson, *supra* note 181, at 757-58.

[FN183]. *Id.* at 758.

[FN184]. See Andrews, *supra* note 180.

[FN185]. See *id.*

[FN186]. See Kaplan, *supra* note 148; see also International Safe Harbor Privacy Principles (Nov. 4, 1998) <<http://www.epic.org/privacy/intl/doc-safeharbor-1198.html>> (displaying the U.S. Dept. of Commerce's proposed safe harbor privacy principles in Attachment B).

[FN187]. For comprehensive coverage of this issue, see Swire & Litan, *supra* note 177 and Schwartz & Reidenberg, *supra* note 181. For a discussion of the conflict between "cookie" files and the Directive principles, see Victor Mayer-Schonberger, *The Internet and Privacy Legislation: Cookies for a Treat?*, 1 W. Va. J. L. & Tech. 1 (1997) <<http://www.wvjolt.wvu.edu/wvjolt/current/issue1/articles/mayer/mayer.htm>>. For the latest draft of the compromise between the United States and the E.U., see U.S. Dept. of Commerce Electronic Commerce Task Force (visited July 13, 2000) <<http://www.ita.doc.gov/td/ecom/menu.html>>. See also Kurtz, *supra* note 4, at 173 (discussing the negotiations between the E.U. and the United States).

[FN188]. Ayla Jean Yackley, *Safe Harbor Vote Delayed* (Apr. 17, 2000) <<http://www.wired.com/news/politics/0,1283,35406-2,00.html>>, <<http://www.wired.com/news/politics/0,1283,35406-2,00.html>>. The European Union and the United States have recently reached an agreement on safe harbor principles. See *U.S.-E.U. Data Privacy Deal Near* (June 5, 2000) <<http://www.salon.com/tech/wire/2000/06/05/privacy/index.html>>.

[FN189]. See Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1994); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994). As Paul Schwartz has pointed out, however, "the law in the United States today protects transactional data for the viewer of a film when rented at the video store, but not when seen over the Internet." Schwartz, *supra* note 19, at 1632 (footnote omitted). See Statement of Marc Rotenberg on the European Union Data Directive and Privacy Before the House of Representatives Committee on International Relations (May 7, 1998) <<http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html>>.

[FN190]. *Who Watches Your Credit?* (June 2, 1999) <http://cnnfn.cnn.com/1999/06/02/life/q_creditaccess/>.

[FN191]. See Andrews, *supra* note 180; see also Caruso, *supra* note 13 ("People and companies that sell personal data want to be able to collect and distribute it pretty much with abandon, and they fight like cornered weasels at even the suggestion of government regulation.").

[FN192]. Jeri Clausing, Administration Seeks Input on Privacy Policy (Nov. 6, 1998) <<http://www.nytimes.com/library/tech/98/11/cyber/articles/06privacy.html>>. See Statement of Marc Rotenberg on the European Union Data Directive and Privacy Before the House of Representatives Committee on International Relations (May 7, 1998) <<http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html>>; see also Schwartz, *supra* note 19, at 1638-40; Kurtz, *supra* note 4, at 171-72 (discussing the limitations of the FTC's ability to investigate corporate privacy practices).

[FN193]. See Stephen Labaton, White House and Agency Split on Internet Privacy (May 23, 2000) <<http://www.nytimes.com/library/tech/00/05/biztech/articles/23privacy.html>> ("Administration officials were decidedly lukewarm [to the FTC's proposal for legislation to protect consumer privacy on the Internet]. They said that the government should continue to rely on the industry to police itself and that the White House had a deeper interest in promoting privacy laws in other areas, including health care and financial services."); Remarks by the President on Financial Privacy and Consumer Protection (May 4, 1999) <http://www.epic.org/privacy/financial/clinton_remarks_5_99.html>.

The technological revolution now makes it easier than ever for people to mine your private, financial data for their profit. While some of your private financial information is protected under existing federal law, your bank or broker or insurance company could still share with affiliated firms information on what you buy with checks and credit cards--or sell this information to the highest bidder. This law, to put it mildly, is outdated and should be changed--to give you the right to control your financial information, to let you decide whether you want to share private information with anyone else. I look forward to working with members in the House and the Senate on this issue.

Id. (quoting President Clinton). See also Bill Raises Risk of Violating Medical Privacy, Physicians' Groups Say (July 22, 1999) <<http://www.contac.org/contaclibrary/rights12.htm>>; Declan McCullagh, New Medical Privacy Mandate (Oct. 29, 1999) <<http://www.wired.com/news/print/0,1294,32209,00.html>> (discussing legislative efforts to protect medical privacy); 2000-04-30 Remarks by President at Eastern Michigan University (Apr. 30, 2000) <<http://ofcn.org/cyber.serv/teledem/pb/2000/apr/msg00230.html>> (quoting President Clinton's commencement speech advocating for more consumer privacy rights and control over access to financial and medical records); Anne Gearan, Clinton Pushes for Consumer Rights, Dayton Daily News, May 1, 2000, at 3A.

Clinton said during a commencement address at Eastern Michigan University [that his] plan would require a company to tell customers it was going to share sensitive consumer information such as medical and insurance records, or lists of what people

buy and where they buy it. [He also said his plan] would give consumers the option not to have that information shared, and give consumers a new right to review their credit reports for errors.

Id.

[FN194]. See Labaton, *supra* note 193 ("Clinton administration officials today threw cold water on a proposal by the Federal Trade Commission for legislation to protect consumer privacy on the Internet.").

[FN195]. See *id.*

[FN196]. See William Matthews, Privacy Fears Prompt Study, Delay (May 22, 2000) <<http://www.cnn.com/2000/TECH/computing/05/22/new.privacy.study.idg/index.html>>.

Mike Hatch, the attorney general of Minnesota, was more blunt, saying Congress' record on privacy protection is not good. For example, when Congress passed the Gramm-Leach-Bliley Act, which was touted as protecting financial privacy, it actually gave banks more authority to trade in consumers' financial information than ever before, he said. Congress failed to meet an August 1999 deadline for passing medical records privacy legislation, leaving it to the Department of Health and Human Services to propose regulations.

Id. See also Daniel Verton, Efforts Made to Prevent Privacy Abuses Against U.S. Citizens (June 7, 1999) <<http://www.cnn.com/TECH/computing/9906/07/privacy.idg/>>;

HouseDemocraticMajority.Gov: Fueling the High-Tech Engine of Economic Growth and National Prosperity (Mar. 28, 2000) <<http://democraticleader.house.gov/media/speeches/readSpeech.asp?ID=12>> (displaying speech given by House Democratic Leader Richard Gephardt). The challenge of protecting the privacy and security of those who use the Internet to engage in e-commerce is significant and daunting in its scope. We can neither ignore this issue nor can we believe that a simple legislative fix will solve this problem. I support and encourage the self-regulatory efforts on the part of Internet businesses in the area of privacy, such as the Better Business Bureau and Trust-e, as well as the public efforts of the Federal Trade Commission. I also encourage industry to take a more active role in educating the public and members of Congress on its ongoing efforts to protect consumer privacy. But Congress cannot stand idly by as consumer confidence in e-commerce is eroded because of privacy concerns. If we must act, we should do so in a way that gives consumers a meaningful choice in how their personal data is used, while not impeding the ability of responsible businesses to collect data and information which is the lifeblood of e-commerce.

Id. See also eContract 2000 (visited June 4, 2000) <<http://www.freedom.gov/econtract/econtract2k.asp>> (quoting House Majority Leader Dick Armey, "We hereby pledge to continue our legislative and oversight efforts to remove the barriers to future innovation, competition, and growth. We assert that freedom is the answer, not government intervention."); Paul Shepard, GOP House Members See No Rush For New Internet Privacy Laws (May 22, 2000) <<http://www.cnn.com/2000/TECH/computing/05/22/new.privacy.study.idg/index.html>>.

www.cnn.com/2000/ALLPOLITICS/stories/05/22/netprivacy.ap/index.html>.

[FN197]. See 18 U.S.C §§ 2510-2522, 3121 (1994).

[FN198]. See Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1994).

[FN199]. See Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994).

[FN200]. See Fair Credit Reporting Act, 15 U.S.C. § 1681 (1994).

[FN201]. See Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320a-7e (2000); see also Statement by President William J. Clinton Upon Signing H.R. 3103 [Health Insurance Portability and Accountability Act], 32 Weekly Comp. Pres. Doc. 1480 (Aug. 26, 1996) ("It provides for... privacy protection recommendations for health information generally, and in the absence of additional legislation, regulations for privacy of health care claims information.").

[FN202]. 18 U.S.C. § 2721 (1994).

[FN203]. See *id.*; see also *Reno v. Condon*, No. 98-1464 (U.S. Jan. 12, 2000) (upholding Congress's constitutional authority to promulgate the Driver's Privacy Protection Act of 1994).

[FN204]. 5 U.S.C. § 552a (1994).

[FN205]. See *id.*; see also Statement of Marc Rotenberg on the European Union Data Directive and Privacy Before the House of Representatives Committee on International Relations (May 7, 1998) <[http:// www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html](http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html)>.

[FN206]. FTC--Self-Regulation and Privacy Online: A Report to Congress (July 13, 1999) <<http://www.ftc.gov/os/1999/9907/privacy99.pdf>>.

[FN207]. *Id.* See also Prepared Statement of the FTC on "Self-Regulation and Privacy Online" Before the House of Representatives (July 13, 1999) <<http://www.ftc.gov/os/1999/9907/pt071399.htm>> (displaying a copy of the prepared statement by the FTC that accompanied submission of the report to Congress).

[FN208]. See Jeri Clausing, Fate Unclear for FTC's Privacy Push (May 22, 2000) <[http:// www.nytimes.com/library/tech/00/05/biztech/articles/22priv.html](http://www.nytimes.com/library/tech/00/05/biztech/articles/22priv.html)>. In May of 2000, the FTC set forth new regulatory guidelines concerning some Internet information sharing. See Keith Perine & Aaron Pressman, FTC Publishes Internet Privacy Rule (May 12, 2000) <<http://www.thestandard.com/article/display/0,1151,15114,00.html?nl=mg>>. But when it takes effect on July 1, 2001, it will apply only to certain "financial institutions," such as online mortgage brokers, real estate brokers, and tax preparers. See *id.* These

entities will be required to provide customers with notice of their privacy policies, and refrain from disclosing financial information to "unaffiliated third parties" unless they satisfy various disclosure and opt out requirements, and affected consumers have not elected to opt out of the disclosures. See Privacy of Consumer Financial Information, 16 C.F.R. pt. 313 (2000).

[FN209]. See Labaton, *supra* note 193 (noting that in opposing the FTC's proposal for legislation to protect consumer privacy on the Internet, "[t]he Republican lawmakers found themselves in an odd alliance with officials from the White House and the Commerce Department"); see also FTC Wants More Privacy Regs (May 22, 2000) <<http://www.wired.com/news/print/0,1294,36516,00.html>> ("[The FTC's request for new powers to protect consumers' online privacy] faced an uncertain future in Congress--the legislation is strongly opposed by the e-commerce industry, disdained by Republicans, and lacking any known White House push."); Jen Muehlbauer, FTC Privacy Plan May Be DOA (May 22, 2000) <<http://www.thestandard.com/article/display/0,1151,15333,00.html>>; Keith Perine, The FTC Rethinks Privacy (May 29, 2000) <<http://www.thestandard.com/article/display/0,1151,15476,00.html>>.

[FN210]. See Labaton, *supra* note 193.

One study cited in the agency's report found that consumer privacy concerns resulted in as much as \$2.8 billion in lost online retail sales last year, while another suggested a potential loss of as much as \$18 billion by 2002, compared with a projected total of \$40 billion. "Internet commerce will not develop to the ultimate extent because people just will continue to not have confidence that their private information will be protected to the maximum," [FTC Chair] Pitofsky said.
Id.

[FN211]. TRUSTe: Building a Web You Can Believe In (visited May 28, 2000) <<http://www.truste.org>>.

[FN212]. BBB Online Privacy Program (visited June 4, 2000) <<http://www.bbbonline.org/businesses/privacy/index.html>>.

[FN213]. Online Privacy Alliance (visited May 28, 2000) <<http://www.privacyalliance.org>>.

[FN214]. Paul Schwartz expressed some optimism about seal programs, but noted that their weaknesses are "that privacy seal companies: (1) certify standards that may fall short of... fair information practice, (2) are limited in their enforcement powers, and (3) have brands that are not widely recognized at present." Schwartz, *supra* note 19, at 1694. He further observed that "[t]hese three shortcomings, unfortunately, all magnify each other." Id.

[FN215]. See Prepared Statement of the FTC on "Self-Regulation and Privacy Online" Before the House of Representatives (July 13, 1999) <<http://>

www.ftc.gov/os/1999/9907/pt071399.htm>.

In the Commission's view, the emergence of online privacy seal programs is a particularly promising development in self-regulation. Here, too, industry faces a considerable challenge. TRUSTe, launched nearly two years ago, currently has more than 500 licensees representing a variety of industries. BBBOnline, a subsidiary of the Council of Better Business Bureaus, which launched its privacy seal program for online businesses last March, currently has 42 licensees and more than 300 applications for licenses. Several other online privacy seal programs are just getting underway. Together, the online privacy seal programs currently encompass only a handful of all Web sites. It is too early to judge how effective these programs will ultimately be in serving as enforcement mechanisms to protect consumers' online privacy.

Id. See *The New E-Industry: Privacy* (Oct. 11, 1999) <<http://www.wired.com/news/business/0,1367,31841,00.html>>; see also Labaton, *supra* note 193 (discussing a recent FTC study determined that "only 8 percent of the most heavily visited Web sites displayed a seal of approval from one of the programs established by the industry").

[FN216]. See *The New E-Industry: Privacy* (Oct. 11, 1999) <<http://www.wired.com/news/business/0,1367,31841,00.html>> (quoting David Taylor, President, and CEO of *enonymous.com*, a TRUSTe competitor).

[FN217]. *RealNetworks* (visited June 17, 2000) <<http://www.realnetworks.com/>>.

[FN218]. See Sarah Robinson, *CD Software Is Said to Monitor Users' Listening Habits* (Nov. 1, 1999) <<http://www10.nytimes.com/library/tech/99/11/biztech/articles/01real.html>>; see also Reidenberg, *supra* note 175, at 777-78.

[FN219]. See Robinson, *supra* note 218; Marilyn Wheeler, *Targeted Real Ads a Real Nuisance* (May 22, 2000) <<http://www.zdnet.com/zdnn/stories/news/0,4586,2573314,00.html>>.

[FN220]. See Robinson, *supra* note 217.

[FN221]. See Lydia Lee, *The Privacy Police?* (Mar. 13, 2000) <<http://www.salon.com/tech/view/2000/03/13/truste/print.html>>. *RealNetworks* has since created two different privacy statements, one for their software and one for their website, the latter still bearing the TRUSTe seal. See *RealNetworks Consumer Software Privacy Statement* (visited July 18, 2000) <http://www.realnetworks.com/company/privacy/software.html?src=home_071400_nav> (displaying the software privacy policy); *RealNetworks Membership in the TRUSTe Program* (visited July 17, 2000) <http://www.realnetworks.com/company/privacy/index.html?src=home_071400_nav> (displaying the website privacy policy).

[FN222]. See Lee, *supra* note 221.

[FN223]. See *id.*; see also Kaitlin Quistgaard, *Honesty is the Best Policy* (Nov. 9, 1999) <<http://www.salon.com/tech/log/1999/11/09/truste/print.html>>.

[FN224]. eBay (visited June 4, 2000) <<http://www.eBay.com>>.

[FN225]. See BBB OnLine Privacy Program Dispute Resolution Decision 2000- 003 (eBay, Inc.) (visited June 4, 2000) <<http://www.bbbonline.org/businesses/privacy/dr/decisions/2000-003.html>>.

[FN226]. See *id.*

[FN227]. See *id.*

[FN228]. *Id.*

[FN229]. *Id.*

[FN230]. See, e.g., Reidenberg, *supra* note 175, at 777-78 (criticizing TRUSTe's seal and BBB Online's programs).

[FN231]. See Statement of Marc Rotenberg on the European Union Data Directive and Privacy Before the House of Representatives Committee on International Relations (May 7, 1998) <<http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html>> ("The most recent Harris poll found that 53% of Americans believe that 'Government should pass laws now for how personal information can be collected and used on the Internet.'"); see also Swire & Litan, *supra* note 175, at 179 ("There is undoubtedly strong public concern about privacy issues in the United States, especially with respect to the Internet. Eighty-seven percent of U.S. computer users report that they are concerned about privacy (56 percent are 'very concerned')." (citing Alan F. Westin & Danielle Maurici, *E-Commerce & Privacy: What Net Users Want* (June 1998) <<http://www.pwcglobal.com/gx/eng/svcs/privacy/images/E-Commerce.pdf>>, at vii)).

[FN232]. See Joseph I. Rosenbaum, Privacy On the Internet: Whose Information is it Anyway?, 38 *Jurimetrics J.* 565 (1998) (asserting that the U.S. notion of privacy is a "moving target," dependent on ever changing technological capabilities, societal values and cultural norms); Joshua B. Sessler, Note & Comment: Computer Cookie Control: Transaction Generated Information and Privacy Regulation on the Internet, 5 *J. L. & Pol'y* 627 (1997) (advocating for passage of personal information privacy protection legislation).

[FN233]. Jeffrey Obser, *Privacy is the Problem, Not the Solution* (June 21, 1997) <<http://www.salonmagazine.com/june97/21st/articleb970626.html>>.

[FN234]. See, e.g., Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-1010 (1994); Declan McCullagh, U.S. Wants Less Web Anonymity (Mar. 1, 2000) <<http://www.wired.com/news/print/0,1294,34659,00.html>>; Declan McCullagh, Clinton Favors Computer Snooping (Jan. 19, 2000) <<http://www.wired.com/news/print/0,1294,33779,00.html>>.

[FN235]. See Robert O'Harrow, Jr. & Liz Leyden, U.S. Helped Fund Photo Database of Driver IDs, Wash. Post, Feb. 18, 1999, at A1.

[FN236]. See *id.*

[FN237]. See Coalition Letter on Federal Databases (Feb. 17, 1999) <http://www.epic.org/privacy/databases/joint_letter_2_99.html>.

[FN238]. See Berman & Mulligan, *supra* note 74, at 560.

[FN239]. Eve Gerber, Account Overwrought (May 12, 1999) <<http://slate.msn.com/HeyWait/99-05-12/HeyWait.asp>>.

[FN240]. See Brown, *supra* note 61 (noting SmartGirl founder Isabel Walcott sees her website as a pro-girl cause, and claims girls visiting site "feel really empowered").

[FN241]. See Williamson, *supra* note 95.

[FN242]. Kang, *supra* note 74, at 1248.

[FN243]. Schwartz, *supra* note 19, at 1661.

[FN244]. *Id.* at 1661.

[FN245]. See *id.* at 1662.

[FN246]. See Williamson, *supra* note 95.

[FN247]. See *id.* (quoting Seth Godin, VP of direct marketing at Yahoo and Author of Permission Marketing, for the proposition that without the inducement of a specific reward or benefit, consumers will not provide personal information like phone numbers).

[FN248]. See Tedeschi, *supra* note 108.

[FN249]. *Id.* (quoting William Bryant, Chairman of Qpass, a company that has developed a billing system for e-commerce sites).

[FN250]. See Kang, *supra* note 74, at 1246-67 (discussing the trade offs between privacy and the ability to participate in the online market). For an expansive

discussion of how little privacy people have in any sphere, see A. Michael Froomkin, *The Death of Privacy?*, 52 *Stan. L. Rev.* 1461 (2000).

[FN251]. Tedeschi, *supra* note 80. See also Marcia Stepanek, *The Privacy Backlash* (Mar. 4, 1997) <<http://www.salonmagazine.com/march97/news/news2970304.html>> (quoting Mark Rotenberg's interpretation of parents' negative reaction to a school district's proposal to create a database with 1,200 pieces of information on each school student, including information about medical histories and family income). But see Tedeschi, *supra* note 18 ("[A]ccording to a study released last week by Privacy and American Business in conjunction with the Opinion Research Corporation, 53% of Net users say they would participate in an Internet program that exchanged benefits for information, if the program fully explained how that information would be used.").

[FN252]. See Caruso, *supra* note 13 (referencing 1997 Georgia Tech survey).

[FN253]. Berman & Mulligan, *supra* note 74, at 564-65 (footnotes omitted).

[FN254]. Matt Richtel, *Survey Shows Few Trust Promises on Online Privacy* (Apr. 17, 2000) <<http://www.nytimes.com/library/tech/00/04/biztech/articles/17data.html>>. See generally Lorrie Faith Cranor et al., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy* (Apr. 14, 1999) <<http://www.research.att.com/projects/privacystudy/>> (discussing results of an extensive survey of Internet users).

[FN255]. Michael Stroud, *Gizmos Gets a Hand from Marketers* (May 25, 2000) <<http://www.wired.com/news/print/0,1294,36484,00.html>>.

[FN256]. See Karen J. Bannan, *Marketers Try Infecting the Internet* (Mar. 2, 2000) <<http://www.nytimes.com/library/tech/00/03/cyber/articles/22viral.html>>.

[FN257]. See Stroud, *supra* note 255.

[FN258]. *Id.* (quoting John Sculley, former Apple and Pepsi executive).

[FN259]. *Id.* (quoting Evan Hendricks, editor of website *Privaytimes.com*).

[FN260]. See Kang, *supra* note 74, at 1260.

[FN261]. Leonard, *supra* note 83. See also Rob Fixmer, *Traveling the Web Without Leaving Footprints* (Aug. 16, 1999) <<http://www.nytimes.com/library/tech/99/08/biztech/articles/16data.html>> ("Little wonder that a recent Harris poll for Business Week found that fears of losing privacy were the top reason people decided not to go online and that among those who do, only three out of 10 give valid information when asked to register at a site.").

[FN262]. See Bob Tedeschi, *Web Publishers, Advertisers Square Off on Ownership of*

Customer Data (Nov. 8, 1999) <<http://www.nytimes.com/library/tech/99/11/cyber/commerce/08commerce.html>>; Kathryn Kranhold & Michael Moss, Companies Fight to Protect Cookies (Mar. 20, 2000) <<http://www.zdnet.com/zdn/stories/news/0,4586,2470654,00.html>>.

[FN263]. See Hiawatha Bray, Going Too Far to Stop Stealing, Boston Globe, July 15, 1999, at D1.

[FN264]. See Kang, *supra* note 74, at 1211.

[FN265]. *Id.* (footnotes omitted).

[FN266]. Laurie J. Flynn, Software Ad Blockers Challenge Web Industry (June 7, 1999) <<http://www.nytimes.com/library/tech/99/06/biztech/articles/07adco.html>>.

[FN267]. See *id.* For discussion of "cookie files," see *infra* Part VIII.B.

[FN268]. Flynn, *supra* note 266.

[FN269]. *Id.* (quoting Scott Mathias, managing editor of ITVWorld.com).

[FN270]. *Id.* (quoting Charles Arruda, a vice president of Channelseek).

[FN271]. See Bob Tedeschi, CDNow Struggles to be Heard (May 24, 1999) <<http://www.nytimes.com/library/tech/99/05/cyber/commerce/24commerce.html>>.

[FN272]. See Chris Oakes, Mouse Pointer Records Clicks (Nov. 30, 1999) <<http://www.wired.com/news/print/0,1294,32788,00.html>>.

[FN273]. See *id.* (explaining how software analyst Richard Smith, after discovering Comet's web tracking practices, wrote Comet a letter of complain leading Comet to subsequently published a new disclosure notice in the privacy policy section of its web site).

[FN274]. See Kranhold & Moss, *supra* note 262.

[FN275]. See *id.*

[FN276]. See Hansell, *supra* note 79, at A24. To disable cookies on the most recent version of Microsoft Internet Explorer, go to the Tools menu and select Internet Options. Go to the Security section and select Custom Level. Scroll down to the Cookies portion of the menu and select Disable. On the most recent version of Netscape Navigator, go to the Edit menu and select Preferences. Click on Advanced and the Cookies options will be displayed. Then, select Disable cookies.

[FN277]. See Bray, *supra* note 78, at G6 .

[FN278]. See, e.g., Peter Wayner, A Tool for Anonymity on the Internet (Dec. 16, 1999) <<http://www.nytimes.com/library/tech/99/12/circuits/articles/16zero.html>> (describing Zero Knowledge); E-Shopping With Privacy (Oct. 4, 1999) <<http://www.wired.com/news/print/1,1294,31665,00.html>> (describing anonymous.com); Fixmer, supra note 261 (describing Web Incognito, a privacy service offered by Privada); Hopper, supra note 77 (describing Privacy Companion); Kang, supra note 74, at 1244-45 (discussing encryption technologies); John Borland, Anti-Napster Fight Takes Aim at Online Anonymity (May 31, 2000) <http://dailynews.yahoo.com/h/cn/20000531/tc/anti-napster_fight_takes_aim_at_online_anonymity_1.html> (discussing anonymizers, Freenet and Zero Knowledge); Kurtz, supra note 4, at 170-71 (discussing the Platform for Privacy Preferences (P3P)).

[FN279]. Jerry Kang has pointed out that "anonymity comes in shades." Kang, supra note 74, at 1209. Even when a specific person is not identified facially, "the individual may be identifiable in context or with additional research." Id.

[FN280]. Schwartz, supra note 19, at 1689-90 (footnote omitted).

[FN281]. See id. at 1690-96.

[FN282]. See Caruso, supra note 13; see also Chris Oakes, PrivaSeek Seeks Attention (Aug. 12, 1999) <http://www.wired.com/news/print_version/business/story/21221.html>; James Glave, The Dawn of the Infomediary (Feb. 24, 1999) <http://www.wired.com/news/print_version/business/story/18094.html>.

[FN283]. See The New E-Industry: Privacy (Oct. 11, 1999) <<http://www.wired.com/news/business/0,1367,31841,00.html>>.

[FN284]. Swire & Litan, supra note 175, at 8.

[FN285]. For a detailed discussion of the economics of "opt in" and "opt out" data collection scenarios, see Jeff Sovern, Opting In, Opting Out, Or No Options At All: The Fight For Control of Personal Information, 74 Wash. L. Rev. 1033 (1999).

[FN286]. See William Safire, On Language: Opt In, Outing the Inside Lingo of Privacy (Dec. 19, 1999) <<http://nytimes.com/library/magazine/home/19991219mag-onlanguage.html>>.

[O]pt out puts the burden on the individual, to click on a box that says, "No--you cannot disclose my personal information." Most people don't know enough to care, or are easily duped into not checking the box by offers of gifts or services--and thereby unwittingly make their purchasing decisions and their lives an open book. Id.

[FN287]. See AOL Privacy Policy Angers Critics (Dec. 1, 1999) <<http://www.usatoday.com/life/cyber/tech/ctg789.htm>>; see also Christopher Sandlund, I

Told You Once... (Nov. 23, 1999) <<http://www.salon.com/tech/log/1999/11/23/aol/print.html>>.

[FN288]. See Sandlund, *supra* note 287.

[FN289]. See *id.*

[FN290]. See Stephanie Olsen & Evan Hansen, Group Calls Privacy Protection Measures Ineffective (May 18, 2000) <<http://news.cnet.com/news//0-1005-200-1891902.html?tag=st.cn.sr.ne.1>>.

[FN291]. See *id.*

[FN292]. See *id.*

[FN293]. See iWon Privacy Policy (visited June 4, 2000) <http://www.iwon.com/home/companyinfo/privacy/privacy_overview/0,11882,,00.html>.

[FN294]. See *id.*

[FN295]. *Id.*

[FN296]. See *id.*

[FN297]. See *id.*

[FN298]. See *id.*

[FN299]. See *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1240 (10th Cir. 1999); see also Court Won't Review Phone Data Ruling (June 5, 2000) <<http://www.nytimes.com/reuters/business/business-court-teleco.html>> (discussing the United States Supreme Court's decision not to review the 10th Circuit's decision).

[FN300]. See discussion *supra* Part VIII.C.3. But see Lydia Lee, Opt-in Rules! (Mar. 6, 2000) <<http://www.salon.com/tech/view/2000/03/06/moore/index.html>>.

[FN301]. See discussion *supra* text accompanying note 261; see also Joanna Glasner, Debating How to Get Your Data (Mar. 2, 2000) <<http://www.wired.com/news/print/0,1294,34685,00.html>> ("If an opt-in policy took effect, DoubleClick would need permission from users before it could collect information about them. If that happened, DoubleClick would have fewer profiles and would forgo extrapolating general information about users.").

[FN302]. See *State St. Bank & Trust Co. v. Signature Fin. Group*, 149 F.3d 1368 (Fed. Cir. 1998), cert. denied, 525 U.S. 1093 (1999).

[FN303]. See 17 U.S.C. § 302 (1999).

[FN304]. See Lydia Pallas Loren, Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and the Importance of the Willfulness Requirement, 77 Wash. U. L. Q. 835, 856-60 (1999).

[FN305]. See id. See, e.g., zPatents.com: Buy & Sell Inventions & Patents! Inventions for Sale & Auction! (visited July 19, 2000) <[http:// www.zpatents.com/services.htm](http://www.zpatents.com/services.htm)> (displaying the web page of a company dedicated to helping inventors sell or license their patents).

[FN306]. See Federal Trademark Dilution Act, 15 U.S.C. § 1125 (1997); Lynda J. Oswald, "Tarnishment" and "Blurring" under the Federal Trademark Dilution Act of 1995, 36 Am. Bus. L.J. 255 (1999).

[FN307]. See, e.g., Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763 (1992) (holding that the certain appearance of a Mexican food restaurant was protectable trade dress under the Lanham Act).

[FN308]. See 18 U.S.C. §§ 1832-1839 (Supp. IV 1999).

[FN309]. See Malla Pollack, The Right to Know?: Delimiting Database Protection at the Juncture of the Commerce Clause, the Intellectual Property Clause, and the First Amendment, 17 Cardozo Arts & Ent. L.J. 47, 48-50 (1999) (discussing the Collections of Information Antipiracy Act).

[FN310]. Litman, *supra* note 121, at 1725.

[FN311]. Rosemary J. Coombe, Symposium: Innovation and the Information Environment: Left Out on the Information Highway, 75 Or. L. Rev. 237, 239 (1996).

[FN312]. Cf. Bray, *supra* note 263, at D1 (discussing the criticisms of legislation aimed at protecting databases).

[FN313]. See Collections of Information Antipiracy Act, H.R. 354, 106th Cong. (1999), H.R. Rep. No. 106-349, pt. 1 (1999). This bill was introduced January 19, 1999 by Howard Coble, Chairman of the House Subcommittee on Courts and Intellectual Property. H.R. 354 is virtually identical to the Collections of Information Act, H.R. 2652, 105th Cong. (1998), H.R. Rep. No. 105-525 (1998), which the House passed twice, once as a stand alone bill and once as part of the House's version of the Digital Millennium Copyright Act.

[FN314]. The "sweat of the brow" doctrine, the idea that effort should be rewarded, was the justification some courts used for according otherwise uncopyrightable facts in databases copyright protections. The Supreme Court, in Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340 (1991), overturned this doctrine.

[FN315]. See Schwartz & Reidenberg, *supra* note 181, at 344 ("[D]ue to the commercial value of profile lists, direct marketing companies will take careful measures to protect their business assets.").

[FN316]. Litman, *supra* note 121, at 1734 (footnote omitted).

[FN317]. See Schwartz & Reidenberg, *supra* note 181, at 326 and accompanying notes.

[FN318]. But see Litman, *supra* note 121, at 1730-31.

[With respect to justifications for exclusive control over trademarks] there is the perennially popular justification of desert. Producers have invested in their trade symbols, the argument goes; they have earned them, so they're entitled to them. But so have we. The argument that trade symbols acquire intrinsic value--apart from their usefulness in designating the source-- derives from consumers' investing those symbols with value for which they are willing to pay real money.... To the extent... that the impulse to protect something beyond any prevention of consumer confusion derives from the perception that this thing has value, that it is something people want to buy, then giving its purveyor intellectual property protection is the wrong response. If the thing itself is valuable, if it is in some sense itself a product, then we want other purveyors to compete in offering it to consumers in their own forms and on their own terms. Competition is, after all, the premise of the system. Without competition, none of the rest of the rules make any practical sense.
Id. (footnotes omitted).

[FN319]. Niva Elkin-Koren has written that the power to control access to information has the power to impose specific meanings. See Elkin-Koren, *supra* note 123, at 236. Denying commercial access to personal data is a mechanism by which individuals express personal meaning, and perhaps sense of worth.

[FN320]. Roberta Rosenthal Kwall, The Right of Publicity vs. The First Amendment: A Property and Liability Rule Analysis, 70 *Ind. L.J.* 47, 70 (1994).

[FN321]. The United States Supreme Court first recognized the common law tort of misappropriation in International News Service v. Associated Press, 248 U.S. 215 (1918), in order to protect "quasi property" interests. In International News Service, the defendant sold its publishing customers news stories plaintiff had gathered and written. See *id.* at 230. The Court upheld an injunction against defendant, holding that since plaintiff had gathered news by its own enterprise and expense it had a quasi-property interest in its product; that the defendant's appropriation thereof was unfair competition. See *id.* at 242. This holding expanded the principle of unfair competition beyond misrepresentation to embrace misappropriation. Tortious "misappropriation" has three basic elements: (1) the plaintiff has created a "thing" through the substantial investment of money, time, and effort such that the "thing" can be characterized as "property"; (2) the defendant has misappropriated this "property" without

compensating the plaintiff for its investment; and (3) the plaintiff has been injured by the misappropriation. Thomas McCarthy, Trademarks and Unfair Competition § 10.25. See also J.A. Brundage Plumbing & Roto-Rooter v. Massachusetts Bay Ins. Co., 818 F. Supp. 553, 557 (W.D.N.Y. 1993) (holding "misappropriation of an advertising idea" means "the wrongful taking of the manner by which another advertises its goods and services").

[FN322]. Samuelson, *supra* note 181, at 770 (citation omitted). See also Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 *Geo. L.J.* 2381 (1996).

[FN323]. Samuelson, *supra* note 181, at 771 (footnote omitted).

[FN324]. See Pamela Samuelson, *Privacy as Intellectual Property?*, 52 *Stan. L. Rev.* (forthcoming 2000) (manuscript at 10-18, on file with author).

[FN325]. See *id.* (manuscript at 13, on file with author).

[FN326]. See *id.* (manuscript at 23, on file with author). She also raises the intriguing possibility of attributing some form of "moral rights" to personal information. See *id.* (manuscript at 18, on file with author).

[FN327]. *Id.* (manuscript at 27, on file with author).

[FN328]. See *id.*

[FN329]. 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.* (forthcoming 2000) (manuscript at 6-7, on file with author).

[FN330]. See *id.* (manuscript at 2-3, on file with author).

[FN331]. See *id.* (manuscript at 7, on file with author).

[FN332]. See *id.* (manuscript at 8, on file with author).

[FN333]. See *id.* (manuscript at 9, on file with author).

[FN334]. See *id.* (manuscript at 9, on file with author).

[FN335]. See *id.* (manuscript at 9-10, on file with author).

[FN336]. But see Rochelle Cooper Dreyfuss, *Warren and Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 *Stan. Tech. L. Rev.* VS 8 <http://stlr.stanford.edu/STLR/Symposia/Privacy/99_VS_8/> ("[T]he fit between what intellectual property provides and what privacy advocates want is imperfect....").

[FN337]. Jeff Howe, Copyrighting the Book of Life (Apr. 12, 2000) <<http://www.feedmag.com/dna/bookoflife.html>>.

[FN338]. Novelty, utility, and non-obviousness are the requirements for patentability. See 35 U.S.C. §§ 101, 102 (1994); 35 U.S.C. § 103 (1995). Patents are generally recognized to be a stronger form of intellectual property protection than copyrights, though they last for a substantially shorter period of time.

[FN339]. The minimum threshold for copyrightability is creativity and originality, as articulated by the Supreme Court in Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 347 (1991).

[FN340]. For an example of exclusive rights derived from authorship, see 17 U.S.C. § 106 (1994). Not everyone agrees that authorship linearly bestows ownership and control. For example, Marci Hamilton has written that copyright law is product-centered, rather than author-centered. See Marci A. Hamilton, *The Historical and Philosophical Underpinnings of the Copyright Clause*, Occasional Papers in Intellectual Property No. 5 (Cardozo School of Law 1999) ("The more commodified the product, the more it is capable of traveling through a culture and its streams of commerce with value attached but without the identity or controlling hand of the author attached.").

[FN341]. See Feist, 499 U.S. at 344.

[FN342]. See 17 U.S.C. § 101 (1994) (defining "compilations").

[FN343]. See *id.*

[FN344]. See Craig Joyce et al., *Copyright Law* 232-33 (4th ed. 1998) & 728- 30 (Supp. 1999) (discussing protection of data compilations).

[FN345]. See 17 U.S.C. § 102 (1994) (defining copyrightable subject matter).

[FN346]. See *id.* § 101 (defining "compilations").

[FN347]. See *id.* § 103 (1994) (discussing extent of copyrightability of compilations).

[FN348]. See 17 U.S.C. § 506 (Supp. 1997) (criminalizing certain types of copyright infringement).

[FN349]. Mark A. Lemley, *The Modern Lanham Act and the Death of Common Sense*, 108 *Yale L.J.* 1687, 1700 (1999).

[FN350]. 15 U.S.C. §§ 1051-1065 (1994).

[FN351]. See John Gibeaut, *Image Conscious*, A.B.A. J., June 1999, at 47, 48.

[FN352]. Litman, *supra* note 121, at 1725-26 (footnotes omitted).

[FN353]. See 15 U.S.C. § 1058 (1994).

[FN354]. Lemley, *supra* note 349, at 1696 (footnotes omitted).

[FN355]. At present, publicity rights "differ widely in the approximately 25 states that recognize them either by statute or common law." Gibeaut, *supra* note 351, at 48.

[FN356]. But see Alice Haemmerli, Whose Who? The Case for a Kantian Right of Publicity, 49 *Duke L.J.* 383, 406-07 (discussing how Judge Jerome Frank of the Second Circuit severed the right of publicity from the right of privacy in Haelen Labs, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866 (1953)).

[FN357]. See Rosemary J. Coombe, *Publicity Rights and Political Aspiration: Mass Culture, Gender Identity and Democracy*, 26 *New Eng. L. Rev.* 1221, 1226 (1992).

[FN358]. Dreyfuss, *supra* note 336.

[FN359]. But see Carl S. Kaplan, *Celebrities Have Trouble Protecting Their Names Online* (July 30, 1999) <<http://www.nytimes.com/library/tech/99/07/cyber/cyberlaw/30law.html>> (discussing how several celebrities have difficulty in protecting their names online).

[FN360]. See Roberta Rosenthal Kwall, Fame, 73 *Ind. L.J.* 1, 31 (1997) ("The growth of [television] has... contributed to the phenomenon of making temporary celebrities out of 'ordinary folks.'").

[FN361]. See *id.* at 29 n.150.

[FN362]. Gibeaut, *supra* note 351, at 47.

[FN363]. See Kwall, *supra* note 360, at 32 ("[I]n the future everyone will be world famous for fifteen minutes.") (quoting Andy Warhol). But see Michael Madow, *Private Ownership of Public Image: Popular Culture and Publicity Rights*, 81 *Calif. L. Rev.* 125, 137 n.39 (1993) ("[T]he right of publicity is in reality special celebrity right.").

[FN364]. Haemmerli, *supra* note 356, at 418 (footnote omitted).

[FN365]. See Madow, *supra* note 363, at 129; Coombe, *supra* note 357, at 1237; Samuelson, *supra* note 181, at 772. But see Haemmerli, *supra* note 356, at 431- 42 (analyzing the criticisms of publicity rights, namely those of Professors Madow and Coombe).

[FN366]. Madow, *supra* note 363, at 144-45 (footnotes omitted) (emphasis added).

[FN367]. Litman, *supra* note 121, at 1733.

[FN368]. Sheldon W. Halpern, The Right of Publicity: Maturation of an Independent Right Protecting the Associative Value of Personality, 46 *Hastings L.J.* 853, 872 (1995).

[FN369]. See Madow, *supra* note 363, at 129.

[FN370]. Kang, *supra* note 74, at 1218 (footnotes omitted).

[FN371]. At present, the First Amendment offers some protection to "authors without authorization" who write about celebrities, but is less likely to shield those who use images of famous people, because a nonpermissive utilization of words gets more First Amendment protection than an unauthorized use of pictures or sounds, especially when digital technologies have been employed. When Dustin Hoffman sued Los Angeles Magazine for merging an old photograph of him with a contemporary photograph of a fashion model, the judge found that the photographs contained in the disputed feature, which also featured the merged visages of other entertainers, "were manipulated and cannibalized to such an extent that the celebrities were commercially exploited and were robbed of their dignity, professionalism and talent. To be blunt, the celebrities were violated by technology." Hoffman v. Capital Cities/ABC, Inc., 33 F. Supp. 2d 867, 873 (C.D. Cal. 1999).

[FN372]. See Madow, *supra* note 363, at 130 n.12.

[FN373]. See Avrahami's Trial Brief: *U.S. News & World Report v. Avrahami* (visited June 17, 2000) <http://www.epic.org/privacy/junk_mail/trial_brief.txt>.

[FN374]. See *id.*

[FN375]. *Id.*

[FN376]. Va. Code Ann. § 8.01-40 (A) (Michie 1995).

[FN377]. See Avrahami's Trial Brief: *U.S. News & World Report v. Avrahami* (visited June 17, 2000) <http://www.epic.org/privacy/junk_mail/trial_brief.txt> (citing to Lavery v. Automation Management Corp., 360 S.E.2d 336, 342 (Va. 1987) and Town & Country Properties v. Riggins, 457 S.E.2d 356, 364 (Va. 1995)).

[FN378]. See Avrahami's Trial Brief: *U.S. News & World Report v. Avrahami* (visited June 17, 2000) <http://www.epic.org/privacy/junk_mail/trial_brief.txt>.

[FN379]. O'Harrow Jr. & Leyden, *supra* note 235, at A1. It should be noted that the

constitutionality of the Driver's Privacy Protection Act of 1994, 18 U.S.C. §§2721-2725 (2000), was upheld in *Reno v. Condon*, No. 98- 1464 (U.S. Jan. 12, 2000), in which Chief Justice Rehnquist wrote that the Act, which bars states from disclosing personal information obtained from their licensed drivers, simply "regulates the States as owners of databases." *Id.* It was reported that in the oral argument, "several justices noted with irritation that a few states earned tens of millions of dollars from disclosing this personal data to mass marketers." David G. Savage, *The 5-4 Federalism Chasm*, A.B.A. J., March 2000, at 37.

[FN380]. See *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999); see also Court Won't Review Phone Data Ruling (June 5, 2000) <<http://www.nytimes.com/reuters/business/business-court-teleco.html>> (discussing the United States Supreme Court's decision not to review the 10th Circuit's decision).

[FN381]. See *U.S. West, Inc.*, 182 F.3d at 1240.

[FN382]. See Volokh, *supra* note 329.

[FN383]. See *id.* (manuscript at 11, on file with author).

[FN384]. See *id.* (manuscript at 12, on file with author).

[FN385]. See *id.*

[FN386]. See *id.*

[FN387]. 471 U.S. 539 (1985).

[FN388]. See *id.* at 542-43.

[FN389]. See *id.* at 569.

[FN390]. See *id.* at 568.

[FN391]. See *id.* at 565-66.

[FN392]. See Volokh, *supra* note 329 (manuscript at 13, on file with the author).

[FN393]. Trademarks that become generic terms for given products through widespread use lose trademark protection. For example, Thermos was a trademark for a particular brand of insulated beverage container, but is now a generic term used to describe any insulated beverage container, and no longer serves a source identifying function. Thermos has therefore "committed genericide."

[FN394]. See, e.g., Lori Schlotfeldt, *Letters to Spy*, *Spy Mag.*, Aug. 1989, at 20 (quoting member of the Customer Relations Dept. of Edward Lowe Industries, the

inventor of Kitty Litter, "In the article in question, KITTY LITTER(R) Brand was referred to in a generic sense. As KITTY LITTER(R) Brand is a registered trademark for a specific premium cat box filler manufacture by Edward Lowe Industries Inc., any use of the name other than as shown here is incorrect...").

[FN395]. See, e.g., Craig Bicknell, *Site No Longer Bugs Terminex*, (Mar. 11, 2000) <<http://www.wired.com/news/print/0,1294,34906,00.html>>; Kathleen Melymuka, *Ford Motors, Web Author Spar in Court* (Aug. 31, 1999) <<http://www.cnn.com/TECH/computing/9908/31/ford.idg/index.html>>; *Dunkin' Donuts Buys Out Critical Web Site* (Aug. 27, 1999) <<http://www.nytimes.com/library/tech/99/08/cyber/articles/27dunkin.html>>; Paul Brandus, *Hot Water: Starbucks Sues a Citizen* (June 1, 2000) <<http://www.salon.com/business/feature/2000/06/01/starbuckssuit/print.html>>; Sandy Lawrence Edry, *Furby Flap* (June 9, 1999) <http://www.newsweek.com/nw-srv/tnw/today/cs/cs01tu_1.htm>.

[FN396]. See Karen S. Frank & Michael J. Higgins, *Fair Use: In the Courts and Out of Control?* 411 PLI/Pat 1, 3 (1995) (citing H.R. Rep. No. 94-1476, at 65 (1976)). Although the courts have considered and ruled upon the fair use doctrine over and over again, no real definition of the concept has ever emerged. Indeed, since the doctrine is an equitable rule of reason, no generally applicable definition is possible, and each case raising the question must be decided on its own facts. *Id.* See also James J. Marcellino & Melise Blakeslee, *Fair Use in the Context of a Global Computer Network--is a Copyright Grab Really Going On?*, 6 *Info. & Comm. Tech. L.* 137 (1997) (discussing how fair use may balance between Internet content providers' rights and benefits to Internet service providers, bulletin board operators and end-users).

[FN397]. See *Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 589-90 (Brennan, J., dissenting).

[FN398]. *Sony Corp. of Am. v. Universal City Studios*, 464 U.S. 417, 429 (1984).

[FN399]. See *id.* at 429 & n.10; see also Albert D. Spalding, *Fair Use of Research and Course Packets in the Classroom*, 31 *Am. Bus. L.J.*, 447, 449-50 (1993); Robert A. Kreiss, *Accessibility and Commercialization in Copyright Theory*, 43 *UCLA L. Rev.* 1, 20 (1995); Jessica Litman, *Revising Copyright Law for the Information Age*, 75 *Or. L. Rev.* 19, 31 (1996). Cf. Barbara Friedman, *From Deontology to Dialogue: The Cultural Consequences of Copyright*, 13 *Cardozo Arts & Ent. L. J.* 157, 160 (1994) (arguing that despite the consequentialist moorings of American law, much of contemporary copyright theory is based on deontological theories of personality or natural rights).

[FN400]. See *American Geophysical Union v. Texaco, Inc.*, 37 F.3d 881 (2d Cir. 1994).

[FN401]. I am perfectly willing to give a royalty free partial license to my friends, and to at least some of my relatives. They can have my address and phone number, occupation, date of birth, and number of children. They do not need to know my income range, though, or anything about my recent purchases. I am less inclined to give educational institutions a free ride. After I have paid them thousands of dollars in tuition, why should my alma maters be allowed access to my data for free? I would require only a modest royalty to appear in an alumni directory, as doing so will undoubtedly provide me with profitable exposure to other potential licensors. I would demand a much larger payment if a university wanted to use my personal data to solicit donations from me, especially if they planned to call during the dinner hour.

[FN402]. See Coombe, *supra* note 357, at 1237.

[FN403]. See, e.g., Ann Bartow Educational Fair Use in Copyright: Reclaiming the Right to Photocopy Freely, 60 U. Pitt. L. Rev. 149 (1998) (discussing the scope of the fair use defense).

[FN404]. See Jonathan M. Winer, Too Much Privacy? (May 8, 2000) <<http://www.thestandard.com/article/display/0,1151,14781,00.html>>.