Richmond Journal of Law and Technology

Volume 6 | Issue 1 Article 3

1999

Who Leads at Halftime?: Three Conflicting Visions of Internet Privacy Policy

Karl D. Belgum

Volume VI, Issue 1, Symposium 1999

Who Leads at Half-time? Three Conflicting Visions of Internet Privacy Policy

by Karl D. Belgum[*]

Cite As: Karl D. Belgum, *Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy*, 6 RICH. J.L. & TECH. 1, (Symposium 1999) <>.[**]

Table of Contents:

I. Introduction

II. Threats to Privacy Online

III. The Current State of Privacy Regulation

IV. Critiques of Privacy Policy

V. Who Leads at Halftime?: Current Privacy Initiatives in the United States

VI. Conclusion

I. Introduction

{1} Concern about privacy on the Internet runs high, but the prescriptions for treatment vary widely. Privacy advocates seek different goals when formulating policy proposals. Some seek to protect individuals and society from the effects of loss of privacy, including the loss of human dignity. Others seek to encourage the development of online markets in personal information, so that consumers can profit from their own information, rather than giving it away. Still, others seek primarily to promote the growth of e-commerce, and see privacy fears as a threat to that goal. These goals are fundamentally inconsistent, and that inconsistency is obscured by the fact that much of the current debate about online privacy focuses on the tools of regulation, rather than the goals for which regulation is sought.

{2} Part I of this article will briefly survey the current concern over online privacy, why it is considered important, and how it is threatened. Part II will identify three distinct perspectives in current thinking about Internet privacy, which will be defined as the "dossier society pessimists", the "market opportunists", and the "privacy peacemakers". Part III reviews current policy initiatives regarding online privacy to see which of the schools of thought identified above predominates in the public policy debate. That section concludes that such initiatives generally fall into the "privacy peacemaker" camp, aiming to control the worst and most visible abuses of privacy, so as to avoid impairing the growth of e-commerce. Current initiatives are not aimed at promoting the goals of the market opportunists, who hope to see markets in personal information develop online; nor are they aimed at averting or reversing the advent of dossier society so feared by the dossier society pessimists.

II. Threats to Privacy Online

A. Public concern over online privacy

{3} From the perspective of many policymakers, the perception that privacy is at risk online is as important as the reality. Public opinion polling data are frequently cited to support the need for privacy regulation.[1] One of the most frequently-cited surveys is an Equifax/Harris poll reported in the March 1998 issue of *Business Week*, which indicated that two-thirds (2/3) of non-Internet users said they would be more likely to begin using the Internet if their privacy were assured.[2] Non-users cited privacy as the most important reason for staying off the Internet -- more important than cost or technical complexity.[3] Of those using the Internet, seventy-eight (78) percent said they would use it more if their privacy were guaranteed.[4]

{4} Not only do the polling data indicate that individuals view privacy as a fundamental value, they also highlight the concern among Internet promoters that privacy fears may slow the public's acceptance of e-commerce, which is an important practical reason for the government to address those concerns.[5]

{5} While the majority of commentators accept the polling data at face value, a dissenting position also exists. The dissenters point out that techniques for protecting online privacy have existed for years, but are not well utilized. Anonymizer services have been available for some time that mask the identity of online users, for a nominal cost. Most users do not take advantage of them;[6] however, either because of the perceived technical complexity of using them, the price, or the mere fact that users do not care as much about privacy as advocates contend.[7] In addition, polling questions which simply ask "do you care about privacy online" are bound to generate more positive responses than surveys that ask respondents to rank privacy in importance, compared with other public and private issues.[8] Regardless of these observations, however, the perceived wisdom of policymakers continues to be that privacy is an important value to Americans which must be safeguarded if e-commerce is to achieve its full potential.[9]

B. Nature of the Threat

{6} The Internet raises new threats to privacy, and enhances old threats as a result of the increased data processing capability of computers combined with the data gathering and dissemination potential of the Internet itself. As the Federal Trade Commission staff noted in a 1998 report on one of its privacy workshops:

> Globalization and new technologies are radically changing the contours of the late Twentieth Century marketplace. In the 1980's, the personal computer revolution enhanced the ability of government, industry and consumers to capture a vast array of personal information automatically. In the 1990's, the technology underlying the Internet is making it even easier and

> less expensive to gather, store, analyze, transmit and reuse personal information in ways that were unimaginable just a few years ago.[10]

{7} Personal data, such as address, phone number, income, property value, and marital status have always been available to those willing to dig.[11] The Internet can make it possible for a much wider class of persons -- essentially all Internet users -- to gain access to similar types of personal information at little or no cost.

{8} "Profiling" is the term used to denote the gathering, assembling, and collating of data about individuals in databases which can be used to identify, segregate, categorize and generally make decisions about individuals known to the decisionmaker only through their computerized profile.[12]

{9} There is a perception that such activities conducted online pose a greater threat to privacy than similar activities in the off-line world. Data obtained and recorded in digital form can be preserved indefinitely, and the perception that a permanent record of our movements and actions is recorded and available to posterity is oppressive to many.[13]

{10} The first step in the process of data gathering can be either overt or covert. It is this stage that receives the most attention in connection with policymaking, in part, because it is the stage of which users are most aware. In addition, data gathering may be the stage of the process most amenable to regulation, since it may be the only stage of the process in which the data subject is directly involved and can therefore assert (or meaningfully waive) his rights. Internet users voluntarily disclose a great deal of information about themselves through registration pages, user surveys, online contests, application forms, and transaction documents.[14] Information disclosures may be required as a condition of participating in an online chat room or bulletin board.[15]

{11} In its 1998 survey of online privacy practices, the Federal Trade Commission ("FTC") found that ninety-two percent (92%) of the 1,402 websites surveyed collected some personal data. The most popular items of data were name, e-mail address, postal address and phone number.[16] The FTC found that websites soliciting personal information usually did not contain any posted privacy policy. Only fourteen percent (14%) of websites had any sort of privacy disclosure, and only a single site was found to meet all the criteria of notice, access, security and third-party disclosure identified by the FTC as critical.[17]

{12} Nervousness about solicitation of personal information online may be enhanced by the fact that, unlike brick and mortar businesses that present a "face" to the real world and may have an incentive to maintain a favorable reputation in the community, webpages appear as purely electronic fronts. The user has only a limited ability to peer behind the front to determine who, if anyone, stands behind the behavior of the page sponsor. Indeed, users may not even know the identity of the entity to which they are giving their personal information.[18]

{13} On the other hand, the interactive nature of Internet communications may foster a greater level of trust in some users, particularly children or the unsophisticated. As the FTC staff noted after a workshop on childrens' privacy:

> [T]he unique qualities of the Internet make it a particularly intrusive medium for children. The medium capitalizes on 'one to one marketing' and permits the site to develop a personal relationship with the user. For example, with more detailed collection of data on a child, future e-mail solicitations may come from an animated character appearing on the child's screen, addressing him by name and urging him to purchase a specific product -- perhaps a product over which the child lingered the last time he visited the site. The safeguards of traditional broadcast media, which bar 'host selling' and require separation between program, editorial and advertising, do not currently exist online.[19]

{14}Websites can also extract information that users do not voluntarily provide, such as the user's e-mail address, the type of browser, the type of computer being used, and the Internet address (URL) from which the user linked to the current site.[20] Websites can identify repeat users through the use of "cookies", which are small programs inserted onto the user's hard drive by the webpage which are accessed when the user revisits the page at a later date.[21] Websites can track the "clickstream" of the user, recording the portions of the page visited, and individual clicks made within each page.[22] This data can be recorded, stored, aggregated, and analyzed as evidence of consumer preferences by the webpage sponsor.[23]

{15} Recently, attention has focused on hardware and software systems that can assign a unique identification number to each personal computer, and the risk posed by such systems that webpages will be able to identify and track individual users. Controversy erupted in February 1999 over the disclosure that Intel's Pentium III chip contained unique numerical identifiers.[24] Similar controversy arose over the discovery that Microsoft software contains a "Registration Wizard," which assigns a unique identifier to each PC on which Microsoft software is loaded.[25]

{16} The most frequent use of data obtained from non-governmental websites online is marketing.[26] Website sponsors use data about their own visitors to learn which aspects of their page, or the goods and services offered on it, users are drawn to most. Such data may be useful even if collected only in aggregate form. In addition, data tied to the identity of individual users allow the page sponsor to program the page to display custom tailored product and service options, as well as advertising, when the user next visits the page. Individual preference data tied to individual name, address, phone or email address information may be sold to direct marketers or others for use in marketing goods and services bearing no relation to the subject matter of the page or transaction through which the information was originally obtained.

III. The Current State of Privacy Regulation

{17} The response to the above-described threats to privacy has been varied. As usual, where some see risk others see opportunity. However, most commentators appear to agree that existing law provides little protection for personal data online.

A. The tort of invasion of privacy

{18} The common law tort of invasion of privacy does not provide significant protection in the off-line world,[27] let alone the new online environment. The reasons for this are many, having to do with the intellectual history of the tort and its antagonistic posture versus the First Amendment and press defendants.[28]

1. Inadequate scope of the common law torts of invasion of privacy

{19} The tort of invasion of privacy had its origins in the seminal article by Warren and Brandeis in 1890, entitled *The Right to Privacy*, in which the authors argued for recognition of the tort we would today call "public disclosure of private facts."[29] Through subsequent common law development and legislation, the tort of invasion of privacy became widely established. In 1960, Dean Prosser surveyed seventy years of experience with the tort and declared that, rather than a single tort, there were really four separate and quite distinct torts masquerading as a single right to privacy: (1) the tort of appropriation of one's name or likeness for the commercial benefit of another, as where a person's picture is used in an advertisement without permission; (2) public disclosure of private facts, the tort first championed by Warren and Brandeis and

directed squarely at disclosure of personal facts in the tabloid press; (3) the tort of intrusion into seclusion, which has been described as a lesser form of trespass; and (4) "false light", which protects against the public use of one's name or image in a way that imputes to the subject views the subject does not hold or otherwise inaccurate circumstances.[30] Prosser's four part reductionist analysis of the tort proved persuasive and was codified in the Restatement (Second) of Torts, for which he was the reporter.[31] Innumerable law reviews have been written about the origin and nature of the four privacy torts. The important fact for the present discussion is that the four common law torts are generally considered to be irrelevant when it comes to online privacy issues, although a few commentators have argued for expansion of common law rights as a partial solution to online privacy threats.[32]

{20} False light can be rejected immediately as a solution to online primary concerns because it requires some element of falsity.[33] The predominant concern with respect to online privacy is that too much truth will be obtained and disseminated about us; a rule that only bars publication of false information is a non-starter. The tort of intrusion into solitude would appear to be inapplicable online because it requires, as the name implies, an "unreasonable and offensive intrusion into the seclusion of another."[34] Much of the personal data obtained online is provided voluntarily by users, and, in any event, no consensus has emerged that time spent on the Internet constitutes time in "seclusion," except perhaps in seclusion from family members and others in the real world who occupy the same residence as the online user.

{21} The tort of public disclosure of private facts would appear to fail for the same reason. To be actionable, there must be a disclosure of facts that are private.[35] Plaintiffs repeatedly lose such cases upon a showing that the fact in question was already in the public domain where, for example, it was obtained from a public record or other source outside the plaintiff's control, or obtained from plaintiff directly while in a public place.[36] Facts obtained from an online user may not be considered private when voluntarily provided by the user to a "stranger" webpage, or when gleaned from observation of online behavior while visiting the webpage. Moreover, public disclosure of private facts hinges on the embarrassment that accompanies publication of private facts to a wide audience.[37] Online privacy concerns regarding profiling are unrelated to the wide distribution of the personal information. The fact that a marketing firm obtains personal information, and uses or sells it to a limited number of third parties, generally does not involve the same kind of embarrassment because the data remains invisible to the data subject as well as the public at large.[38]

{22} The tort of appropriation also has little apparent application online.[39] What is appropriated from online users is their personal information, which has value in a marketing context. Online information is not used to sell products to others by associating the subject with the product in a testimonial manner or by use of the subject's face on the product packaging. Instead, the information is used to make decisions about how to market products or services to the subject himself. While information about the subject is certainly "appropriated" online, it is not the kind of information, or the kind of appropriation, that has traditionally been the subject of the appropriation tort.

{23} On a more general level, the common law privacy torts fail to protect online privacy because they do not protect actions taken in public,[40] and the Internet is arguably a public environment. The torts protect only private facts, whereas, a great deal of online privacy concern focuses on information that is "personal," without really being "private" -- name, address, phone number, e-mail address, and information regarding our conduct in the presence of, or in transactions with, strangers. Finally, the common law privacy torts are aimed at protecting against egregious conduct which causes a socially unacceptable level of shame or humiliation, a level of protection far more limited than what most consumers seem to want online.

B. Limitations on the current "sectoral" approach to privacy regulation in the United States

{24} Legislative protection of privacy in the United States is sometimes charitably referred to as "sectoral", meaning that legislation is directed in piecemeal fashion toward specific industries or issues, rather than

constituting a global privacy policy for the nation as a whole.[41] Apologists for the American system stress the flexibility of this form of regulation, its ability to tailor regulation closely to the needs of individual situations, and its tendency to avoid the sins of overregulation which might accompany a more comprehensive, "one-size-fits-all" regulatory scheme.[42] Less charitably, the current U.S. regulatory scheme could be referred to as a disorganized patchwork thrown up in response to individual, highly-publicized instances of abuse, but leaving certain important areas of privacy underprotected.[43]

{25} Regulation of personal data privacy can be found in a handful of separate federal statutes.[44] Specific statutes protect privacy interests in video rental records,[45] student loan information,[46] and drivers license information.[47] The Fair Credit Reporting Act[48] regulates the conduct of credit reporting agencies. Other statutes specifically limit the ability of the government to disclose personal information about individuals.[49] In addition, several federal statutes protect electronic communications from disclosure.[50]

{26} While no federal agency has general authority to regulate online privacy, unfair and deceptive practices with respect to privacy -- such as posting a privacy policy and then violating it -- may give rise to FTC enforcement action.[51]

IV. Critiques of Privacy Policy

{27} Commentators, legislators and regulators viewing the online privacy landscape and asking the question, "where do we go from here?" arrive at dramatically different answers. The conflicting points of view can be categorized and contrasted in various ways. For this article, I have divided them into three "camps" which I have labeled the "dossier society pessimists", the "market opportunists", and the "privacy peacemakers".[52]

A. The dossier society pessimists

1. What is the dossier society?

{28} The phrase "dossier society" conjures up the image of a society in which every detail of life is recorded and preserved in a central filing system accessible to those with power over their fellow citizens. Concerns about the dossier society certainly pre-date the advent of the computer, especially with respect to surveillance by totalitarian and repressive governments.[53] In 1971, Arthur Miller found that establishment of a dossier society was well under way in America, stating that, "the dossier society's genesis dates back several decades to the federal government's entry into the taxation and social welfare spheres."[54] Miller cited as examples, the federal census and the government's involvement in defense, housing, welfare, and jobs programs, all of which gather and use tremendous amounts of data about individuals in the course of administering various programs. But, with the increasing use of the credit card and the mainframe computer in the 1960's, the critical commentary came to focus increasingly on the abuses that were possible in the private sphere.[55] Numerous popular and academic accounts predicted a dramatic impact on individuals and society from the combination of increased information gathering, data storage capacity, computation abilities, and communicative capabilities of digital computers.[56]

{29} The concerns of dossier society critics are summed up by Professor Vern Countryman in his 1971 article:

> The computer has further facilitated the quest for efficiency. With its endless capacity to store data and to regurgitate it with lightning-like speed, it is inefficient not to use the computer to combine the various dossiers compiled on each

> individual. If the present trend continues, the day will come when the push of a button will produce a complete 'data profile' on each citizen, from his departure from the womb (or perhaps sometime earlier) to some time after he enters his tomb.[57]

2. Concerns about Accuracy, Discrimination and Human Dignity

{30} More specifically, "dossier society" concerns can be discussed under three separate headings: accuracy, discrimination, and human dignity. Unfairness results when decisions are made based on inaccurate data. Inaccuracies can arise in personal information databases when data becomes outdated or stale, or when data is improperly entered in the first instance. In addition, errors or distortions in reading and interpreting data are likely when data is collected (accurately) for one purpose, but is then transferred to another entity for use in answering questions not directly related to the reasons the data was collected in the first instance.

{31} Statistically-generated profiles may mask old-fashioned race prejudice or other illicit biases which are explicitly ruled out of order on grounds of public policy.[58] On a more subtle level, a form of bias may be inherent in the way computers think. The use of computer matching to answer questions about an individual frequently involves an exercise in sorting, matching, and averaging that individual's traits compared with others -- what we in human terms, would call stereotyping. There is something offensive to our notion of individualism when we are judged solely based on the average characteristics of the various classes to which we may be assigned membership, even if there is nothing "suspect" about the classes themselves.[59]

{32} This concern with discrimination is also related to a general concern with the impact that constant monitoring and judging of human behavior have on "human dignity."[60] Critics view the recording of daily events, purchases, communications, and inquiries as a form of surveillance. Data gathering and maintenance through the Internet arguably more resembles surveillance than casual observation in public. Unlike a casual glance in a public space, the "view" of an online observer with respect to online behavior is crisp and clear, since one-hundred percent of online behavior can be captured, and it is unforgettable, since data recorded digitally can be preserved in perpetuity at minimal cost.[61]

{33} One effect of surveillance is to promote law-abiding behavior, and surveillance (more innocuously termed "monitoring") is useful for both education and training, as well as punishment.[62] However, the fear is that constant surveillance inevitably induces caution and self-censorship. Surveillance discourages not only illegal or immoral behavior, but originality, spontaneity, and risk taking in general.[63] Advocates of strong privacy protection maintain that room to experiment and to make mistakes is essential to human growth and a feeling of freedom. There is also a perception that being observed without consent is a form of violation, as reflected in laws regarding wiretapping, eavesdropping, and "peeping Toms."[64]

{34} From a political perspective, the concern is that online digital surveillance will tend to limit dissent and the expression of unpopular opinion.[65] This insight is reflected in cases upholding the right to participate in political activities on an anonymous basis.[66] Even without the assumption that Internet surveillance will be used directly to expose dissenters to public opprobrium, constant monitoring may be harmful to the social fabric in more subtle ways. Preservation of free, unmonitored individual space may be essential to maintenance of a society based on the value of individualism. As a result, the loss of privacy may be harmful not only to the sensitive individuals who feel aggrieved by its loss. It may also constitute a harm to society itself,[67] even if individual members of that society do not mind the loss, and willingly give up their privacy or trade it away for financial or other consideration. The logical consequence of this viewpoint is that society itself has an interest in preventing individuals from exposing themselves to too much loss of privacy.

3. Policy initiatives related to acceptance of the dossier society critique

{35} As a working hypothesis, we can consider public policy pronouncements to embody elements that the

dossier society critique if they include certain identifiable features. One such feature would be outright limits on alienability of data, designed to protect individuals and society as a whole from the debilitating effects of the dossier society, despite the pressure posed by technology, commercial markets in information, or just plain citizen apathy.

{36} A second feature would be limitations on the use of personal information databases and data-matching programs to make decisions about individual rights or opportunities.[68] Such measures would reflect the concern with discrimination inherent in such programming.

{37} Third, proposals motivated by dossier society concerns might be expected to place limits on the sheer quantity of data collected or stored. Such limits would include requirements that data be destroyed after a certain period of time, or prohibitions on collecting certain types of data even at all.[69]

{38} Finally, such prophylactic measures would not limit themselves to regulation at the point of data collection, but would extend to data obtained from public records and to other third party sources.

B. The Privacy Market Opportunists

{39} By the label "privacy market opportunist", I mean to describe those who promote the development of markets in personal data.[70] Privacy market opportunists begin with the assumption that, even though privacy may be a "fundamental human right," that does not mean that individuals should not have the ability to decide for themselves how much that right is worth to them personally, and whether to sell, trade or give away their private information in their own self-interest.[71]

{40} As a result, the market opportunist analysis does not focus on the importance of privacy or the role it plays in the lives of individuals or society. Instead, it focuses on describing the theoretical benefits and limitations of free and active markets in private information, identifying obstacles to creation of such markets, and proposing policy measures designed to foster development of such markets.[72] The goal is to let consumers share in the value of their own personal information.[73]

1. Benefits of a market in personal information

{41} Market opportunists observe that the current state of the law results in personal data being too cheaply valued and therefore, overutilized.[74] However, there is also the general recognition that, absent some change in the existing law or technology, efficient markets in personal data are unlikely to emerge any time soon.[75] In short, the current "crisis" in privacy, which results in so much commentary and attention in legal and regulatory circles, is not merely a result of technological changes that make increased surveillance possible; it is also the result of market failures due to poor social choice in the allocation of property rights in information.[76]

{42} Under the existing United States privacy regime, personal data is the property of the person or entity who captures and organizes it.[77] Those favoring the development of markets in personal data reject the assumption that data appropriators necessarily own such data merely because they collected it through their webpage and compiled it into a useful format.[78] Instead, the determination of how to allocation property rights in data must be made based upon an evaluation of the relative amount of information and power in the hands of the parties to the transaction, and the social goals (efficiency usually predominant among them) to be achieved by allowing such trades.[79]

{43} Some commentators have speculated as to what markets in personal data might look like. One vision is of individual consumers entering into transactions online with individual websites, in which requests for information, either overt or surreptitious, prompt the consumer to demand a *quid pro quo* in the form of either money, or more likely, a credit for additional online goods and services which would otherwise not be free.

Others see consumers using intermediaries as information brokers to bundle up the information provided by a "tranch" of 1,000 or more similarly-situated individuals, and to market that information to commercial buyers. Royalties on such sales would be returned to the data subjects in some form, minus a profit for the broker.[80]

{44} It is apparent that in some ways, the Internet is the ideal environment for envisioning the development of markets in personal information. Contract terms can be offered, and consent registered and documented very efficiently online. The personal data itself can be transferred from the subject to the commercial entity online (again, whether overtly or covertly), and the consideration for the trade can flow back to the data subject online as well, in the form of credits for online services.

{45} There is some indication that this world is already upon us. Companies called infomediaries are already springing up to market individual data, and others are offering goods and services online in exchange for personal information.[81] Consumers are already willing to pay for privacy in other areas of their lives, and may be more than willing to enter into privacy transactions online.[82]

2. Obstacles to the creation of markets in personal information

{46} Enthusiasm for markets in individual information is tempered by the practical difficulties accompanying any attempt to set up such markets. First, a great deal of information about individuals is already in the public domain, including information from public and semi-public sources. That information will compete with any information an individual attempts to sell about himself.[83] Second, once an individual sells his information, control of that information is lost. Even if the terms of the contract of sale or license prohibit retransmission to third parties or reuse for purposes not agreed upon, such terms would be very difficult to enforce. Punishment of cheaters and leakers will be difficult and rare. As a result, some admit that exactly how a market in privacy would actually work in practice is only dimly understood at this point.[84]

{47} Moreover, asymmetries in information and bargaining power may result in built-in advantages for commercial information appropriators, as compared with individual data subjects. The buyer will usually know more about the anticipated use of the information than the seller. A consumer may face relatively high costs in the form of money, time and inconvenience by turning down an online transaction merely because it would entail certain information disclosures; whereas, to the merchant, one individual's potential transaction may be far too insignificant to make it worth bargaining over privacy rights on an individual basis.[85] On the other hand, the attempt to establish a market in personal information, combined with recognized property rights in such data, may require creation a legal and enforcement system with an unacceptably high level of expense and complexity.[86]

{48} In light of the above concerns, one may wonder whether any markets in individual information are likely to develop. This author tends to think such markets will develop simply because the consumer is always in possession of at least one key piece of information that is unavailable from public sources, and as such, because it changes daily, is always fresh and valuable for sale. That information consists of the consumer's own subjective interest in being marketed a given product, service, or subject matter. An individual who wakes up one morning with the desire to buy a new car or a set of golf clubs has something valuable to sell in the form of his own subjective state of mind. This information has a short shelf life and may not be available to marketers through any source other than the consumer himself.

3. Policy initiatives of the market opportunists

{49} The first principle for any market opportunist, of course, must be that the law should allow transactions in personal information to occur. They would oppose inalienability rules preventing individuals from determining whether to sell information about themselves or how much to charge for that information.[87]

{50} In general, proponents of markets in personal data would encourage government action intended to equalize information among participants in data transactions by requiring websites to post privacy policies, disclose the use being made of information gathered online, and otherwise ensure that consumer consent is meaningful when obtained.[88] Proponents of markets in personal information suggest modifying the "default rule" as one way to equalize information.[89] The present default rule is that, absent explicit agreement to the contrary, the webpage sponsor is presumed to be the owner of any information obtained on the page. A contrary default rule could be imposed as a matter of law; however, under which the use of personal information for purposes beyond the transaction in which it was provided would be barred, absent affirmative consent. A modified form of the present rule would be an "opt out" rule, under which consumers would have the right to remove their name from mailing lists or otherwise retrieve their personal information by taking affirmative steps. The contrary rule would be an "opt in" rule.

{51} An "opt in" rule can be seen as transaction forcing and market promoting. By requiring the webpage sponsor to bring the issue to the data subject's attention in an explicit manner and to seek affirmative consent, it is much more likely that consent will not be granted absent a transaction involving consideration flowing to the data subject. Under the present system data subjects give their data away not realizing they are even parting with something of potential value.

{52} Not everyone who examines the issue concludes that an "opt in" rule is warranted. Such a rule may be inefficient if it discourages too many individuals from participating, and, as a result, the total data pool becomes less valuable for everyone.[90] In general, however, we would consider transaction forcing "opt in" rules to be the hallmarks of the privacy market opportunist.

{53} Consistent with the above proposals, privacy market opportunists might also support initiatives to clarify a data subject's property rights in personal data obtained from all sources, including third parties, not just from the subject himself.[91] Establishment of such rights would be onerous to data appropriators, and would pose a much higher burden on the commercial use of personal data because it would require the appropriator to affirmatively contact data subjects with which he has no other relationship in order to obtain permission for the use of their data.[92]

{54} Finally, one of the principal difficulties in maintaining a fair market in privacy is the difficulty private citizens would face in policing adherence to stated privacy policies, or the terms of any transaction allowing only limited use of specific personal data.[93] Privacy market opportunists should be expected to support measures to bring government enforcement to bear on Internet sites that abuse information by using it beyond the scope of any license agreed to in the transaction.

C. The Privacy Peacemakers

1. Concern over promoting online commerce

{55} The third orientation discussed here is referred to as the "privacy peacemaker". This perspective focuses not on protecting society from the debilitating effects of loss of privacy, nor promoting a transfer of ownership rights in personal data from appropriators to data subjects, forcing markets in such information to develop. Instead, the main concern of the "privacy peacemakers" is to ensure that privacy fears -- well founded or otherwise -- do not impede the continued growth on online commerce.

{56} The idea that privacy concerns must be dealt with in order for the Internet to achieve its full potential is stated explicitly in the pronouncements of numerous government organizations proposing online privacy guidelines.[94] Such concerns are also cited by private sector commentators interested in promoting development of the Internet.[95] Such statements are frequently accompanied by citations to public opinion polling data, as cited in Section I, evidencing a high level of public concern about the issue.[96]

{57} A related argument expresses the fear that unless privacy is dealt with through industry self-regulation, the public will demand imposition of heavy-handed government regulation,which will hamper the development of the Internet.[97] The main point, however, is that "privacy peacemakers" measure any proposed privacy protection scheme as much by what it does not accomplish (impairing the growth of the Internet), as by what it does accomplish. In seeking an accommodation of privacy concerns while making the minimum imposition on business, "privacy peacemakers" frequently use the rhetoric of "balancing." The desire of online users for privacy must be balanced against the American tradition of free transfer of information, the First Amendment, and the legitimate needs of business.[98]

{58} Not surprisingly, the ranks of the "privacy peacemakers" are made up largely of representatives of the Internet industry and politicians, whose job is to balance the demands of competing constituencies. As a result, the "privacy peacemaker" camp is far more numerous and better funded than either the dossier society pessimists (who tend to be academics or public interest privacy advocates) or the market optimists (who are almost exclusively academics).

2. "Privacy peacemaker" thinking in public policy initiatives

{59} Policy initiatives reflecting the peacemaker orientation would be expected to focus on scandalous and controversial forms of privacy abuse that might impact public trust in the Internet or prompt legislative overreaction. Regulation would focus on sensitive financial or medical information, information related to gender, children, or personal safety. Identity theft and child stalking would be at the top of the list, regardless of their actual prevalence in the society. One would expect to see little or no protection of neutral biographical data (other than that useful for committing identity theft) or information related to consumer preferences and lifestyle, regardless of whether that information might have commercial value.[99]

{60} Second, one would expect "privacy peacemaker" regulation to focus on protection where it is most visible, and therefore reassuring. The most visible portion of the personal information spectrum is the nexus where information is gathered from or provided to the individual consumers. One would expect to see few or no restrictions imposed on the use of data outside public view.

{61} Finally, one might expect to see a higher level of protection being made available to the committed, vocal and technologically savvy minority of citizens who are well informed about online privacy issues and know how to protect their rights.[100] Provisions allowing consumers to "opt out" of certain uses of their personal information may respond to the goals of "privacy peacemakers", in that they provide a safety valve for the concerned minority who might protest if no such outlet were provided. One would not expect "privacy peacemaker" proposals to contain inalienability provisions or other limitations on the use of data for its own sake, nor would one expect to see proposals to vest individuals with anything like a property right in their personal information.

V. Who Leads at Halftime?: Current Privacy Initiatives in the United States

{62} The game of defining and regulating online privacy rights is far from over. At most, it is halftime, with the final score unknown. Still, trends have emerged which lead one to conclude that the "privacy peacemaker" camp clearly holds the halftime lead, dominating the debate in most arenas and having the largest influence on policy proposals. Dossier society pessimist and market opportunist concerns are marginalized, appearing only inferentially in policy proposals. This paper concludes by reviewing current policy proposals in two areas: (1) "fair information handling practices," which form the basis for online privacy proposals by the Clinton administration, and (2) the Federal Trade Commission's legislative proposal for regulating online privacy.

A. Fair information handling practices and the Clinton Administration

{63} Various entities have compiled lists of fair information handling practices for their own internal use, in an effort to influence public policy or to encourage voluntary adherence by others. In 1972, the Department of Health Education and Welfare ("HEW") established a federal advisory committee which reviewed the handling of information at the federal agency level and promulgated a series of "fair information practices," which have been cited and built upon by numerous other entities since that time.[101] In 1980, the Organization for Economic Cooperation and Development ("OECD") issued its own guidelines for handling personal data.[102] The Council of Europe adopted a Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data in 1985.[103] A 1995 report by the Privacy Policy Working Group of the United States Government's Information Infrastructure Task Force [104] also included fair information handling principles. In 1995, the European Commission issued its Privacy Directive, setting out the rights of data subjects and the responsibilities of data processors.[105] Each of these documents was built upon the concept of defining fair information handling practices.

{64} On July 1, 1997, the Clinton White House released the Framework for Global Electronic Commerce, [106] a general policy statement setting out the administration's philosophy regarding the relationship between government and the world of electronic commerce. The portion of that document addressing online privacy endorsed general privacy principles articulated in several prior policy statements, including the 1995 report by the IITF Task Force.[107]

{65} More recently, a 1998 paper by the Department of Commerce ("DOC") entitled, "Elements of Effective Self-Regulation for the Protection of Privacy and Questions Related to Online Privacy" listed nine privacy principles[108] regarded as typical fair information handling guidelines:

1. "Awareness": Disclosure of the identity of the data collecting party and means for avoiding participating in such transactions;

2. "Choice": A mechanism to exercise options, including "affirmative choice" for certain "sensitive" categories of information relating to, for example, medical conditions, or children;

3. "Data security": Protections against improper alteration or misappropriation of data;

4. "Data integrity": Keeping data which is accurate and relevant for the purposes for which it was collected;

5. "Consumer access": The ability of consumers to review and correct data about themselves, although the document warns that the extent of access may vary by industry, due to the costs involved; and

6. "Accountability": Companies should be accountable in some manner for compliance with their own policies.

In addition, the Principles include three "enforcement principles":

1. "Consumer recourse": A way to resolve disputes that is "readily available and affordable";

2. "Verification": A third-party check on compliance; and

3. "Consequences": Sanctions for failure to comply.

{66} Several areas of dispute exist with respect to the interpretation and adequacy of these types of fair information handling practices. With respect to "awareness" (sometimes also called "notice"), it may be questioned whether posting a privacy notice on a webpage really provides notice to more than a small handful of users who actually bother to access the posted policy and read it. The fact that only a small minority of users will access such policy statements indicates that the peacemaker function of such notices provides protection only for the vocal and informed few, but not the mass of Internet users.

{67} The principle of "choice" (or "consent") implicates the selection of default rules discussed above, and whether affirmative consent ("opt in") must be obtained before a website sponsor can use information gathered in one transaction for other purposes or transfer it to third parties.[109] Statements of fair information handling practices usually assume that "opt out" rules are generally adequate.[110] The highest level of protection offered generally consists of an affirmative "opt in" requirement for some kinds of sensitive information or classes of vulnerable persons.[111] The "opt out" nature of consent in most fair information handling guidelines gives them a decidedly peacemaker bent. They do little to force, or to even encourage, transactions in personal data.

{68} Controversy also exists regarding the extent to which consumers are entitled to see the information kept about them, and on what terms access will be provided.[112] This debate highlights the fact that fair handling practices guidelines do not recognize a property right in the data subject; the data is presumed to be owned by the data collector and, as a result, the data subject's right to access must be balanced against considerations of cost and convenience to the data appropriator.

{69} Some fair information practices guidelines stress that only "relevant" information should be gathered, and that once the purpose of the information has been fulfilled, it should be destroyed.[113] These sorts of limitations, unenforceable as they may be, reflect the concerns of the dossier society pessimists in limiting the existence of information dossiers in general, separate and apart from any particular showing of abuse or harm. However, such guidelines generally shrink from imposing concrete limitations that are capable of enforcement.[114]

{70} Finally, disputes exist over the concept of enforcement and accountability,[115] which revolve around the extent to which commercial entities (or their trade organizations) should be allowed to police themselves, or whether an external audit and disciplinary function is necessary. Proposals range from the relatively toothless[116] to the full panoply of administrative sanctions and private rights of action, including provisions for attorneys' fees and punitive damages.[117]

{71} In addition, fair information handling guidelines directed specifically at the online environment generally fall into the peacemaker camp in that they tend to address rights only for information collected from the subject online. Notice, access and other similar rights apply to information gathered directly from the individual, not to all information collected by the entity from third parties, nor do such guidelines contain inalienability rules.[118]

{72} The current negotiations between the United States and the European Union ("EU") over the 1995 Privacy Directive ("Directive") concern the issues cited above. The Directive is perceived to be substantially more protective of privacy than the current American regulatory scheme for various reasons. First, the Directive contemplates the establishment of national privacy regulators in each EU member state,[119] something unknown in the United States. Moreover, the Directive establishes and requires adoption of a nationwide privacy law in each member state, governing all processing of personal data, whether by computer or manually, and applying across the board to all industry segments and transactions.[120] The Directive is not limited to the regulation of handling information obtained at the data gathering stage, nor to

that obtained through a particular medium. The Directive applies to all processing of data, regardless of how that data came into the hands of the processor,[121] and it contains an expanded list of subjects deemed to be sensitive, as to which special restrictions on use and transfer apply.[122]

{73} Nevertheless, the Directive is built around a list of rights of data subjects,[123] and duties of data processors,[124] that track, in broad brush, the same fair information handling practices principles described above.[125] In that regard, while the Directive contemplates a greater government role in privacy regulation, it must still be considered fundamentally a "privacy peacemaker" regulation.

{74} The fundamental similarity between the goals of privacy regulation in the United States and the EU can be seen in the dramatic narrowing of the debate between the two sides in recent months. Because the Directive provides that data may not be exported from the EU to any country that does not provide roughly equivalent privacy protection,[126] the threat that data flows from the EU to the U.S. will be cut off has prompted extensive negotiations between Clinton administration officials and EU privacy negotiators.[127] The United States' position in those negotiations has been to urge that self-regulatory measures by industry trade associations can constitute adequate protection to qualify members of those associations to receive data flows from entities in the EU.[128] At last report, the U.S. negotiators maintained that the two sides were close to reaching an agreement.[129]

B. Legislation

{75} A review of Internet-related privacy legislation proposed by the FTC confirms the impression discussed above. The public policy debate is taking place largely within the privacy peacemaker model, and is not directed toward substantially curtailing the use of personal information dossiers in business, nor is it intended to encourage the development of markets in such information. Leaving aside statutes prohibiting interception of electronic communications, the principle statute aimed at online privacy at the federal level to date is the Children's Online Privacy Protection Act.[130] As of the date of this article, no general Internet privacy legislation has been passed.[131]

{76} In the summer of 1998, the Federal Trade Commission ("FTC") reported to Congress that the vast majority of websites collect personal data of some sort from site visitors, but that very few of them even post a privacy policy, considered the bare minimum of privacy protection to most.[132] FTC Chairman, Robert Pitofsky testified before Congress in July 1998, that the failure of the business community to implement a system of self-regulation for online privacy prompted the agency to recommend federal legislation for online privacy protection.[133] In that testimony, the FTC chairman outlined the Commission's vision of what Internet privacy regulation should look like.[134] That vision is, fundamentally, a peacemaker model.

{77} The FTC-proposed legislation setting forth four basic privacy principles, adopted from various existing fair information handling practices guidelines. Those principles would include (1) "Notice/awareness"; (2) "Choice/consent"; (3) "Access/participation" (the right to obtain access to and correct personal data); and (4) "Security/Integrity".[135] A regulatory agency (presumably, the FTC) would then be given the responsibility to issue more detailed regulations enforcing these basic principles. Self-regulation would still be encouraged, however, as a preferred solution. The agency would be authorized to approve industry self-regulatory schemes, and once approved, participation in such schemes would serve as a safe harbor from further federal regulation and enforcement.[136]

{78} Evaluation of such a scheme is difficult in the abstract because so much would depend on the specific regulations adopted by the agency. Noticeably absent from the FTC's proposed basic principles; however, is any language fundamentally limiting the current business practice of gathering extensive amounts of personal information or indicating that significant aspects of such use should be curtailed on grounds the dossier society pessimists would recognize. The statutory scheme outlined by the FTC would not appear to authorize

the agency to recognize property rights in personal information on behalf of data subjects, nor impose transaction forcing measures for the sake of spurring a market in such information.

VI. Conclusion

{79} Most discussions of online privacy policy focus on the tools of privacy protection -- the choice between government regulation, industry self-regulation, or laissez faire market discipline. At the same time, however, a number of diverse commentators are raising fundamental questions about what society ultimately hopes to accomplish in regulating online privacy. Some raise questions about whether cyberspace is the place to draw a line in the sand in the battle against the emerging dossier society. Others seek to take advantage of the unique features of the Internet to promote a market in personal information which, if successful, would constitute a significant transfer of wealth to the middle class, whose personal data is highly valued by business. The viewpoints of those authors have not featured prominently in the privacy proposals debated in Washington, D.C. Many new proposals for privacy regulation are bound to be introduced in the regulatory and legislative sphere over the upcoming year. The intent of this article has been to assist observers of the ongoing privacy debate in evaluating policy proposals more critically, in terms of what goals they promote, and what assumptions they embody, as well as what regulatory tools they seek to employ.

---

[*] Karl D. Belgum is an attorney with Thelen, Reid & Priest, LLP of San Francisco, California where he is a partner in the Business Litigation Group and is head of the firm's Internet practice initiative.

[**]**NOTE:** All endnote citations in this article follow the conventions appropriate to the edition of THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION that was in effect at the time of publication. When citing to this article, please use the format required by the Seventeenth Edition of THE BLUEBOOK, provided below for your convenience.

Karl D. Belgum, *Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy*, 6 RICH. J.L. & TECH. 1, (Symposium 1999), *at* .

[1]*See e.g.*, Information Policy Committee, National Information Infrastructure Task Force, *Options for Promoting Privacy on the National Information Infrastructure*, April 1997 (Draft for Public Comment), n.24 and accompanying text (*citing* 1996 Equifax/Harris Consumer Privacy Survey showing that sixty-five percent of respondents thought privacy was "very important") *available at* (visited May 23, 1999) <http://www.iitf.nist.gov/ipc/privacy.htm/> [hereinafter *Promoting Privacy*]; Federal Trade Commission, *Individual Reference Services: A Report to Congress*, December 1997, accompanying text to n.133 (finding that "[s]urvey research over the past twenty years demonstrates that increasing numbers of Americans are concerned about how personal information is being used in the Computer Age.") *available at* (visited May 15, 1999) <http://www.ftg.gov/bcp/privacy/wkshp97/irsdoc1.htm/> [hereinafter *Individual Reference Services*]; *Hearings on Consumer Privacy on the World Wide Web Before the Subcomm. on Telecommunications, Trade and Consumer Protection of the House Comm. on Commerce*, July 21, 1998 (prepared statement of Robert Pitofsky, Chairman, FTC), n.16 and accompanying text (citing to March 1998 *Business Week* survey) *available at* (visited May 23, 1999) <http://www.ftc.gov/os/1998/9807/privac98.htm/> [hereinafter *Consumer Privacy on the World Wide Web*]; Eric Sinron & Barak D. Jolish, *Privacy Lost in the Brave New Web?*, 2 J. INTERNET L. 1, (Sept. 1998).

[2] Keith H. Hammonds, ed., *Online Insecurity*, BUS. WK., Mar. 16, 1998, at 102.

[3]*Id*.

[4]*Id*.

[5]*See, e.g.*, Federal Trade Commission, *Privacy Online: A Report to Congress*, June 1998, at II. B. 2b. ("If such [privacy] protections are not implemented, the online marketplace will fail to reach its full potential.") *available in* 1998 WL 299974 FTC, at *91, and <http://www.ftg.gov/reports/privacy3/toc.htm> [hereinafter *Privacy Online*].

[6] Keith Sharfman, *Regulating Cyberactivity Disclosures: A Contractarian Approach*, U. CHI. LEGAL F. 639, 642 & nn.17 & 30 (1996) [hereinafter *Sharfman*], (claiming that most persons do not care about disclosure of online activity based, for example, on limited use of anonymous remailers).

[7] Another author cites telephone subscribers' willingness to pay for an unlisted number as evidence that privacy is important to people, and that they are willing to pay for it. Eli M. Noam, *Privacy and Self Regulation: Markets for Electronic Privacy*, *in* Privacy and Self- Regulation in the Information Age (1997) [hereinafter *Noam*] 21, 23 (unlisted number service purchased by thirty-four percent of residences in Manhattan, twenty-four percent of residences in New York State, and fifty-five percent of all residences in California).

[8] Privacy "focus groups" sponsored by the Direct Marketing Association ("DMA") find that consumers are more concerned about personal safety issues than the intrusion of marketing; that they are suspicious of government regulation and open to self-regulatory initiatives from the private sector; and that in general privacy is not one of the issues of highest concern to consumers or voters. *See* Stanley B. Greenberg, *Privacy Concerns and the Internet: A Focus Group Study on Public Attitudes* (Report prepared for the Federal Trade Commission by Greenberg Research, dated May 30, 1997, sponsored by the DMA) *available at* (visited May 31, 1999) <http://www.richmond.edu/jolt/v6i1/<http://www.ftc.gov/bcp/privacy/wkshp97/comments3/greenbrg.htm>. According to the DMA focus group data, privacy lags behind such other concerns as "crime, jobs or family breakdown." The main concerns about privacy online were reported to be access to pornography, improper advances being made to children, and personal information collected from children (but only from a safety, not a marketing, perspective).

[9]*See Privacy Online, supra* note 5.

[10] FTC Staff Report, *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, December 1996, Section I, *available at* (visited May 15, 1999) <http://www.ftc.gov/reports/privacy/privacy2.htm> [hereinafter *FTC 1996 Workshop*]. *See also*, Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, June 6, 1995, Introduction (discussing the threat to privacy caused by the "social trend" toward more exchange of information when engaging in transactions, including credit card transactions, combined with a "technological trend" toward increasingly powerful hardware and software) *available at* (visited June 23, 1999) <http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html> [hereinafter *Privacy and the NII*].

[11]

> [B]efore the NII, in order to build a profile of an individual who had lived in various states, one would have to travel from state to state and search public records for information about the individual. This process would have required filling out forms, paying fees, and waiting in line

for record searches at local, state, and federal agencies, such as the departments of motor vehicles, deed record offices, electoral commissions, and county record offices. Although one could manually compile a personal profile in this manner, it would be a time-consuming and costly exercise, one that would not be undertaken unless the offsetting rewards were considerable. In sharp contrast, today, as more and more personal information appears online, such a profile can be built in a matter of minutes, at minimal cost.

Privacy and the NII, *supra* note10, at 1-2.

[12] The term profiling is used, for example, in Roger Clark, *Profiling: A Hidden Challenge to the Regulation of Data Surveillance*, 4 J. L. & INFO. SCI. 2 (1993), and in Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* (1996) 312-15 (discussing profiling by marketers: "Direct marketers typically offer profiles selected according to income, ethnicity, sex, age and marital status."). *See also* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1239 (1998), for further references on profiling and data mining. Examples of data matching at the federal level are described in Madsen, *Handbook of Personal Data Protection* 116-25 (Stockton Press 1992) (discussing data matching using computers in various government departments, including the Department of State, the Immigration and Naturalization Service, Customs Service, Treasury Department, Defense Department, FBI, Public Health Service, Bureau of Alcohol, Tobacco and Firearms, and others).

[13]*See* Kang, *supra* note 12, at 1260-61.

[14]*See Consumer Privacy on the World Wide Web*, *supra* note 1, at 2.

[15]*See FTC 1996 Workshop*, *supra* note 10, at 1.

[16] The results of the FTC's web site survey are included in *Privacy Online: A Report to Congress*, *supra* note 5, issued by the FTC in June 1998.

[17]*See id*. at 27. A May 1999 survey of Internet privacy practices conducted by the McDonough School of Business at Georgetown University reported slightly more encouraging results. *See* Mary J. Culnan, *Privacy Online in 1999: A Report to the Federal Trade Commission* (the Georgetown Internet Privacy Policy Study), May 17, 1999 draft, *available at* <"http://www.msb.edu.faculty/culnanm/gippshome.html> [hereinafter *Georgetown Survey*]. That survey of 364 of the most visited web sites revealed that 92.9% collected some form of personal information and eighty-four percent collected at least some "demographic" data as well. While the vast majority of sites contained some privacy information, very loosely defined, fewer than half had a "Privacy Policy Notice" as that term was used by the survey authors, describing the site's overall privacy policy, and only 9.5% of all sites surveyed contained a privacy disclosure that dealt with all five elements of a thorough privacy policy disclosure targeted by the surveyors. *Id* at Executive Summary and 8-9.

[18] The FTC Staff noted that [n]otice of the identity of the information collector is not always simple. While most sites surveyed by staff identify their sponsor, others are operated by a Web developer or other agency, and, as a result, the identity of the entity for whom the site ultimately collects data may not be revealed. *FTC 1996 Workshop*, *supra* note 10, at 4.

[19]*Id*. at 2.

[20]*See id*. at 1.

[21]

> [W]eb sites can use "cookies" to tag users so they can be recognized upon their return. Cookie technology allows a web site's server to place information about a consumer's visits to the site on the consumer's computer in a text file that only the web site's server can read. Using cookies a web site assigns each consumer a unique identifier (not the actual identity of the consumer), so that the consumer may be recognized on subsequent visits to the site. On each return visit the site can call up user-specific information which could include the consumer's preferences or interests, as indicated by the documents the consumer accessed in prior visits or items the consumer clicked on while in the site. Web sites can also collect information about consumers through hidden electronic navigational software that captures information about site visits, including Web pages visited and information downloaded, the types of browser used, and the referring Web sites' Internet address.

Privacy Online, *supra* note 8, at II. B n.7.

[22]*See id*.

[23]*See id*. at 1. Participants in the 1996 FTC workshop disagreed as to whether it was feasible for a web page sponsor to capture clickstream data for individual users, combine it with identifying information such as email address or URL, and create meaningful profiles of individual users. *See FTC 1996 Workshop*, *supra* note 10, at 1, & n.7. "Some panelists argued that it is indeed possible to use the clickstream data to create a profile of individuals' preferences and usage patterns. Others asserted that tracking site activity for individuals generates large, complex data files that cannot be used for profiling with current technology." *Id*. at n.7 (citations omitted). A more recent article by an attorney at America Online appears to assume that capture of such information is feasible.

> [E]ach time a user clicks her mouse while on a web site, the potential exists for the company to record the location of her "click" and thus to collect information about her online behavior -- where she goes, what she buys, when she buys, and how frequently she buys. Merchants want this granular information because of its consumer market research value.

Elizabeth deGrazia Blumenfeld, *Privacy Please: Will the Internet Industry Act to Protect Consumer Privacy Before the Government Steps In?*, 54 BUS. LAW. 349, 351 (1998) [hereinafter *Blumenfeld*].

[24]*See* John Markoff, *IBM Says New Feature Increases Pentium's Security*, N.Y. Times, Feb. 25, 1998, at C5; Stephanie Miles, *Groups Press on Pentium III*, CNET News.com, Mar. 8, 1999, (visited May 29, 1999) <http://www.news.com/News/Item/0,4,33481,00.htm>.

[25]*See* Erich Luening & Mike Ricciuti, *New Security Hole Found in Windows 98*, CNET News.com, March 10, 1999, (visited May 28, 1999) <http://www.news.com/News/Item/0,4,33625,00.htm>; Stephanie Miles, *Groups Press on Pentium III*, *supra* note 24.

[26]*See* Schwartz & Reidenberg, supra note 12, at 307-11.

[27] Many law review authors have observed that the tort of invasion of privacy is not the basis for many successful actions and frequently must give way in the face of a First Amendment challenge. *See* Andrew J. McClurg, *Bringing Privacy Out of the Closet: A Tort Theory of Liability for Intrusion in Public Places*, 73 N.C. LAW REV. 989 (1995) (proposing to revive the tort of invasion of privacy in public places through application of a multipart test); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis' Privacy Tort*, 68 CORNELL L. REV. 291 (1983).

[28]*See* Ruth Gavison, *Too Early for a Requiem: Warren and Brandeis Were Right on Privacy v. Free Speech*,

43 S.C. L. REV. 437, 446 (Spring 1992) (arguing that the courts have been overly solicitous of First Amendment concerns at the expense of privacy rights); George Trubow, *Protecting Informational Privacy in the Information Society*, 10 N. ILL. U. L. REV. 521, 534 (1990) (discussing First Amendment limitations on the common law tort of invasion of privacy).

[29]*See* Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 5 HARV. L. REV. 193 (1890).

[30]*See* Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960). The same basic analysis is presented in PROSSER & KEETON, HANDBOOK ON THE LAW OF TORTS, Ch. 20 (5th ed.) (1984).

[31]*See* RESTATEMENT (SECOND) OF TORTS (1965); McClurg, *supra* note 27, at 998 n.40 (discussing Prosser's role as Reporter for the RESTATEMENT (SECOND) OF TORTS and incorporation of his views on the privacy tort into the RESTATEMENT).

[32]*See, e.g.*, Kenneth C. Laudon, *Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information*, *in* Privacy and Self Regulation in the Information Age 41 (1997) [hereinafter *Laudon*].

[33]*See* PROSSER & KEETON, *supra* note 30, at 863 et seq.

[34]*Id*. at 854.

[35]*See id*. at 856.

[36]*See id*. at 858-59. In addition, this aspect of the tort of privacy has been crippled by First Amendment precedents holding that no tort liability may attach to the press for giving further publicity to facts obtained from public sources. *See e.g.*, Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1974) (holding that states may not impose sanctions for the publication of truthful information which is contained in official records or open to public inspection.); Florida Star v. B.J.F., 491 U.S. 524, (1989) (holding that the First Amendment precludes liability for the illegal publication of a rape victim's name obtained by newspapers from a public source).

[37]*See* McClurg, *supra* note 27, at 991-1010 (discussing reluctance of courts to provide remedy where privacy invasion occurs in public); Prosser & Keeton, *supra* note 30; *but c.f. id*. at 857-58 ("There is considerable doubt about the necessity for a public disclosure....[I]t has been held to be an invasion of the plaintiff's right of privacy to communicate a private fact to a newspaper, military agency, neighbor, or disinterested employer").

[38] Scenarios can be imagined in which public disclosures widely disseminated on the Internet, for example in a chatroom, could support such a claim. In such a case the theory would treat the web as a publication medium rather than a medium for obtaining and collating private information.

[39] "[T]he effect of the appropriation decisions is to recognize or create an exclusive right in the individual plaintiff to a species of trade name, his own, and a kind of trade mark in his likeness." PROSSER & KEETON, *supra* note 30, at 854.

[40]*See generally*, McClurg, *supra* note 27 (advocating recognition of privacy rights in public spaces).

[41]*See* Schwartz & Reidenberg, *supra* note 12, at 7 ("In order to minimize state intrusions on information flows, the United States approaches fair information practices through attention to discrete sectoral and subsectoral processing activity."); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights*, 44 FED. COMM. L. J. 195, 208 (1992) ("The American legal system does not contain a comprehensive set of privacy rights or principles that collectively address the acquisition, storage,

transmission, use and disclosure of personal information within the business community. ... [L]egal protection is accorded exclusively through privacy rights created on an ad hoc basis."). A list of the subject matters covered by privacy legislation at the state level, on a "sectoral" basis, would include records regarding abortion, adoption, AIDS tests, applications for public housing, arrest, autopsy, bank information, children receiving social service help, child abuse, drug abuse, education, grand juries, library circulation, medical, mental health, income tax, rape victims, rent control, social security numbers, unemployment insurance compensation forms, video and audio tape rental records. *See* Madsen, *supra* note 12, at 145-46.

[42]*See* Promoting Privacy, *supra* note 1, at 24. Supporters of the current regulatory system argue that a "one size fits all" approach may "constrain innovation and reduce competition at the expense of the consumer"; that privacy is only one of a number of social issues about which persons care; that sectoral regulation may promote competition among agencies to be perceived as most effective in regulating privacy in their respective spheres; and that "reactive" regulation, which waits for and reacts to problems that emerge in a concrete context, avoids unnecessary overbreadth that can accompany "anticipatory" regulation. *Id*. at 24.

[43]*See* Schwartz & Reidenberg, *supra* note 12, at 10. Regulations are often the result of a particular perceived crisis or "horror story." The federal Video Privacy Protection Act, known as the "Bork Bill," is an excellent example of this ad hoc protection. The law regulates the treatment of personal information collected in connection with video sales and rentals. It exists because of the public uproar that ensued immediately following the publication by a Washington magazine of the video titles that Robert Bork, then a federal appellate judge and a nominee for the United States Supreme Court, had rented.

[44] "The standards in place for fair information practices depend entirely on the context. In one context, such as direct marketing, personal information may have only limited protection against unfair use. In another context, such as employee recordkeeping, the same personal information may be subject to stringent legal and business controls." Schwartz & Reidenberg, *supra* note 12, at 12 (presenting a thorough discussion of privacy legislation not limited to the online context). *See* Madsen, *supra* note 12, Chapter 4 (describing the evolution of federal privacy legislation). For a helpful chart of federal privacy statutes, *see* Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L. J. 1 (1996).

[45]*See* Video Privacy Protection Act of 1988, 18 U.S.C. Sections 2710-11 (1999) (preventing videotape rental companies from disclosing personal information regarding tape rentals).

[46]*See* Family Educational Rights and Privacy Act of 1974, 20 U.S.C. Section 1232g (1999) (limiting disclosure of student loan records to third parties without consent of the data subject).

[47]*See* Driver's Privacy Protection Act of 1994, 18 U.S.C. Sections 2721-2725 (1999) (prohibiting state governments from disclosing (i.e., selling) personal identifying information held in drivers license bureaus, such as the driver's photograph, social security number, drivers license number, address, phone number, and medical or disability information). The Act has been challenged on Tenth Amendment grounds in numerous recent federal court cases. *See, e.g.*, Condon v. Reno, 155 F.3d 453 (4th Cir. 1998), *cert. granted*, 119 S. Ct. 1753 (1999) (striking down the Act as a violation of the Tenth Amendment); Travis v. Reno, 163 F.3d 1000 (7th Cir. 1998) (upholding the Act); Oklahoma v. United States, 161 F.3d 1266 (10th Circuit 1998) (upholding the Act).

[48]*See* Fair Credit Reporting Act, 15 U.S.C. Sections1681-1681t (1999). The Act limits disclosure of consumer records and provides certain rights to inspect and correct, or at least supplement, erroneous credit agency records.

[49]*See* The Privacy Act of 1974, 5 U.S.C. Section 552 (1999) (The Privacy Act was amended in 1994 to

limit the ability of federal agencies to make decisions about individual entitlements based solely on computer matches.). Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. Section 552a (1999) (The amendment also imposed an obligation on agencies taking negative action based on a computer database match to notify the affected individual and afford an opportunity to challenge the determination).

[50]*See, e.g.*, Electronic Communications Privacy Act of 1986, 18 U.S.C. Section 2701 (1999) (explaining that this Act requires that a government entity seeking information including subscriber information from an Internet service provider obtain a subpoena and warrant or court order to obtain such information. It also prohibits any "person or entity providing an electronic communication service to the public" from disclosing the contents of electronic communications such as e-mails).

[51]*See* In re GeoCities, 63 Fed. Reg. 44,624 (FTC 1988) (stating that the order recites that GeoCities failed to abide by its published policy of not sharing personal data with third parties).

[52] My division of the privacy commentary into three schools of thought differs from the more common way of categorizing the current privacy debate on a continuum where one pole is "market discipline" (i.e., laissez faire), the other pole is "government regulation," and the middle ground is "self regulation" *See, e.g.*, Peter Swire, *Markets, Self-Regulation and Government Enforcement in the Protection of Personal Information*, *in* Privacy and Self-Regulation in the Information Age 3 (1997). While this typology serves well to categorize the tools available to regulate privacy, my interest here is focusing on the divergent goals that privacy proponents seek to advance.

[53] The classic account is, of course, George Orwell's Nineteen Eighty-Four (1949).

[54] Arthur R. Miller, The Assault on Privacy 20 (1971).

[55]*See, e.g.*, *Big Corporations Can Have Their Own CIA*, THE NEW REPUBLIC, Feb. 18, 1967, at 18. Thirty years ago Alan Westin identified various factors related to the growth of the dossier society: The number of public and private programs gathering data, personal mobility, the facility of gathering and manipulating data through the digital computer, the ability of computers to share information through common computer languages, and the advent of credit cards and other alternatives to cash. *See* Alan Westin, Privacy and Freedom 160-63 (1967).

[56]*See, e.g.*, William H. Whyte, Jr., The Organization Man (1956), Myron Brenton, The Privacy Invaders (1964); Alan F. Westin, Privacy and Freedom (1967); Jerry Martin Rosenberg, The Death of Privacy (1969); Arthur R. Miller, Assault on Privacy (1971).

[57] Vern Countryman, *The Diminishing Right of Privacy: The Personal Dossier and the Computer*, 49 TEX. L. REV. 837, 838 (1971). One author highlights the threat posed by the combination of relational databases with point of sale ("POS") systems that gather data about individual purchases. Frequent shopper programs allow any marketing firm, manufacturer, employer, private investigator or Federal agency to know who has hemorrhoids, who reads supermarket tabloids, who eats chunky peanut butter, or who smokes cigarettes. . .One could imagine a person losing medical or health insurance coverage because he or she happens to buy a pack of cigarettes for a friend. Madsen, *supra* note 12, at 136.

[58] An example would be discrimination based on zip code as a proxy for racial discrimination. As the demographic formulas used for marketing or other purposes become more and more complex, it becomes increasingly difficult, bordering on the impossible, to probe behind the demographic formula to find the suspect discriminatory core, however dossier society critics like Oscar Gandy suspect it lurks there. *See* Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*, 1996 U. CHI. LEGAL F. 77-79 (1996).

[59] "[M]y concern about the status of privacy in cyberspace is fundamentally a concern with discrimination." *Id*. at 79. The management of relations between individuals and corporations is based on the treatment of individuals as members of these constructed classes, rather than as unique and autonomous individuals. . . "Rejection based on the performance of the group in the area, rather than individual performance, is permitted within the bounds of the qualifications set forth." *Id*. at 130 (quoting Robert J. Posch, Jr., The Complete Guide to Marketing and the Law 765 (Prentice Hall 1988)).

[60] For a philosophic discussion of the value of privacy see Julie Inness, Privacy, Intimacy and Isolation, (1992) (stating that privacy is desirable because it favors other goods such as self respect and the ability to foster intimate relationships). A sociological discussion of the value and uses of privacy is contained in Westin, Privacy and Freedom , *supra*, note 56. The arguments regarding uses of privacy are reviewed in numerous law review articles as well. *See, e.g*., Kang, *supra* note 12.

[61]*See*, Kang, *supra* note 12, at 1260-61.

[62]*See, e.g*., Michel Foucault, Discipline and Punish (Alan Sheridan trans., Pantheon Books 1977) (1975).

[63]*See* Kang, *supra* note 12, at 1260; Gavison, *supra* note 28, at 460; Foucault, *supra* note 62, at 35 (discussing the "chilling effect" of surveillance); Jeffrey Reiman, *Driving to the Panopticon, A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 Computer & High Tech. L. J. 27, 28 n. 2 (1995) (discussing loss of privacy that will result from complete visibility of behavior for drivers using an Intelligent Vehicle Highway System "IVHS").

[64]*See* Gandy, *No End In Sight*, *supra* note 59, at 123-25 (being watched, as by a peeping Tom, injures our "moral ownership of ourself."); Kang, *supra* note 13, at 1063 (highlighting that Professor Kang poses a vivid hypothetical example of a machine which would allow the remote sensation of touch without the subject being aware of its use, and describes the sense of violation most people would feel in connection with the use of such a machine). *Id*. at 1263.

[65]*See* Gandy, *No End In Sight*, *supra* note 59, at 123-25; Westin, *supra* note 55, at 24 (noting the universal tendency of democratic societies to restrict surveillance by their governments).

[66]*See* David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonimity and Limited Liability in Cyberspace*, 1996 U. Chi. Legal F. 139 (1996) (arguing that anonymous or pseudonymous communication in cyberspace fulfills an important political role, but also acknowledging the possible benefits of imposing a bonding requirement to protect against the harm that can be caused by such speech).

[67]*See* Gandy, *No End In Sight supra* note 54, at 123-25 (depicting that constant surveillance stunts the maturity of citizens and injures them as individualists because persons always being monitored and supervised never develop the capacity of self control and remain forever the moral equivalent of children); Reiman, *supra* note 63 (discussing "total visibility infantilizes people. It impoverishes their inner life and makes them more vulnerable to oppression from without." Reiman also makes the point that privacy and the individualism it fosters are integral to a liberal conception of politics and society).

[68] Those concerns are reflected, for example, in the Computer Matching and Privacy Protection Act, *supra* note 49, and the Fair Credit Reporting Act, *supra* note 48, both of which provide certain protections against harm from inaccurate results of computer processed personal data.

[69]*See, e.g*., Countryman, *supra* note 57, at 869 (arguing that the only hope for substantial protection for privacy against computerized dossiers is that they not be allowed to exist).

[70] Market language is also used in a related, though different, sense by some commentators and advocates.

See, e.g., President Willam J. Clinton, Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce*, July 1, 1997, at 17 *available at* (visited May 15, 1999) <http://www.iitf.nist.gov/eleccomm/ecomm.html/>. (stating that "disclosure [of privacy policies] by data gatherers is designed to stimulate market resolution of privacy concerns by empowering individuals to obtain relevant knowledge about why information is being collected, what the information will be used for. . ."). "Market resolution" in this sense means simply that consumers can avoid sites that make unwanted demands on their privacy, not that a market in information will develop, which I have identified as the core of the market opportunist position. Other sources discuss the likelihood that "market discipline" will punish sites or institutions that the public associates with abusive privacy practices. It seems likely, however, that such market discipline only will be brought to bear against egregious violators of community norms whose activities take place in the visible portion of the privacy spectrum.

[71] Professor Noam discusses and rejects three arguments against developing markets in personal data. *See* Noam, *supra* note 7, at 30-32. First, just because privacy may be a fundamental right does not mean individuals should not be allowed to trade it, based on the value they perceive it to have for themselves. Second, the fact that consumers have less knowledge of the value of the transaction than their commercial counterparties, and therefore will be unable to trade effectively, underestimates the information leveling effect of competition. Third, the argument that the poor will be forced to sell their privacy to make ends meet ignores the equally unfortunate fact that personal information about the poor is of limited value to commercial marketers. *Id*.

[72]*See, e.g.*, Noam, *supra* note 7, at 22 ("[M]arkets can be utilized much more than in the past."); Laudon, *supra* note 33, at 41; Hal Varian, *Economic Aspects of Personal Privacy*, *in* Privacy and Self-Regulation in the Information Age 35, 39 (1997). In addition, the following authors, while not necessarily advocating government measures to promote trading markets in personal data, have analyzed privacy issues from a market perspective. Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L. J. 2381 (1996); Paul M. Schwartz, *Privacy and the Economics of Personal Healthcare Information*, 76 TEX. L. REV. 1 (1997); Peter P. Swire, *Cyberbanking and Privacy: the Contracts Model*, (abstract of talk for Computers, Freedom & Privacy '97, San Francisco (March 1997)), *available at* (visited May 30, 1999) <http://www.osu.edu/units/law.swire.htm>; Kang, *supra* note 13; Sharfman, *supra* note 6.

[73]*See* Noam, *supra* note 7, at n.33 (stating that consumer information business is a "multi-billion dollar a year business, centered on credit bureaus. . . .").

[74]*See* Laudon, *supra*, note 32, at 41. As a further consequence [of lack of individual rights in personal data] the price of personal information is so low that information-intense industries become inefficient in its use. The price is low because the price of personal information does not reflect the true social costs of coping with personal information. The market is dominated by privacy-invading institutions. As a result, there is a disturbing growth in privacy invasion.

[75]*See* Swire, *supra* note 52, at 6.

> The key market failures with respect to privacy concern information and bargaining costs. The information costs arise because of the information asymmetry between the company and the customer -- the company typically knows far more than the customer about how the information will be used by the company. . .The costs of learning about companies' policies are magnified by the difficulty customers face in detecting whether companies in fact are complying with those policies. . . .The problems are exacerbated by the costs of bargaining for the desired level of privacy. . . To be successful, bargaining would likely require a considerable degree of expertise in privacy issues, as well as a substantial commitment of time and effort.

> The cost of this elaborate bargaining process is likely to exceed the incremental benefit in privacy to that citizen.

[76]*See* Laudon, *supra* note 32, at 41. Under current law, the ownership right to personal information is given to the collector of that information, and not to the individual to whom the information refers. Individuals have no property rights in their own personal information. As a result, they cannot participate in the flourishing market for personal information . . . .

[77]*Id*.

[78]*See id*. at 43.

[79]*See* Sharfman, *supra* note 6, at 639 (1996) (favoring an online default rule under which website promoters can obtain rights to information by publishing warnings noting that the environment is a "disclosure environment" -- meaning that none of the activity online is private -- and an opportunity to opt out. An opt in rule would be inefficient since data sources, like phone books, are only valuable if most people participate. As a result, he opposes, on efficiency grounds, any rule that would create an incentive for people to opt out.); Kang, *supra* note 13 (favoring a default rule under which data can only be used in connection with the actual transaction for which it is gathered, absent consent; Professor Kang fears that the transaction costs to consumers of learning about how to protect and buy back their privacy rights, plus the impossibility of buying back all of them, will result in any other default rule giving individuals less than the optimum amount of privacy over personal information).

[80]*See* Laudon, *supra*, note 32, at 42. Professor Laudon foresees establishment of a marketplace in which individual ownership of personal information would be recognized, and individuals would have the right to sell their information to information intermediaries on a "National Information Exchange." *Id*.

[81]*See* Denise Caruso, *Digital Commerce: Personal Information is Like Gold in the Internet Economy, and the Rush is on to both Exploit It and Protect It*, N.Y. TIMES, Mar. 1, 1999, at C4. This article also discusses the advent of "Free PC," a company which offers to provide consumers with a free PC if they will agree to fill out a detailed questionnaire regarding their personal characteristics and lifestyle, then submit to being bombarded with marketing materials from advertisers. *Id*. The author credits the terms "infomediaries" to John Hagel, author of Net Worth: Shaping Markets When Customers Make the Rules (1999).

[82]*See* Noam, *supra*, note 7, at 23 (citing data regarding willingness of telephone subscribers to pay additional fee for unlisted numbers as proof that consumers are willing to pay for privacy at least under certain circumstances).

[83]*See id*. at 28-29. Professor Noam notes that because the same personal information can be valuable to multiple marketing entities the information may be sold more than once, making it more valuable to the seller. As a result, it will be difficult for consumers to outbid those entities to "buy back" their privacy rights at a reasonable price. "[F]or personal data banks containing information about individuals, market transactions are unlikely when the information is of use to many others, or it will be acquired by them. In either case the personal information, if valuable, becomes public information." *Id*.

[84]*See* Laudon, *supra*, note 32, at 43.

[85] Swire, *supra* note 52, at 6.

[86]*See* Henry H. Perritt, Jr., *Regulatory Models for Protecting Privacy in the Internet*, *in* Privacy and Self Regulation in the Information Age 107-09 (1997) (stating that property right in personal information would be cumbersome and expensive to administer; enforcement would be a "nightmare"; the failure of some

subjects to part with their data would make personal information databases incomplete and therefore less valuable for everyone; demands for compensation - even at small amounts per person - would be too expensive and it would be difficult to deliver consideration in small increments).

[87]*See* Varian, *supra* note 72, at 40 (citing fears that government will assign ownership of personal data to individuals in a manner that makes it difficult or impossible to sell it, thereby hampering development of a market in such data.); Noam, *supra* note 7, at 26, 30-31 (stating that markets require a legal environment which allows such transactions to be carried out; the author would limit government regulation to elimination of high transaction costs which otherwise prevent a market in such information from developing).

[88]*See* Noam, *supra* note 7, at 26 (stating that one of the prerequisites for markets in personal information to develop is "[s]ymmetry of information among the transacting parties.")

[89]*See* discussion *supra* note 79. Professor Kang analyzes alternative default rules in light of both market and human dignity concerns and concludes that the rule he proposes meets the objectives of both sorts of analyses. *See* Kang, *supra*, note 13.

[90]*See* Perritt, Jr., *supra* note 86, at 108.

[91]*See* Patricia Mell, *supra* note 43, at 78 (advocating statutory recognition of property rights in a "persona" consisting of personal information about the individual); Laudon, *supra*, note 32, at 42 (discussing that "the function of government here should be to restore power to one class of participants in the market, namely individuals, by vesting ownership of personal information in the individual. The second function of government is to ensure the orderly functioning of a personal information marketplace." Laudon suggests recognition of a common law property right of an individual in his or her "data image", analogous to photographic images of individuals which already receive protection at common law); Noam, *supra*, note 7, at 26 (mentioning "[t]he ability to create property rights, or to exclude" as a prerequisite to the creation of a market in personal data. This implies either government action to recognize and enforce such property rights, or the development of technological means to exclude others regardless of the state of the law).

[92] Some have taken the position that the entire superstructure of contracting, enforcement, and payment of consideration may simply be too complicated and expensive to be practical, even given the efficiencies of the Internet. *See e.g.*, Perritt, *supra* note 86, at 108.

[93]*See* Swire, *supra* note 52 at 5-6 (stating that one of the difficulties in establishing markets for privacy is the difficulty individual consumers would have in policing the behavior of online partners).

[94]*See, e.g.*, Clinton & Gore, *supra* note 70, at 16 ("commerce on the GII [Global Information Infrastructure] will thrive only if the privacy rights of individuals are balanced with the benefits associated with the free flow of information"); *Privacy Online*, *supra* note 5, at 4. (Public opinion poll findings "suggest that consumers will continue to distrust online companies and will remain wary of engaging in electronic commerce until meaningful and effective consumer privacy protections are implemented in the online marketplace. If such protections are not implemented, the online marketplace will fail to reach its full potential").

[95]*See* Peter Swire, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive (1998). In Chapter 4, Professor Swire weighs the arguments that privacy regulation will hinder or promote the development of ecommerce, and concludes that certain modest and focused regulatory efforts, or measures to define rights in personal data, may foster consumer confidence and hence boost ecommerce, but that sweeping information rights schemes will probably hinder it. *Id.* at 76-89; *see also* Blumenfeld, *supra* note 23, at 349-50 (The potential of the Internet to become a "virtual business market

without walls" will be "stifled if those running the shops do not address consumer's privacy concerns").

[96]*See supra* note 1.

[97]*See* Blumenfeld, *supra* note 23, at 382 (urging business to engage in self regulation so government will not "step in and fill the void").

[98]*See* Clinton & Gore, *supra* note 70, at 16 (referring to "balancing" privacy rights against "the benefits associated with the free flow of information"); *Privacy and the NII*, *supra* note 13, at 3 ("[P]rivacy interests are not absolute and must be balanced against the need for accountability, since the unabridged flow of information."); Irene Hashfield and Sara Fitzgerald, *The Role of Consumer Education in a Self Regulatory Privacy Regime*, *in* Privacy and Self-Regulation in the Information Age 155, 157 (1997) ("Effective ways of addressing [privacy] concerns are complicated by a number of factors, including: . . . the need to balance the protection of legitimate personal privacy rights with legitimate commercial activities. . .").

[99]*See* Swire, *supra*, note 52, at 83 ("Privacy laws are likely to be significantly less important for bolstering consumer confidence if the security risk, and the accompanying risk of direct financial loss, is understood to be small").

[100]*See* Sharfman, *supra* note 6 (Most persons do not care about disclosure of online activity based, for example, on limited use of anonymous remailers; as a result, all that fairness and efficiency require is that the users that do care be given an opportunity to "opt out").

[101] The HEW Advisory Comm. Report included five privacy principles, referred to as the "Code of Fair Information Practices":

> 1. There must be no personal data record-keeping system whose very existence is secret.
>
> 2. There must be a way for individuals to find out what information about them is in a record and how it is used.
>
> 3. There must be a way for individuals to prevent information about them obtained for one purpose from being used or made available for other purposes without their consent.
>
> 4. There must be a way for individuals to correct or amend a record of identifiable information about them.
>
> 5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of data.

Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dep't of Health, Education & Welfare, Pub. No. (OS) 73-94, Records, Computers and the Rights of Citizens 41 (1973).

[102]*See* OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

> The Guidelines establish eight privacy principles: (1) collection limitation principle (data to be collected lawfully and "where appropriate" with the subjects consent; (2) data quality principle (data to be kept accurate); (3) purpose specification principle (purpose of collection to be specified); (4) use limitation principle (no disclosure for other purposes without consent); (5)

security safeguards principle (security of data), (6) openness principle (ability to establish the identity of the data controller); (7) individual participation principle (data subjects right of access); and (8) accountability (enforcement and sanctions).

See id. at para. 7-14.

[103]*See* Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe European Treaty Series No. 108, Oct. 1, 1985. This convention includes principles similar to the OECD guidelines.

[104]*See Privacy and the NII*, *supra* note 10. That report, in turn, built on the work already done by other entities including the OECD.

[105]*See* Directive 95/46/EC of the European Parliament and of the Council of Oct. 24, 1995, on the protection of individuals with regard to the processing of personal data an on the free movement of such data. Official Journal No. L 281, 23/11/1995 p.003.

[106]*See* Clinton & Gore, *supra* note 70. The document was generated by a task force headed by Ira C. Magaziner, Senior Advisor to the President for Policy Development. The Information Infrastructure Task Force is an interdepartmental task force established by the Clinton Admin. and chaired by the Sec. of Commerce to address issues related to the "National Information Infrastructure." The final draft of the report was issued by the Task Force on Jan. 17, 1997, and the document was issued by the White House under the names of President Clinton and Vice President Gore on July 1, 1997. Information regarding organization of the IITF can be obtained at the IITF web- page, *available at* (visited on May 15, 1999) <http://www.iitf.nist.gov/index.html>.

[107] According to the *Framework*, the two main principles for fair information practices are "awareness" and "choice" -"data gatherers should inform consumers what information they are collecting and how they intend to use such data, and [d]ata-gatherers should provide consumers with a meaningful way to limit use and re-use of personal information." Clinton & Gore, *supra* note 70, at 17.

[108]*See* Dept. of Commerce, *Elements of Effective Self Regulation for the Protection of Privacy and Questions Related to Online Privacy*, No. 980422102-8102-01, *available at* <http://www.ntia.doc/ntiahome/privacy/6_5_98fedreg.htm>.

[109]*See supra* note 79.

[110] The fair information practices handling guidelines discussed previously, generally assume that "opt out" rules are adequate except for certain categories of sensitive data. The OECD Guidelines state that "Personal Data should not be disclosed, made available or otherwise used for purposes other than those specified. . . except with the consent of the data subject . . ." except for those purposes disclosed at the time the information was gathered or other "not incompatible" uses which are "specified on each occasion of change of purpose." OECD, *supra* note 102 at para.. 10, "Use Limitation Principle," and para. 9, "Purpose Specification Principle." This appears to allow a data appropriator to use data for new purposes upon giving subsequent notice without giving the subject the ability to opt out. The Privacy Working Group Guidelines state, "If an information user seeks to use personal information in an incompatible manner (compared with the understanding of the data subject at the time the information was obtained regarding the uses that would be made of the information), the user must first notify the individual and obtain his or her consent." *Privacy and the NII*, *supra* note 6, at para. 22. However they also provide that "opt out" consent may be sufficient, depending on the significance of the information and its use to the individual. The individual's understanding is principally a matter of the notice given when the information was first obtained. *Id*. The Elements of

Effective Self-Regulation created by the Dept. of Commerce clearly contemplate "opt out" consent for non-sensitive information. *See Elements of Effective Self Reputation*, *supra* note 108, at para. A2.

[111] The Council of Europe Convention states, "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions." Council of Europe, *supra* note 102, at Art. 6. The *Elements of Effective Self Regulation*, state that, "for certain kinds of information, e.g., medical information or information related to children, affirmative choice by consumers may be appropriate. In these cases companies should not use personal information unless its use is explicitly consented to by the individual, or in the case of children, his parent or guardian." *Elements of Effective Self Regulation*, *supra* note 108 at para. A2.

[112] The OECD Guidelines state that a "not excessive" charge may be assessed as a condition for obtaining access to one's data. *See* OECD, *supra* note 102, at para 13. The Council of Europe Convention, Art. 8.b, refers to obtaining access without "excessive delay or expense." Council of Europe, *supra* note 103.

[113] The OECD Guidelines state that only relevant information should be gathered. *See* OECD, *supra* note 102, at para. 10. The Privacy Working Group guidelines, state that "In all cases, the information user should only acquire that information reasonably expected to support those activities." *Privacy and the NII*, *supra* note 6 at para. 9. The Council of Europe Convention, states that data should be "adequate, relevant, and not excessive in relation to the purposes for which they are stored." Council of Europe, *supra* note 103, at Art. 5.

[114] The Privacy Working Group guidelines start out sounding highly protective. They state: "Although information storage costs decrease continually, it is inappropriate to collect volumes of personal information simply because some of the information may, in the future, prove to be so some unanticipated value." However the exception that follows swallows the rule: "Also, personal information that has served its purpose and is no longer reasonably expected to support *any current or planned activities* should not be kept." *Privacy and the NII*, *supra* note 6. This vague standard not likely to impose any significant obligation to prune databases of unneeded information.

[115] The OECD Guidelines, state simply that the data controller "shall be accountable." OECD *supra* note 102, at para. 14. The Privacy Working Group guidelines, state only that "work needs to be done" to find verification mechanisms that are not too expensive to business. *See Privacy and the NII*, *supra* note 10, at para. B2.

[116] The Privacy Working Group guidelines do not mention civil litigation or criminal sanctions, but such omissions may be understandable given that the guidelines' focus is on self-regulation. Instead the guidelines mention "cancellation of the right to use a certifying seal or logo, posting the name of the non-complier on a 'bad actor' list, or disqualification from membership in an industry trade association." *Privacy and the NII*, *supra* note 10, at para. B3. The guidelines also state that non-compliers should pay the costs of assessing their own noncompliance, and that FTC or other regulatory involvement may be appropriate when companies fail to comply with their own posted policies. *Id*. *A Framework for Global Electronic Commerce* states simply that "Consumers are entitled to redress if they are harmed by improper use or disclosure of personal information or if decisions are based on inaccurate, outdated, incomplete, or irrelevant personal information." Clinton & Gore, *supra* note 70 at 17.

[117] The OECD Guidelines state that member states should endeavor to encourage self regulation and "provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles." OECD, *supra* note 102 at para. 19(d). The Privacy Working Group guidelines are more explicit as to options for redress, stating that "When redress is appropriate, the Principles envision various forms including, but not limited to, informal complaint resolution, mediation, arbitration, civil litigation,

regulatory enforcement, and criminal prosecution, in various private, local, state, and federal forums with the goal of providing relief in the most cost-effective manner possible." *Privacy and the NII*, *supra* note 10, at para. 34.

[118] The OECD and Council of Europe guidelines and the EU Directive are not limited to the online environment, nor are they limited to data collected directly from the individual data subject. *See* OECD, *supra* note 102, at para. 2; Council of Europe, *supra* note 103, at Art. 3 (scope of the Convention is "automated personal data files and automatic processing of personal data."). *See also*, Directive, *supra* note 105, discussed at nn.120-127, *infra*. The guidelines of the Privacy Working Group specifically limit notice obligations to situations where data is gathered directly from the data subject. *See Privacy and the NII*, *supra* note 10, at II.B para. 1.

> Personal information can be collected ... directly from the individual or obtained from some secondary sources. By necessity, the principles governing these two methods of acquiring information differ. While notice obligations can be placed on all those who collect information directly from the individual, they cannot be imposed uniformly on entities that have no such direct relationship.

[119] The Directive provides, "Each member state shall provide that one or more public authorities are responsible for the application within its territory of the provisions adopted by the Member States pursuant to this directive. These authorities shall act with complete independence in exercising the functions entrusted to them." Directive, *supra* note 105, at Art. 29 para. 1. Earlier proposals made in connection with adoption of the Privacy Act of 1974, *see supra* note 49, included provision for a privacy commission to govern privacy issues within the federal government, but that proposal was watered down until the final bill included only provision for a privacy commission which would prepare a report on privacy issues and then disband. The report, when it finally was issued in 1977, contained a recommendation that a permanent privacy commission be established. *See* Madsen, *supra* note 12 at 140-41 (discussing various legislative proposals for establishment of a federal privacy commission in the 1980s). That recommendation has never been acted on.

[120] The Directive provides that each member state is to adopt and apply its own national law consistent with the Directive. *See id*. at Article 4. For a thorough discussion of the Directive and its practical impact on United States concerns, see Peter Swire, None of Your Business, World Data Flows, Electronic Commerce and the European Privacy Directive (1998).

[121] The definition of "processing" in the Directive is very sweeping. "[P]rocessing personal data ... shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Directive, *supra* note 105, at Article 2 para. (b).

[122] Member states are required to "prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." *Id*. at Article 8, para. 1.

[123] The Directive lists five "principles relating to data quality," including the principle that data must be collected fairly and lawfully, that data be collected for specific legitimate purposes and not "processed" in a way incompatible with those purposes, that data not be kept which are "excessive" in relation to the purpose for which they were collected, and that data be kept in personally identifiable form only so long as necessary. *Id*. at Article 6. Pursuant to the Directive, "Information providers should therefore not sell the personal data of their customers without their consent." *See* Dr. Herbert Burkert, *Addressing the Issue of Privacy in a European Regulatory Environment*, Presentation at the Information Superhighway Asia I, in Singapore, Sept.

5, 1996, *available at* (visited October 24, 1998) <http://www.richmond.edu/jolt/v6i1/<http://www.gmd.de/People/Herbert.Burkert/singap02.html> (Dr. Herbert is described as Senior Advisor, BMD German National research Center for Information Technology and Chairman of the Legal Advisory Board for the Information Market, European Commission.).

[124] "Criteria for making data processing legitimate" are listed separately, including the requirement that "the data subject has unambiguously given his consent", however exceptions exist which undercut the consent principle, including the provision allowing processing of data "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties who whom the data are disclosed." *Id*. at Art. 7.

[125]*Id*.

[126] The purpose of the Directive is to harmonize privacy policy in the EU to the extent that data flows can be allowed to take place freely among EU member states without the concern that exportation of data from one member state to another will diminish the protections that would otherwise be applicable to that data. *See* Directive, *supra* note 98, at Art.1 para. 2. With respect to non EU countries, however, the Directive provides that personal data transfers may only take place "if ... the third country in question ensures an adequate level of protection." *Id*. at Art. 25 para. 1. *See also*, Fred H . Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431 (1995) (discussing limitations on data flows to United States business if the Directive is enforced).

[127] While the government representatives negotiate, business groups have taken the lead in trying to find a way to comply with the EU Directive sufficient to allow data flows to continue. Many of those ideas involve voluntary commitments, through contract with EU-based data sources or commitments directly with the EU itself, to abide by the EU standard. *See, e.g.*, *The International Chamber of Commerce, Working Party on Privacy and Data Protection of the Commission on Telecommunications and Information Technologies*. (discussing model clauses prepared by the IIC that can be incorporated in contracts between U.S. recipients of data and companies in the EU desiring to transmit such personal data abroad. Such clauses essentially authorize the data exporter to enforce EU privacy standards against the data importer, and make the exporter the proxy for the importer in defending against charges of data misuse brought in the EU as a result of the importer's conduct).

[128] On Nov. 4, 1998, the Department of Commerce issued a letter headed, "Dear Industry Representative" setting forth the United States' position that self regulatory measures adopted by industry trade organizations should constitute a "safe harbor" disciplinary action or a cutoff of data flows from the European Union. The text of the Department of Commerce letter on "Safe Harbor" is *available at* <http://www.ita.doc.gov/ecom/menu.htm>. *See also* the EPIC Policy Alert for Nov. 10, 1998 *available at* <http://www.richmond.edu/jolt/v6i1/<http://www.epic.org/alert/EPIC_Alert_5.16.html>.

[129] Ambassador David L. Aaron, Undersecretary for International Trade, is leading the United States negotiating team with respect to issues related to the Directive. He issued a letter to "Dear Colleagues" on April 19, 1999, reporting on the status of the negotiations. In that letter he concluded that "the two sides have achieved a substantial level of consensus on the content of the principles, on the content of more specific guidance (frequently asked questions), and on the safe harbor procedures and benefits." Letter from Ambassador Aaron, April 19, 1999 *available at* <http://www.ita.doc.gov/ecom/aaron419.html>. The main points of disagreement are reported to be (1) rights of access to data by data subjects (the United States holding out for more limited access rights in the interest of avoiding expense to industry) and enforcement (again, the United States favoring self enforcement by industry associations). *See* James Glave, *US, EU Still Stuck on Privacy*, WIRED NEWS, Apr. 21, 1999, 3:00 A.M. P.D.T.

[130]*See* Childrens Online Privacy Protection Act of 1998, 15 U.S.C. Section 6501 (1998). The Act prohibits solicitation of information from children younger than thirteen without the affirmative consent of their parents.

[131] To monitor the status of legislation affecting online privacy issues, visit the website of the Electronic Privacy Information Center, *available at* <http://www.epic.org/>.

[132]*See Privacy Online*, *supra* note 5.

[133]*See Consumer Privacy on the World Wide Web*, *supra* note 1.

[134]*See id*. at n. 23.

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

[135]*Id*. at 5-6. The meaning of these basic principles is further discussed in *Privacy Online*, *supra* note 5, at 7.

[136]*See id*. at 6-7.
