



**From the SelectedWorks of Malla Pollack**

---

July 2001

## Opt-In Government: Using the InterNet to Empower Choice – Privacy Application

Contact  
Author

Start Your Own  
SelectedWorks

Notify Me  
of New Work

---

Available at: [http://works.bepress.com/malla\\_pollack/13](http://works.bepress.com/malla_pollack/13)

C

Catholic University Law Review

Spring 2001

Article

\*653 OPT-IN GOVERNMENT: USING THE INTERNET TO EMPOWER CHOICE-  
-PRIVACY  
APPLICATION

[Malla Pollack \[FN1\]](#)

Copyright © 2001 Catholic University of America; Malla Pollack

This is the way the [privacy] ends

This is the way the [privacy] ends

This is the way the [privacy] ends

Not with a bang but a whimper. [\[FN1\]](#)

#### I. The Suggestion: Opt-In Government

This article proposes a relatively novel model of government regulation and illustrates how the model might work with respect to Internet privacy protection for U.S. residents. [\[FN2\]](#) I suggest "opt-in government" as a practical method to integrate the democratic concept of voice with the market model of choice. [\[FN3\]](#) "Opt-in government" either (i) creates "a safe place" that persons may enter only if they wish to do so, or (ii) enables a choice that the so-called private sector has not offered. [\[FN4\]](#) One \*654 reason to try the opt-in model is that pure self-regulation does not work; business requires a strong governmental push. [\[FN5\]](#) Many Americans, [\[FN6\]](#) nevertheless, seem to honor Calvin Coolidge's aphorism that "the business of America is business."

[FN7] Further, the federal government appears intent on making the private sector "lead" in many areas. [FN8] We need a method to combine this \*655 attitude with taking care of the real business of America--Americans. [FN9]

## II. The On-Line Privacy Problem

### A. Background

Recently, the FTC recognized that the perceived lack of privacy [FN10] on the Internet bothers Americans. Privacy concerns \*656 impact both of the FTC's missions: promoting American commerce [FN11] and protecting American consumers. [FN12] Even if the business of America is business, consumer willingness to grow business to consumer electronic commerce (BtoC) [FN13] by shopping on the Internet requires, at a minimum, a change in consumer perceptions. [FN14] In 1995, the FTC began a privacy initiative dedicated to business self-regulation. [FN15] In 1998, however, the FTC suggested legislation to protect children's on-line privacy. [FN16] \*657 Disappointed by self-regulation efforts, the FTC recommended more sweeping privacy legislation in May 2000. [FN17] The majority of the FTC requested that Congress pass technologically-neutral legislation phrased in general terms, with the terms to be fleshed out by later FTC action. [FN18] However, Commissioner Orson Swindle dissented and continued to argue that allowing informed consumers to vote using their computer mice could better solve any problem. [FN19] Since 1999, major on-line businesses have showed the FTC a new framework for self-regulation, providing additional arguments against the enactment of legislation. [FN20]

Other governance models exist. For example, in 1995 the European Union (EU) issued a sweeping top-down Directive on \*658 Data Protection, [FN21] requiring member states to enact privacy protection laws both enforceable by individual lawsuits with monetary remedies [FN22] and backed by one or more public authorities (i.e., government bodies) with investigative, adjudicative, and regulatory power. [FN23] Member states were also required to halt transfer of personal data to third countries lacking adequate data privacy protections. [FN24] As a result of the EU directive, American businesses pressured the U.S. government to protect transborder data

flow between pro-privacy Europe and consumer-beware United States. [FN25] Long negotiations between the U.S. and the EU on transborder data flow [FN26] resulted, not in a United States Privacy Agency, but a set of safe harbor provisions [FN27] that met the EU's requirements. [FN28] These safe harbor provisions are entirely voluntary. If an American business desires more certainty about the continuity of data transfer to it from the EU, it may self-certify itself as \*659 conforming to the guidelines. A self-certifying business can choose between several "adequate" privacy approaches, but none require it to treat data originating outside of the EU with any care. [FN29] In sum, both bottom-up and top-down regulation of Internet privacy already exist; however, both regulatory models are problematic for protecting U.S. residents.

## B. Top-Down Regulation

### 1. Theoretical Problems

"Top-down" regulation suffers from governmental inefficiency; it is costly and time-consuming. In the fast moving technical world of the Internet, an enactment may not be promulgated in time to match the technology in use. Statutory prohibitions may fail because they consistently emerge only after the harm has been done and the technology has advanced to other anti-privacy methods. [FN30] Government, therefore, may be tempted to force effectiveness by ordering technology to freeze in place, thus denying the public the benefits of progress. Top-down regulation also prevents persons from individually choosing to allow a "harm" that, in their personal opinion, is "harmless." [FN31] If some businesses choose to offer free or less costly services in exchange for information (usually tied to advertising exposure), \*660 what is the harm in allowing consumers to accept these offers?

This type of "free service" funded by advertisers is, after all, the business model of broadcast television and radio. [FN32] Such "free service" has supported large-scale information distribution on the Internet. [FN33] Regulating against the exchange may constitute an unwarranted governmental limitation on personal freedom. [FN34] \*661 A government privacy czar raises First Amendment concerns. [FN35] The federal Constitution, [FN36] after all, sees government

(especially national government) as the proverbial bad guy [\[FN37\]](#) and is relentlessly blind to non-governmental "Big Brothers" keeping watch. [\[FN38\]](#)

A recent study reported a strong belief among U.S residents that the government can track them on the Internet, as well as a belief that someone was monitoring them on-line. [\[FN39\]](#) The press's \*662 disclosure of the FBI's Carnivore E-Mail surveillance system supports such fears, [\[FN40\]](#) as does the recent General Accounting Office report asserting that many federal government web sites are not respecting surfers' privacy. [\[FN41\]](#) Furthermore, generally worded legislation leaves the highly important details to an administrative agency. An agency could be captured by the regulated industry and could (quietly) weaken the controls through rule making and adjudicative choices. [\[FN42\]](#) The courts would likely defer. [\[FN43\]](#)

#### \*663 2. Current Status in the United States [\[FN44\]](#)

Additional privacy legislation in the United States may be likely. Congress has jumped on the privacy bandwagon. It recently enacted both the Children's Online Privacy Protection Act [\[FN45\]](#) and the Gramm-Leach-Bliley Act. [\[FN46\]](#) Many bills that mention "privacy" were pending at the end of the 106 th Congress. Of these, the Consumer Privacy Protection Act of 2000 (Privacy Act) [\[FN47\]](#) responds to the FTC's May 2000 call for general privacy legislation. [\[FN48\]](#) The Privacy Act was introduced in the Senate on May 23, 2000, and referred to the Senate Committee on Commerce, Science, and Transportation. [\[FN49\]](#)

The Privacy Act does not go far enough, despite its many good features. The Act opens with findings that declare ground breaking theoretical rights:

(1) The right to privacy is a personal and fundamental right worthy of protection through appropriate legislation.

(2) Consumers engaging in and interacting with companies engaged in interstate commerce have an ownership interest in their personal information, as well as a right to control how that information is collected, \*664 used, or transferred. [\[FN50\]](#)

Implementation details do not quite match the theory. Broadly speaking, if enacted, the Privacy Act would require consumer opt-in consent to online collection of personally identifiable information (PII) and opt-out consent for non-personally identifiable information (non-PII). [\[FN51\]](#) Third parties operating advertising services on host web sites would be bound by these limitations. [\[FN52\]](#) Personally identifiable information would not be sellable as an asset if its collector enters bankruptcy. [\[FN53\]](#) Both the FTC and state attorneys general would have standing to sue violating entities, and private parties would have individual causes of action for misuse of personally identifiable information. To encourage discovery of violations, whistle blowers would be protected from employer retaliation, at least theoretically. [\[FN54\]](#)

The FTC may extend the definition of PII:

The term "personally identifiable information" means individually identifiable information about an individual collected online, including:

- (A) a first and last name, whether given at birth or \*665 adoption, assumed, or legally changed;
- (B) a home or other physical address including street name and name of a city or town;
- (C) an e-mail address;
- (D) a telephone number;
- (E) a Social Security number;
- (F) a credit card number;
- (G) a birth date, birth certificate number, or place of birth;
- (H) any other identifier that the [Federal Trade] Commission determines permits the physical or online contacting [\[FN55\]](#) of a specific individual; or
- (I) unique identifiable information that an Internet service provider, online service provider, or operator of a commercial website collects and combines with an identifier described in this paragraph. [\[FN56\]](#)

The borderline item missing from this list, unless the FTC rules include it, is the Internet Pro-

toocol address (IP address) of individual browsers. The extent to which IP addresses are PII is controversial. Static IP addresses may be nearly as tied to one person as an email address. [\[FN57\]](#) Certainly, an IP address can be tied to a specific computer (or human surfer) if personally identifiable information is submitted; the information collector simply records both in tandem. Some sites can read the email address stored in the surfing browser without the human surfer's knowledge. [\[FN58\]](#) Presumably, a very interested observer could tie together multiple sessions by the same person using different IP addresses by catching the same PII used with different IP addresses. An IP address, with variable effort, can be traced back to a specific computer, which itself may be strongly related to a specific person, or a small group of persons.

A static IP address is clearly more revealing to a third person than is a dial-up address provided by an Internet service \*666 provider such as AOL; a dial-up address may be different for each session. The extent to which such addresses actually vary, however, is neither clear nor legally controlled in the United States. Even if a dial-up service provider routinely changes a user's IP address, the service provider can easily obtain the correlations. [\[FN59\]](#) Furthermore, most service providers track their users' trips across the web. [\[FN60\]](#)

According to a recent study by Joel Reidenberg and Paul Schwartz, the member states of the EU, although ahead of the United States in developing privacy law, have yet to reach a clear policy on the status of IP addresses. [\[FN61\]](#) For example, although Belgian law favors anonymity, determining whether IP addresses are covered by Belgian data protection law is problematic. [\[FN62\]](#) Belgian authorities have stated that information is not fully anonymous unless the content of the data is such that its possessor cannot re-identify the person concerned without special effort. French law is also wary of any information that might be traced back to a specific person or to a relatively small group of persons. Rulings relating to different media, however, can be analogized to support opposite outcomes as to IP addresses. [\[FN63\]](#) The issue still remains open in German law, but IP addresses are likely to be protected if other available types of information may be used to allow identification of an \*667 individual. [\[FN64\]](#) In the United Kingdom, IP ad-

addresses are likely to be considered protected personal information when a data possessor has access to additional data allowing identification of the subject, but not otherwise. [\[FN65\]](#)

American Internet advertising services, furthermore, place advertisements as if the browser IP address was tied to a human target with a known psyche. For example, 24/7 Media "target[s] advertisements to specific computers and . . . measure[s] ad effectiveness" by using "anonymous, non-personal, demographic information" supplied by some "advertisers [and] Web publishers" in combination with "other anonymous demographic information" that is "contained in 24/7 Media's database." [\[FN66\]](#) If the Privacy Act does not protect IP addresses, it will not fully protect specific human psyches from intrusion and shadowing.

In addition to its failure to handle IP addresses, the Privacy Act is underinclusive in other ways. It would reach only web sites and on-line services operated for commercial purposes, excluding non-profit entities. [\[FN67\]](#) The non-profit health site that you visit may, therefore, pass information onto your insurance company without violating the statute - despite the "rights" proclaimed in the bill's findings. Even if backed by unusually strong FTC-promulgated regulations, the Privacy Act would not sufficiently combat anonymous on-line profiling. Private individuals have no cause of action regarding non-PII; and opt-out "choice" is allowed. Further, the Privacy Act would not create an easily navigable, fully private Internet space. [\[FN68\]](#) Still, \*668 the bill would be an enormous advance in individual control of \*669 personal information for U.S. residents.

## C. Bottom-Up Regulation

### 1. Theoretical Problems

Tight bottom up regulation, however, seems even less likely. The problems include: (a) non-transparency; [\[FN69\]](#) (b) consumers' time constraints; (c) consumers' limited technical expertise; (d) business' reluctance to invoke sufficient penalties; and (e) Peter Swire's mice-players who cannot be controlled effectively by regulatory entities because they are small, mobile, and breed

rapidly. [\[FN70\]](#) Existing partial solutions, furthermore, disadvantage small businesses [\[FN71\]](#)-  
-despite hoopla about the Internet-empowering, less capitalized businesspersons. [\[FN72\]](#)

**\*670** Market choice activation of the "invisible hand" requires transparency. Consumers cannot choose x unless they can tell when x is, and is not, part of the offer. In many ways, transparency does not exist in the market for on-line privacy. First, a user may not find out that his private information was shared with a third party. Second, if the user does find out that his private information was shared (perhaps he receives unrequested catalogs or e-mail advertisements), he is unlikely to know which information collector is responsible. Putting a different false statement into each submission in order to identify any information thief is an unrealistically large burden **\*671** for a non-paranoid Internet user. [\[FN73\]](#) Third, on-line information collection can be accomplished without the consumer's knowledge. "Cookie" technology can abstract information invisibly as one merely browses a web page; one does not have to enter information into data fields or click on banner advertisements. Furthermore, an unannounced third party administering advertising content on the web page, "banner advertisements," may collect this information. [\[FN74\]](#) Information regarding a consumer's Internet activities can be consolidated without the consumer's knowledge. [\[FN75\]](#)

If consolidated and shared with interested third parties, information that is innocuous in some contexts may have serious repercussions. This raises questions such as: (1) would you want perspective employers to know that you looked up AIDS in ten free on-line medical databases?; [\[FN76\]](#) (2) would you **\*672** want your boss to know that you routinely cruise help-wanted ads?; (3) would you, if a teacher, want the parents of your grade school students to know your interest in nude vacation resorts?; (4) even if you are "innocent," would you want the burden of justifying your actions? [\[FN77\]](#); and (5) would you want to relinquish the ability to act in different locally appropriate manners inside different normative communities? [\[FN78\]](#)

Even to people who enjoy receiving targeted advertising enabled by "cookies," [\[FN79\]](#) some outcomes of consolidated information may be unwelcome. For example, if you visit an on-line

store, would you want the vendor to know that you have an above average interest in the vendor's specialty product and a relatively deep pocket? If so, you may be asked to pay more for that product at every store you visit. [\[FN80\]](#) Retailers with more information are more likely to use the negotiation price strategy for high-ticket items.

**\*673** Even if you believe that your life is blameless and bland enough to showcase in a Macy's store window without embarrassment, is it desirable to allow profiling that enables red-lining? Or to enable more efficient manipulation of consumers? Of voters? [\[FN81\]](#) Inconsistent pronouncements are easier to hide if one can send different content to multiple targeted groups. Information affects reality, even if that information is wrong, misleading, or misunderstood. [\[FN82\]](#)

## 2. Current Status in the United States [\[FN83\]](#)

Web page privacy notices are a good beginning, as are the emerging "seal" programs, such as TRUSTe and BBBOnLine, which reassure consumers that the visited site follows certain privacy guidelines. [\[FN84\]](#) In the summer of 2000, the National Advertising Initiative (NAI) announced a new policy providing some protection against invisible advertisement-placement **\*674** firms.

Under the NAI principles, consumers will be notified of network advertisers' profiling activities on host web sites and their ability to choose not to participate in profiling. Where PII is collected for profiling "robust notice will be required at the time and place such information is collected and before the personal data are entered." [\[FN85\]](#) Where non-PII is collected for profiling, clear and conspicuous notice will be in the host web site's privacy policy. Under the NAI principles, NAI companies will contractually require that host web sites provide such disclosure and will make reasonable efforts to enforce these requirements.

At the time of the announcement, NAI's membership allegedly controlled about ninety percent of the network advertising industry (looking at revenue and number of advertisements). [\[FN86\]](#) The FTC, especially its Commissioner Orson Swindle, greeted the NAI guidelines with

enthusiasm. [\[FN87\]](#) The stock market presumably saw the guidelines as pro-advertiser because shares in the Internet advertising firm DoubleClick rose thirteen percent in one day. [\[FN88\]](#) Such self-regulation, however, leaves ten percent of Internet advertising unlinked to privacy notices. In \*675 addition, some firms may drop out of the program, [\[FN89\]](#) new market entrants may not join, and some website hosts may not cooperate. [\[FN90\]](#) Most violations, except for the notice provisions of the guidelines, will be difficult for consumers to detect.

Furthermore, privacy notices, even with opt-out or opt-in provisions, are not enough. [\[FN91\]](#) Many existing policies are long, complex, confusing, and self-contradictory. [\[FN92\]](#) Even ignoring problems surrounding the clarity and credibility of privacy policies, the user must sacrifice a considerable amount of time to read the policy at each website visited. [\[FN93\]](#)

Individually obtained technological privacy protection is not sufficient. Disregarding the pros and cons of specific privacy-enhancing technology, [\[FN94\]](#) to expect users to acquire technology to \*676 block privacy invasions puts the burden on consumers. Privacy should not be a luxury reserved for the computer savvy or for those who can afford such protection. [\[FN95\]](#) The time burden, even for the savvy, is heavy and never-ending, and even the installation of the most up-to-date pro-privacy technology will not defend against technology upgrades. Furthermore, information seeking technology may be protected as a trade secret inaccessible even to the computer savvy.

a. Focused Reality Check: NAI Principles, September 2000

Government is not the only slow mover. Industry has not rushed into privacy protection. In 1995, the FTC began publicizing the need for privacy protection on the Internet and its desire for industry to take charge. [\[FN96\]](#) In November 1999, the FTC held a public workshop on on-line profiling, [\[FN97\]](#) and the NAI responded by submitting drafts of proposed self-regulation. [\[FN98\]](#) The final text was not given to the FTC, however, until July 27, 2000. [\[FN99\]](#) With one exception--the ban on merging PII with non-PII--no one is required to follow the NAI principles for yet another six months. [\[FN100\]](#) Entities can join the NAI after the principles are in force and

still get another six months to \*677 comply, with this same exception. [FN101] Furthermore, the NAI principles may be amended by a four-fifths vote of the signatories. [FN102] A one-stop opt-out spot expected to have pro-NAI publicity is supposed to be established; however, it presently has no opt-out. [FN103] Perhaps some improvement will occur when the six-month window elapses. [FN104]

Certainly self-regulation is an improvement over no regulation, but the NAI principles are incomplete. First, the NAI principles do not affect targeted advertising using non-PII. A user can still be followed around the Internet by advertisements chosen, partially because of the sites he has previously visited, the search terms he has used, his domain name, and unclarified other data. Advertisers have no duty to notify the Internet user of this practice or of the data collection on which it is based, or to provide the user with the ability to opt-out of such advertising or the supporting data collection. [FN105] The NAI principles also do not stop statistical reporting based on non-PII. [FN106] The NAI principles do require an opt-in notice for collection of PII, [FN107] but PII seemingly does not include potentially revealing Internet protocol addresses. These addresses may be used to obtain PII, as the NAI principles obliquely admit.

This admission meshes with a gigantic loophole inside NAI's "Dissemination Restrictions," which state that "[n]etwork advertisers shall contractually require that any third parties to which they provided PII data adhere to, at a minimum, OPA Guidelines." [FN108] For third parties to whom advertisers provide \*678 non-aggregate, non-PII data to be merged with PII data possessed by the third party, the network advertisers must require those transferees to adhere to the NAI self-regulatory principles--"unless the non-personally identifiable data is the proprietary data of the particular third-party publisher or advertiser." [FN109]

Any network advertiser is allowed to sell individuals' non-personally identifiable dossiers to any client. If technology did not allow this data to be merged with individuals' names, addresses, and social security numbers, i.e., their PII, no restrictions would be required. Restrictions, however, were written. I conclude, therefore, that privacy advocates who warned the FTC that

non-PII was easily integrated with PII were correct. [\[FN110\]](#) To be able to merge PII and non-PII without even theoretical restraint, furthermore, the client and network advertiser merely need to declare that the PII is the client's property, as opposed to the property of the network advertiser. These are merely straw regulations to comfort straw men. [\[FN111\]](#)

NAI members are supposed to contract for their clients to follow certain notice, choice, and non-merger provisions. NAI members, however, have no obligation to stop selling information to clients who violate such covenants, to sue clients who violate these covenants, or to report the identity of uncooperative clients to the public or the appropriate \*679 governmental body. NAI members are merely required to "make reasonable efforts to enforce the contract." [\[FN112\]](#) Again, these are straw regulations to comfort straw men.

b. Focused Reality Check: The Direct Marketing Association, September 2000

The privacy policy posted on the Direct Marketing Association "DMA" web site in September of 2000 offers an interesting reality check. [\[FN113\]](#) DMA is one of the proud parents of the NAI. [\[FN114\]](#) Near the beginning of its privacy policy, I was reassured by the statement that "[f]or each visitor, our Web server does not recognize information regarding the e-mail address and we do not place cookies on visitors' hard drive[s]." [\[FN115\]](#) But several paragraphs later into the policy, I discovered that "we" does not cover all entities involved in the site: "The DMA works with a third party that serves ads to this site. To find out more about how Flycast manages the privacy information in conjunction with serving ads on this site, please go to [http://www.flycast.com/about\\_us/about-privacy.shtml](http://www.flycast.com/about_us/about-privacy.shtml)." [\[FN116\]](#) The DMA's notice does not indicate the information being collected by Flycast; nor does it state that you can opt-out of Flycast's information collection by visiting the supplied URL. [\[FN117\]](#) Both of these wording choices lessen browsers' incentives to follow the supplied hyperlink. [\[FN118\]](#) If you do attempt to reach \*680 <http://www.flycast.com>, the URL listed on your browser automatically morphs into <http://www.engage.com>. [\[FN119\]](#) At this point, many jumpers may assume that the hyperlink is incorrect and may stop trying to locate an opt-out point. [\[FN120\]](#)

Engage.com, also a proud member of the NAI, [\[FN121\]](#) does place cookies on visitors' browsers (presumably including when you visit the DMA site). A visitor can opt-out of allowing Engage.com to track him across the Internet by accepting an "opt-out cookie." The privacy material at the Engage.com site, however, does not mention the DMA site. [\[FN122\]](#) Rather, the privacy-seeking surfer has to understand the Internet sufficiently to recognize the relationship between banner advertisements on other sites and Engage.com's privacy discussion. Otherwise, the surfer may inadvertently ask to be excepted only from being tracked \*681 while at Engage.com's home site. [\[FN123\]](#) Opting out of being tracked on the DMA site, therefore, is more than a de minimus burden for the unsophisticated or time-conscious Internet surfer.

Neither the DMA nor Engage site contains factual misstatements; many unsophisticated, rushed, or trusting customers visiting the DMA site, however, may stop reading its privacy policy as soon as they reach "[w]e do not place cookies on visitors hard drives." [\[FN124\]](#) I do not consider this "clear notice." Nor do I care that Engage uses double-blind patent pending technology [\[FN125\]](#) to keep the 800-item profile (used to justify charging advertisers the most for banner advertisements) [\[FN126\]](#) to segregate any personally identifiable information from the ad-choosing profile it is building. [\[FN127\]](#)

First, "anonymous" does not mean "harmless." The NAI self-regulation rules were issued in response to FTC pressure about on-line profiling (including anonymous profiling). The FTC exerted this pressure because many Americans were very upset by the practice of profiling customers, even "anonymous profiling." [\[FN128\]](#) Sixty-three percent of consumers are uncomfortable with anonymous web tracking. Ninety-one percent are uncomfortable with web sites sharing information in order to track people across multiple sites. [\[FN129\]](#)

Second, a consumer cannot be sure that a company will never attempt to integrate the consumer's "anonymous" ad-choosing \*682 800-item profile with PII. [\[FN130\]](#) At the FTC's Workshop on Online Profiling, DoubleClick claimed that technological barriers prevented joining its anonymous profiles to PII without consumer approval. [\[FN131\]](#) DoubleClick, however, now ad-

mits that one of its advertising customers does join the allegedly unjoinable. [\[FN132\]](#) The FTC's report to Congress takes joinder seriously:

The [2000] Survey data also demonstrate that 68% of [Web] sites in the Random Sample, and 77% in the Most Popular Group, collect non-identifiable information. The weighted analysis figure is 76%. Most of the sites surveyed, therefore, are capable of creating personal profiles of online consumers by tying any demographic, interest, purchasing behavior or surfing behavior information they collect to personally identifiable information. [\[FN133\]](#)

Additionally, permanent enforceability of privacy policies cannot be assumed. Ecommerce companies do change hands and go bankrupt. Bankruptcy abrogates contracts. The Internet retailer Toysmart.com (Toysmart), for example, represented in its posted privacy policy that it would never share \*683 consumers' personal information with any third party. [\[FN134\]](#) When Toysmart entered into bankruptcy proceedings, however, it attempted to sell its customer information database. The FTC sued. FTC and Toysmart reached a settlement that did not enforce the privacy policy. [\[FN135\]](#) The settlement did, however, limit possible buyers of the database to businesses that "concentrate [their] business in the family commerce market, involving the areas of education, toys, learning" and that "expressly agree to be Toysmart's successor- in-interest" regarding the database. [\[FN136\]](#) Bankruptcy Judge Carol Kenner dismissed the agreement between the FTC and Toysmart as premature, "without prejudice to the parties raising these issues" later. [\[FN137\]](#) According to some sources, the judge commented, more disturbingly, that she "concur[s] with the creditors' committee opinion that to restrict the sale to a particular type of buyer is counterproductive to the interests of the estate." [\[FN138\]](#) Toysmart's database included information on some 190,000 human (as opposed to merely juridical) persons. [\[FN139\]](#) These persons might have been over-trusting because Toysmart displayed a TRUSTe seal. [\[FN140\]](#) A ray of hope, though, Congress may pass legislation preventing transfer of PII at bankruptcy if the transfer violates the debtor's privacy policy. [\[FN141\]](#)

\*684 c. Focused Reality Check: Banner Advertisements on Yahoo!, September

2000

Since the vast majority of websurfers user commercial search engines, I experimented further by visiting Yahoo! [\[FN142\]](#) My conclusion is that the time and frustration costs of opting out are unacceptable burdens on web surfers. Yahoo! collects PII, in addition to information it obtains from its business partners; however, Yahoo! allegedly uses or shares this information only to provide ordered services, unless the information source consents. [\[FN143\]](#) Yahoo! does not divulge whether it collects individual or aggregated non-personally identifiable information, nor does it state how it classifies browser IP addresses.

I began my web journey by linking from Yahoo!'s web page to its privacy home page. (The link is at the very bottom of a long, crowded page). From there, the viewer can link to any of eleven other sites. I linked directly to "third party ad servers." Yahoo! opens the discussion by assuring viewers that "Yahoo! sends to [their] web browsers most of the advertisements [they] see when [they] use the Yahoo! network of web sites." [\[FN144\]](#) A surfer who is not easily reassured may continue down the page and discover that "to prevent a third-party ad server from sending and reading cookies on [her] computer, currently [the viewer] must visit each ad network's web site and individually opt out (if they \*685 offer this capability)." [\[FN145\]](#)

Yahoo!, therefore, both discourages its viewers from pursuing privacy and raises the time cost of obtaining privacy. In September 2000, Yahoo! listed nineteen different third party advertisers. To illustrate the barriers to privacy, the following pages report on some of these nineteen advertisers as viewed from Yahoo!'s links.

1. 24/7 Media: [\[FN146\]](#) The link from Yahoo! lands on a twenty-three-page privacy statement with sufficient notice. [\[FN147\]](#) At the beginning of the statement, the user is proffered direct links to many different sections of the privacy document, including "Opt-Out Policy," where the user may opt out of data collection. [\[FN148\]](#) If you read the entire statement, however, you locate additional links to "interrelated business lines"; [\[FN149\]](#) some of these links offer "more information" and some offer separate privacy policies. [\[FN150\]](#) 24/7 gathers a large amount of

data; the collected "anonymous data" includes computer IP addresses and is sufficient to allow "psycho-graphically" targeted advertising. [\[FN151\]](#) Aggregated anonymous data is shared with advertiser clients. [\[FN152\]](#) PII is used, among other purposes, to "[g]ain a better general understanding of the type of individuals viewing ads and visiting Web sites serviced by 24/7 Media." [\[FN153\]](#) In the future, 24/7 does expect to link PII and "Anonymous Data" for surfers who want super-\*686 targeted advertisements. [\[FN154\]](#)

2. AdForce: [\[FN155\]](#) The link from Yahoo! ends at a relatively concise and understandable privacy statement, opening with an explanation of how advertising enables low-cost content and how data collection enables helpful advertising. [\[FN156\]](#) AdForce reassures the user that it does not collect PII, and lists what non-PII it does collect. [\[FN157\]](#) This includes one item that may be personally identifiable (and is often at least group-identifiable): the "IP address of the machine (browser/proxy) connecting to AdForce." [\[FN158\]](#) At the bottom of the page, AdForce presents an option to opt out of data collection. [\[FN159\]](#) AdForce assures that all opt-out cookies are indistinguishable and even offers a link to instructions explaining how to disengage all cookies on your browser. [\[FN160\]](#)

3. AdMonitor.net: You can't get there from here. Despite repeated efforts, I could not reach AdMonitor.net from Yahoo!'s supplied link, from the go-to function on my browser, or from any of the hits obtained from Yahoo! searches for "AdMonitor" and "AdMonitor.net."

4. AppNet/admaximize/i33: You land on a privacy statement but not a helpful one. The first paragraph (shades of Engage) tells you that the page covers information collected at the "corporate Website." The offered links are "services," "clients," "invest," and "careers"--no hint on how to opt-out of information collected on other sites to whom AppNet serves advertisements. AppNet does supply an e-mail address for persons with questions or comments about the privacy policy. I sent an e-mail regarding their policy on September 4, 2000; I have still received no response.

5. BeFree: [\[FN161\]](#) Yes, you land on a privacy policy, but not one that encourages a belief in self-regulation. [\[FN162\]](#) The policy opens \*687 with a TRUSTe logo and a long paragraph about BeFree following TRUSTe's guidelines, followed by a cliché paragraph about "responsible on-line marketing." [\[FN163\]](#) When you get to the "privacy section," bold print highlights that "BeFree does not track the identify or contact information of end users." However, it "does record IP addresses and it uses cookies to observe the online behavior of anonymous visitors." [\[FN164\]](#) To stop tracking, users "always have the option to refuse cookies." [\[FN165\]](#) But the company fails to provide information on how to do this or give an option to opt-out of just BeFree's cookie. Furthermore, "[a]s BeFree manages affiliate programs for its merchant clients, it is possible that BeFree has access on its servers to personally identifiable information on end users. This information belongs to merchants, and BeFree does not share such information with third parties." [\[FN166\]](#) BeFree never states whether (with BeFree's help) these merchant clients and their affiliates tie PII to the "anonymous" tracking data. Furthermore, BeFree has no control over the information practices of its merchant clients and their affiliates. In other words, BeFree is collecting information about users and letting unnamed, unnumbered "clients and their associates" do whatever they want to do with the information. [\[FN167\]](#)

6. ClickHere: You do not land on a privacy policy. You reach a home page that first blasts you with audiovisual content and, only then, offers you a few links. None of the links take you to any mention of a privacy policy or to a privacy link. I did not bother sending an e-mail.

7. MatchLogic: [\[FN168\]](#) The link from Yahoo! lands on MatchLogic's home page, which has a privacy link. The privacy policy discusses three types of data collection tied to three different services that MatchLogic runs. [\[FN169\]](#) The company sponsors contests to collect PII and may exchange such information with \*688 "selected partners." [\[FN170\]](#) "Selected partners" store their data collections with MatchLogic. In other words, look out; someone may be collecting a large dossier on you. While MatchLogic promises to stop using your PII on request, it does not mention if its "selected partners" will stop. MatchLogic also runs targeted banner advertisements

using cookies to collect non-PII. The customer may opt-out of MatchLogic's cookie, but a visitor must opt-out anytime he changes browsers or resets his cookie file. [\[FN171\]](#) MatchLogic does assure visitors that it keeps its anonymous and PII databases separate.

8. Mediaplex: [\[FN172\]](#) From Yahoo! you reach a three-page privacy policy written in very small print. The company uses cookies but allows opt-out. [\[FN173\]](#) Mediaplex does not collect quite the same data as other banner-advertisement companies because it uses the data its customers collect when targeting advertisements; therefore, the viewer is advised to check the privacy policies of the web sites he visits. [\[FN174\]](#) Mediaplex does not "maintain, share or sell any personally identifiable data or anonymous user profile information." [\[FN175\]](#)

9. Sabela: [\[FN176\]](#) From Yahoo! you land on a two-page privacy policy with readable print. Sabela uses cookies to create an individual, anonymous profile, which it uses to serve targeted advertisements to the visitor as he visits Sabela's customers' Internet sites. [\[FN177\]](#) Sabela promises that it never shares private individual profiles with others--including its clients; rather, Sabela shares only aggregated information. [\[FN178\]](#) The anonymity, however, seems potentially breachable because Sabela changes a user's anonymous profile when it interacts with a client's site \*689 on which that user has changed his information. [\[FN179\]](#)

10. VitaBella: [\[FN180\]](#) Yahoo! links directly to a privacy policy. [\[FN181\]](#) VitaBella uses cookies with "unique id number[s]" to serve targeted advertisements; however, the company does not build or maintain profiles, nor does it aggregate data from multiple clients. [\[FN182\]](#) VitaBella may collect voluntarily provided PII on behalf of clients running promotions, but any PII collected is supposedly kept separate from the anonymous information. [\[FN183\]](#)

11. WebConnect: [\[FN184\]](#) While you do not land on a privacy policy, you are offered a direct link to a "privacy pledge." [\[FN185\]](#) The pledge is totally silent on what WebConnect does when it services banner advertisements. The pledge is totally silent on whether WebConnect collects information or how it handles any information it collects. WebConnect merely "promises

that it encourages" its "Consumer Catalog clients to comply with the DMA Promise Privacy Policy." [\[FN186\]](#) If you follow the "What We Do" link, you discover that WebConnect does collect information: "[W]e target, place and track advertising . . . [with a] . . . proprietary ICS tracking system . . . [in order to] . . . collect[] vital statistics throughout the entire sales process." [\[FN187\]](#) WebConnect claims that its tracking tool, "BrandROI," is the first of its kind. BrandROI allegedly "can capture actual return on investment from Internet advertisements seen, but not clicked on. Advertisers can now track the amount of sales or inquiries that result from the brand effect created via a specific Internet advertisement." [\[FN188\]](#) The company also uses CustomView, an Internet advertisement replacement system, which "allows [the advertising client] to adapt [its] campaigns for individual Internet users and apply a viewer 'frequency cap' to [its] different \*690 Internet advertisements." [\[FN189\]](#)

Has this subsection been tedious? Consider the plight of a surfer who works through all Yahoo!'s third-party advertisers.

In sum, if you want to control your private information, stay off Yahoo! If you want to prevent profiling, stay off Yahoo! Yahoo!, by the way, has a TRUSTe seal covering all of its English language sites. After this trip through Yahoo!'s looking glass, I am not surprised that a majority of U.S. consumers do not trust ecommerce firms sufficiently to want relationships with them. [\[FN190\]](#)

d. Focused Reality Check: Seal Organizations, September, 2000

Some hail the entrance of private seal organizations such as TRUSTe and BBBOnLine Some action is better than no action. Seal-backed privacy polices, however, are inadequate for several reasons: (1) too few entities post them; (2) the seal organizations do not have sufficient reputational clout; (3) the remedies for violations are inadequate; and (4) the seal requirements are too low to satisfy a large portion of the public.

Privacy policies are too rare on the Internet. Yes, they have become more common since the

FTC began publicizing online privacy in 1995. [\[FN191\]](#) The FTC's 2000 survey, however, found that only 20% of randomly sampled sites and 42% in the "most popular group" which collect PII partially implement the four core principles: notice, choice, access, and security. Notice means advising consumers what the company is doing; choice means asking consumers to opt-in or opt-out of information collection; access means allowing consumers to look at the information the company has collected on them and to correct inaccuracies; security means protecting the information \*691 collected from unauthorized third parties. [\[FN192\]](#) A consumer is only 32% likely to land on a site that partially follows these four principles. [\[FN193\]](#) Only 41% of randomly sampled sites and 60% in the "most popular group" met even the FTC's very basic notice and choice hurdles. A consumer has only a 58% percent chance of encountering such a site. [\[FN194\]](#)

These figures are overly cheerful. The FTC counted a site as providing notice if it posted a privacy policy with any information about the data it collects, how it uses that data internally, and whether it shares the data with third parties. [\[FN195\]](#) Although 78% of sites in the "most popular group" allow third parties to place cookies on their sites, only 51% of these sites disclose that fact. [\[FN196\]](#) The FTC did not quantify the absence of the fifth core principle--enforcement of posted policies and redress for harmed individuals. [\[FN197\]](#)

As for sites with privacy policies backed by private seal organizations, the FTC's 2000 survey reported that only about 8% of randomly sampled sites and 45% of the "most popular group" display privacy seals. [\[FN198\]](#) Looking only at the biggest players, BBBOnline, "a subsidiary of the Council of Better Business Bureaus," claims more than 3500 seal holders. [\[FN199\]](#) In January of 2000, TRUSTe announced its 1000th seal. [\[FN200\]](#) TRUSTe's growth has been phenomenal; by late August, 2000, \*692 TRUSTe had almost 2000 seals. [\[FN201\]](#) These numbers, however, are dwarfed by the size of the Internet. An empirical study of the publicly indexable web, performed in February 1999, reported 2.8 million active, publicly accessible server addresses. [\[FN202\]](#) Internet growth already may have dwarfed that figure.

The concept of a privacy policy backed by a seal is that consumers will trust the seal organization, [\[FN203\]](#) even if they do not know the host company. [\[FN204\]](#) There is little indication, however, that consumers feel this way. The small number of seals issued implies the opposite, so does the small number of privacy disputes brought to the seal organizations. [\[FN205\]](#)

**\*693** Nielsen/NetRatings put TRUSTe in the top ten web advertisers both for the month of July, 2000, and for the week ending August 20, 2000. The NetRatings, however, are based solely on the number of "impressions," [\[FN206\]](#) i.e. the number of times one individual has been exposed to one advertisement. [\[FN207\]](#) An advertising "impression" does not necessarily fulfill the dictionary definition of "impression": "a strong effect produced on the intellect, feelings, conscience, etc." [\[FN208\]](#) If each advertising impression produced such a strong mental and emotional impression on exposed humans, then the threat of manipulation by anonymous on-line profiling would swamp any positive benefit produced by the miniature seal programs. [\[FN209\]](#)

**\*694** TRUSTe has publicized the positive results [\[FN210\]](#) of the recently released study "Trust in the Wired Americas" [\[FN211\]](#) by Cheskin Research. [\[FN212\]](#) Although TRUSTe may have reason to celebrate, the study fails to demonstrate that TRUSTe has gained the American public's confidence. [\[FN213\]](#) Ignoring the fact that the sample used is not an accurate representation of the U.S. population, [\[FN214\]](#) the study does not demonstrate confidence in the privacy protection provided by a TRUSTe seal.

The study merely shows that persons seeing the seal may feel less uncomfortable. Cheskin reports that American consumers believe "that there are essentially no rules to the way information is managed and protected across cyberspace," leading to a "heightened sense of risk" for transactions. [\[FN215\]](#) Six factors allegedly may reduce the perception of risk: (1) a strong brand identity; (2) easy navigation on the web site; (3) reliable fulfillment of orders; (4) professional presentation on the web site; (5) up-to-date technology; and (6) seals of approval. [\[FN216\]](#) **\*695** Notice that brands comes first and seals of approval last. [\[FN217\]](#) This is not much help for smaller e-businesses. Study subjects were shown pictures of five seals: Visa, MasterCard,

TRUSTe, VeriSign, [\[FN218\]](#) and BBBOnLine. The subjects were asked if they "had seen" the seals. In the United States, 89% had seen Visa's seal, 69% TRUSTe's, 63% MasterCard's, 59% VeriSign's, and 18% BBBOnLine's. [\[FN219\]](#) Few subjects, however, had read the privacy statements associated with the symbols. [\[FN220\]](#)

Subjects were not asked if seeing one of these symbols made them feel safe-- as to privacy or any other concern. They were asked if posting these symbols increased the trustworthiness of a web site. Here TRUSTe earned 55% in the United States, BBBOnLine 40%, Visa 38%, VeriSign 38%, and MasterCard 27%--a giant improvement for TRUSTe over 1999. [\[FN221\]](#) As for the \*696 "most trustworthy" sites, subjects were not prompted. Picks included over 600 different sites, none of which were mentioned by over 15% of respondents. [\[FN222\]](#) In the United States, the seven most frequently "trusted" were (in descending order): Yahoo!, Amazon, Hotmail/MSN, eBay, AOL, iwon, and Microsoft. [\[FN223\]](#) Again, remember the question asked; "most trusted" is a comparative; the "most trusted" may be perceived as the best of a very bad lot.

How you view the results of the 2000 Cheskin study depends on your goal. If you want to lull consumers into going online to shop at the lowest cost to business, the news that people respond somewhat to familiar symbols, even without knowing the policies the symbols stand for, is good news. If you want to assure privacy, as requested by a supermajority of the United States public, the news means that the market by itself is extremely unlikely to produce an acceptable Internet. Not enough people seem to invest enough time to read the small print. Yahoo!, for example, is the most trusted site in the United States. My tedious investigation of Yahoo!'s third party advertising services, however, shows this trust is somewhat misplaced.

As to remedies, BBBOnLine may order an offender to correct its action. If the offender does not comply, BBBOnLine may cancel the seal, publicize the problem, or refer the offense to a government agency. [\[FN224\]](#) BBBOnLine's own dispute resolution process is unable to direct an offending seal member to pay money damages. [\[FN225\]](#) Similarly, PrivacyBot's and TRUSTe's ultimate sanctions are publicity, seal cancellation, and referral to appropriate government agen-

cies. [\[FN226\]](#) Even the safe harbor \*697 agreement that the United States negotiated with the EU does not require monetary remedies for violations, [\[FN227\]](#) despite the fact that the EU Directive requires member states to enact national legislation to enable individuals to sue for monetary damages. [\[FN228\]](#) The difference is not based on public opinion; the United States public endorses strong penalties. [\[FN229\]](#) As the Internet industry recognizes, government enforcement means less enforcement; the government simply has too few regulators. [\[FN230\]](#)

Seal organizations are insufficient, furthermore, because they do not require enough. Even though the majority of Americans do not know the extent of the information collection routinely performed on-line, [\[FN231\]](#) Americans want better privacy protection than is necessary to qualify for a BBBOOnLine or TRUSTe privacy seal. They also want better privacy policies than that promised by the NAI. Some 87% of Americans want "complete control" of online information collection. [\[FN232\]](#) If Americans knew more about technological capabilities, more Americans might favor strong privacy rights. NAI's privacy policy has been discussed in detail above. Although the specifics are more complex, the essence of both the BBBOOnLine and TRUSTe seal programs is following a posted privacy policy, not keeping out of the information collection business.

\*698 What does the American public want? According to the Pew Internet & American Life Project a vast majority of Americans want a presumption of privacy when they are on-line. [\[FN233\]](#) Opt-in choice is demanded by 86%; 54% consider on-line tracking a harmful invasion of privacy. [\[FN234\]](#) Over 90% of Americans are concerned about privacy, and well over 75% are "seriously concerned." [\[FN235\]](#) DoubleClick, the mammoth on-line advertising firm, sponsored a 1999 study conducted by privacy expert Dr. Alan A. Westin. [\[FN236\]](#) Although survey respondents were not qualified by knowledge about on-line snooping and possible data consolidation, [\[FN237\]](#) "a solid . . . 32 to 49 percent . . . would not be willing to give or have their personal information collected for various types of banner ad personalization." [\[FN238\]](#) Those willing to allow tracking for the purpose of on-line advertisement targeting were strongly con-

cerned that the information not be used for other purposes, not be shared with other entities, and be editable by its subjects. [\[FN239\]](#)

In sum, the seal organizations are some improvement for people who want information about data collection. The seal organization may eventually satisfy the needs of that portion of the population willing to trade information for access. [\[FN240\]](#) The organizations do not, however, provide the private spot desired by at least a substantial minority of Americans. Opt-in Government could provide such a safe spot.

### III. The Example: Opt-In Government to Allow On-Line Privacy

American citizens and the federal government should want more Americans on the Internet, not just to grow ecommerce, but to grow informed citizens. In the words of James Madison, \*699 "knowledge will forever govern ignorance; [[a] popular government without popular information . . . or the means of acquiring it is but a prologue to a farce or tragedy or perhaps both." [\[FN241\]](#) The Internet has already become an important information resource to the vast majority of people with access. [\[FN242\]](#)

Finding even non-commercial information on-line, however, can be hazardous to your privacy. Even if the site you are looking for does not plant cookies or bristle with advertisements that do, you need to find the right site. Most search engines are prime Internet advertising space [\[FN243\]](#) shadowed by multiple third party advertisement vendors--as my investigation of Yahoo! illustrates. To feel safe to look for information, you need to be able to find the site you want without using an advertising-supported search engine. You also need to know that you will not waste your time (or lose your privacy) by inadvertently following a search engine result hyperlink onto a site that contains cookies. [\[FN244\]](#) After you get to a site, you need to know when a hyperlink is leading you off safe territory.

This is a job for "Opt-In Government."

The federal government should establish a private zone on the Internet by setting up a search

engine that will only link to web sites providing the highest level of privacy. Let us dub this site PrivateSearch.gov. [\[FN245\]](#) Only the federal government has a high enough profile to be visible to Internet surfers most at risk: the \*700 nontechnological, rushed Internet users. Only the federal government can provide sufficiently rigorous penalties for privacy violations. [\[FN246\]](#)

Cost is not prohibitive compared to other government projects. List price for an Internet search engine is about (1) \$300,000 a year for indexing the first one million pages; (2) \$100,000 for each additional million pages indexed; and (3) four dollars per 1000 queries run. Substantial volume discounts are usually negotiated. [\[FN247\]](#) In comparison, the Privacy Commission Act would have appropriated \$2,500,000 for a report on privacy, which would merely discuss the problem. [\[FN248\]](#) The Constitution allows exclusive rights to authors and inventors in order to "promote the progress of science and the useful arts" [\[FN249\]](#) by creating material for public use. [\[FN250\]](#) The fees that intellectual property holders pay to the Patent and Trademark Office (PTO), therefore, would be singularly appropriate to partially underwrite public access to information on the Internet. [\[FN251\]](#)

Private foundations might help fund PrivateSearch.gov. The Federal Search Foundation, founded by Dr. Eric Brewer, is building a search engine for the federal government to provide better access to government supplied information. [\[FN252\]](#) Access is \*701 private. [\[FN253\]](#) Access is free not only to citizens, but to independent web entities that promise not to track individual actions on the site. [\[FN254\]](#)

PrivateSearch.gov could operate by searching only those sites registered with the search engine. [\[FN255\]](#) If a company desires its site to be included, the company could file a brief declaration stating that: (1) it did not collect or use any of its visitors' information except to answer inquiries from those visitors or to complete transactions requested by those visitors; (2) it shared such information only with third parties needed to complete the transaction, such as UPS, who used it for no other purpose; (3) the information was discarded after its use; and (4) hyperlinks leading to independent sites are clearly marked. Any violations would be punishable. I suggest

that harmed visitors have private causes of action for injunction, compensatory and statutory damages, [\[FN256\]](#) and attorney's fees. States' attorneys general and the FTC should have the power to sue for criminal penalties. These remedies largely parallel the EC Directive.

The government could charge a modest fee for handling each registration. Yahoo! and other commercial search engines, after all, charge fees to web sites for accelerated or higher quality \*702 indexing. [\[FN257\]](#) Registration would be effective for a stated time, such as one year. If the registration was not renewed, the site would be dropped from PrivateSearch.gov. A site could exit the system at any time by filing a certificate. Filings could be done on-line. [\[FN258\]](#) The government could underwrite indexing certain public service sites, perhaps public libraries, museums, or local government material. A registered site would have the right to state this on its site, thus reassuring persons who reached the site independently of PrivateSearch.gov.

Small businesses would benefit greatly from such a system. No available seal promises consumers such a high level of privacy. No available seal projects as much clout with the public as the trademarks of major businesses. [\[FN259\]](#) Nor are the major seals tied to search engines. Many small businesses may be following high quality privacy practices, but have no affordable way of informing interested potential customers. [\[FN260\]](#)

This government project would not intrude on the unconcerned. Consumers who want to trade content or price for personal information would be free to do so. Companies that want to use cookie-directed advertising would remain free to do so. Persons and companies, however, who want to act on the highest privacy level would also be empowered, unlike non-techies under the current self-regulatory system.

PrivateSearch.gov, furthermore, would provide a way of empirically testing American's feelings about privacy. We would finally be able to vote for privacy with our computer mice.

[\[FN1\]](#). Visiting Associate Professor, Northern Illinois University, College of Law. My thanks for helpful comments on earlier versions to Ann Bartow, David E. Sorkin, and Jonathan Winer.

Any errors are my own. [Editor's note: the following article conforms to The Bluebook: A Uniform System of Citation (16th ed. 1996)].

[FN1]. Thomas Stearns Eliot, *The Hollow Men*, in *Immortal Poems of the English Language* 542 (Oscar Williams, ed., 2d ed. 1960).

[FN2]. For a brief explanation as to how this method could address consumer protection issues, see Malla Pollack, *U.S. Perspectives on Consumer Protection in the Global Electronic Marketplace*, Comment P994312 to the Federal Trade Commission (April 30, 1999), available in <http://www.ftc.gov/bcp/icpw/comments/pollack.htm>.

[FN3]. "Voice" allows individuals to be heard about the conditions of their lives. "Choice" in the market is merely a theoretical option to decline a proffered transaction, i.e., "exit." The market may not offer any "choice" that the "chooser" relishes, even when life requires the chooser to choose something. Furthermore, the market does not operate on the principle of "one person, one vote." Individuals with more discretionary income have a greater impact on available market choices than do individuals with less discretionary income. See generally Elizabeth Anderson, *Value in Ethics and Economics* (1993) (discussing "choice," "voice," "exit," and when each is morally appropriate).

[FN4]. Some opt-in government strategies fulfill both possibilities. Although not part of the main model, sufficiently successful ventures started by government could be privatized later. Privatization, however, creates major issues outside the scope of this article. Consider, for example, the multiple complaints about the insularity of Internet Corporation for Assigned Names and Numbers (ICANN) and its predecessors. See, e.g., A. Michael Froomkin, *Of Governments and Governance*, 14 *Berkeley Tech. L.J.* 617, 623-32 (1999) (discussing the lack of effective democratic checks during World Intellectual Property Organization's (WIPO) trademark/domain name process).

[FN5]. For example, as discussed below, the Federal Trade Commission (FTC) began its invest-

igation into Internet privacy issues with a strong bias toward self-regulation, yet quickly called for child-specific and general legislation because industry response was sluggish, at best. The FTC has also recently reported that the self-regulating motion picture, music recording, and electronic game industries routinely target children under 17 as the audience for movies, music, and games that the industries themselves acknowledge are inappropriate for children. See FTC Release Report on the Marketing Violent Entertainment to Children, available in <http://www.ftc.gov/opa/2000/09/youthviol.htm> [hereinafter FTC Violence]; see also, e.g., Douglas C. Michael, [Federal Agency Use of Audited Self-Regulation as a Regulatory Technique](#), 47 *Admin. L. Rev.* 171 (1995). But see, e.g., Sagi Lizerov, Greenspan's Privacy Solution, *The Industry Standard*, Sept. 4, 2000, at 93 (arguing that higher interest rates and slower returns in net businesses will raise entry barriers and, therefore, increase likelihood of privacy self-regulation).

[FN6]. Unless the context clearly shows otherwise, this paper uses "American" to mean of or pertaining to the United States of America. "United Statesian" is, unfortunately, not yet acceptable for law review publication.

[FN7]. Calvin Coolidge, Speech to Society of American Newspaper Editors, Washington D.C. (Jan. 1925), available at <http://www.sddt.com/features/convention/elections/1924.htm>.

[FN8]. E.g., The White House, A Framework for Global Electronic Commerce <http://www.ecommerce.gov/framework.htm> (visited Oct. 23, 2000). The five principals are:

1. The private sector should lead.
2. Governments should avoid undue restrictions on electronic commerce.
3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.
4. Governments should recognize the unique qualities of the Internet.
5. Electronic Commerce over the Internet should be facilitated on a global basis.

Id. at 1. The 2000 Republican Platform also supported business leadership:

Government also has a responsibility to protect personal privacy, which is the single greatest concern Americans now have about the Information Revolution. Citizens must have the confidence that their personal privacy will be respected in the use of technology by both business and government. That privacy is an essential part of our personal freedom and our family life, and it must not be sacrificed in the name of progress. At the same time, consumers should have the benefit of new products, services, and treatments that result from the legitimate use of data with appropriate safeguards. We applaud the leadership already demonstrated in this regard by many outstanding businesses, which are ensuring individuals' privacy in various ways and promoting public education about the consumer's right to privacy.

The Republican National Committee, *The American Dream: Prosperity with a Purpose* (2000 Platform) <http://www.rnc.org/2000/2000platform2> (visited Oct. 23, 2000). The 2000 Democratic Platform supported on-line privacy, but did not, at that exact spot, repeat the mantra of business leadership:

While fighting to expand Internet access, [Al Gore] has led the Administration's efforts to give parents, schools, and communities effective tools to protect children from inappropriate content on-line. In particular, Al Gore has focused on the challenge of protecting Americans' personal privacy on-line as well as the medical and financial information that can all too easily be intercepted and abused by others.

Al Gore has called for an Electronic Bill of Rights for this electronic age-including the right to choose whether personal information is disclosed; the right to know how, when, and how much of that information is being used; the right to see it yourself; and the right to know if is accurate.

Democratic National Committee, *Prosperity, Progress, and Peace* [http:// www.democrats. org/hq/resources/platform/index.html](http://www.democrats.org/hq/resources/platform/index.html) (visited Sept. 1, 2000).

[FN9]. See, e.g., Robert B. Reich, *The Work of Nations* 8-9 ("Neither the profitability of a nation's corporations nor the successes of its investors necessarily improve the standard of living of most of a nation's citizens.... The underlying question concerns the future of American society as

distinct from the American economy.").

[FN10]. The FTC accepts the basic principles of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. See OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. <http://www.oecd.fr/dsti/sti/it/secur/act/prod/pnv-en.htm> (visited Oct. 13, 2000). These principles are notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress. See FTC, Privacy Online: A Report to Congress, at 7-11 (June 1998), available at <http://www.ftc.gov/privacy/index.html> [hereinafter FTC, Privacy].

[FN11]. Modern international business practices undermine the concept of "American" commerce. See, e.g., Reich, *supra* note 9, at 119-70 (explaining that businesses no longer substantively support their nominal countries of citizenship); see also, e.g., U.S. Dep't. of Commerce, Digital Economy 2000, at vii (June 2000), available at <http://www.doc.gov/ecommerce>.

Paradoxically, although America's IT [information technology] producing companies are world-class, the United States regularly runs large trade deficits in IT goods--an estimated \$66 billion in 1999. One reason is that American IT firms more often service foreign customers with sales from their overseas affiliates than by exports from their U.S. operations.

Id.

[FN12]. See FTC, Working for Consumer Protection and a Competitive Marketplace <http://www.ftc.gov> (visited Oct. 13, 2000) (displaying the slogan and links to FTC materials); see also FTC, Vision, Mission and Goals <http://www/ftc.gov/ftc/misssion.htm> (visited Oct. 14, 2000) ("The Commission seeks to ensure that the nation's markets function competitively, and are vigorous, efficient, and free of undue restrictions. The Commission also works to enhance the smooth operation of the marketplace by eliminating acts or practices that are unfair or deceptive.").

[FN13]. "BtoC ecommerce" means business to consumer electronic commerce.

[FN14]. See e.g., FTC, Privacy, supra note 10, at ii (indicating that the FTC's privacy efforts "have been based on the belief that greater protection of personal privacy on the Internet will not only protect consumers, but also increase consumer confidence and ultimately their participation in the online marketplace"). The European Union is also concerned about consumer perceptions that deter BtoC ecommerce. See, e.g., Commissioner David Byrne, Address at the Launch of the 360atlantic Project for Health and Consumer Protection (Sept. 25, 2000), available at [http://europa.eu.int/comm/dgs/health\\_consumer/library/speeches/speech56\\_en.html](http://europa.eu.int/comm/dgs/health_consumer/library/speeches/speech56_en.html) (addressing the "confidence gap" by encouraging "best market protections," creating alternative dispute resolution procedures, and setting jurisdiction in the consumer's home court system).

[FN15]. See FTC, Privacy, supra note 10, at 2.

[FN16]. See id. at 42 ("In the specific area of children's online privacy ... the Commission now recommends that Congress develop legislation placing parents in control of the online collection and use of personal information from their children."). Congress responded with the Children's Online Privacy Protection Act of 1998. [15 U.S.C. §§ 6501-6506 \(West, Supp. 2000\)](#) [hereinafter COPPA]. The FTC then requested comments on the suitability of TRUSTe's children's privacy seal as a safe harbor under COPPA. See, e.g., FTC, Requests Public Comments on TRUSTe Application for COPPA Safe Harbor Status, 5 Electronic Com. & L. (BNA), No. 35, at 916 (Sept. 13, 2000). Recent American privacy legislation includes the Gramm-Leach-Bliley Act, which covers, among other things, consumers' financial information. See Pub. Law. No. 106-102, 113 Stat. 1338, 1340 (1999). The FTC has requested comments on regulations to effectuate this act. See, e.g., FTC, in Preliminary Action Seeks Comment on Privacy Safeguards for Forthcoming Rule, 5 Electronic Com. & L. (BNA), No. 35, at 914 (Sept. 13, 2000).

[FN17]. See FTC, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress, at 36-38, available at <http://www.ftc.gov/privacy/index.html> [hereinafter FTC, Privacy II]. Besides personally identifiable information, the FTC also has investigated online profiling. See Dept. of Com. & FTC, Public Workshop on Online Profiling (Nov. 8, 1999),

available at <http://www.ftc.gov/privacy/index.htm> [hereinafter Profiling Workshop]; see also FTC, Online Profiling: A Federal Trade Commission Report to Congress, Part 2, available at <http://www.ftc.gov/privacy/index.html> [hereinafter Online Profiling Part 2]; FTC, Online Profiling: A Federal Trade Commission Report to Congress, Part 1, available at <http://www.ftc.gov/privacy/index.html> [hereinafter Online Profiling Part 1]; Prepared Statement of the FTC On "Online Profiling: Benefits and Concerns" Before the Senate Comm. on Com., Sci. and Transp., 106th Cong. (2000) (prepared statement of Jodie Bernstein, Director of the Bureau of Consumer Protection of the Federal Trade Commission), available at <http://www.ftc.gov/privacy/index.html> [hereinafter Benefits/Concerns]; Statement of Commissioner Orson Swindle Concurring in Part and Dissenting in Part to Prepared Statement of the FTC On Online Profiling: Benefits and Concerns Before the Senate Comm. on Com., Sci. and Transp., 106th Cong. (2000), available at <http://www.ftc.gov/privacy/index.html> [hereinafter Swindle on Profiling].

[FN18]. See FTC, Privacy II, *supra* note 17, at 37.

[FN19]. See Dissenting Statement of Commissioner Orson Swindle in Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress, at 4-5 (May 2000), available at <http://www.ftc.gov/05/2000/05/index.htm> [hereinafter Swindle Statement].

[FN20]. See Online Profiling Part 2, *supra* note 17, at 4 (discussing the National Advertising Initiative and pending federal legislation).

[FN21]. See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 On the Protection of Individuals with Regard to the Processing of Personal Data and On the Free Movement of Such Data, 1995 O.J. (L281) 31, available at [http://europa.eu.int/eur-lex/en/lif/date/1995/en\\_395L0046.html](http://europa.eu.int/eur-lex/en/lif/date/1995/en_395L0046.html) [hereinafter EC Directive].

[FN22]. See *id.*, arts. 22-24.

[FN23]. See *id.*, art. 28.

[FN24]. See *id.*, arts. 25, 26.

[FN25]. See, e.g., [Industries Clamor for Privacy ' Safe Harbor'. Ins. Regulator, Nov. 30, 1998, available at 1998 WL 5050155](#) ("Several financial trade associations ... are pressuring the task force on electronic commerce at the Department of Commerce to clarify and provide assurances that U.S. companies fall within the safe harbors for the European Union data privacy directive.").

[FN26]. See Dep't of Commerce, International Trade Administration, Electronic Commerce Task Force <http://www.ita.doc.gov/td/ecom/menu.html> (visited Oct. 22, 2000) (providing negotiation documents in reverse chronological order from November 1998 through July 21, 2000).

[FN27]. See [Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 \(July 24, 2000\)](#) (providing full text and explanatory material); [Issuance of Safe Harbor Principles and Transmission to European Commission; Procedures and Start Date for Safe Harbor List, 65 Fed. Reg. 56,534 \(Sept. 19, 2000\)](#) (containing corrections to final documents published in [65 Fed. Reg. 45,666](#)).

[FN28]. See Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the U.S. Department of Commerce [http://www.ita.doc.gov/td/ecom/Decision\\_SECGEN-EN.htm](http://www.ita.doc.gov/td/ecom/Decision_SECGEN-EN.htm) (visited Oct. 21, 2000) (finding safe harbor to provide "adequate protection" as required by EC Directive).

[FN29]. Because data protection is among "the fundamental rights and freedoms of natural persons, and in particular their right to privacy," the EU may eventually posit that the Directive covers all citizens or habitual residents of EU member countries. European Parliament and Council Directive 95/46/EC, ch.1, art. 1, 1995 O.J. (L 281) 31-50, available at [http://eurpoa.eu.int/eur-lex/en/lif/dat/1995/en\\_395L0046.html](http://eurpoa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html)>. The safe harbor principles do refer to

"human resources personal information transferred from the EU for use in the context of an employment relationship." Dep't of Com., Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000, available at <http://www.ita.doc.gov/td/ecom/SHPRINCIPLESFINAL.htm>> [hereinafter Safe Harbor Privacy Principles].

[FN30]. See FTC, Self-Regulation and Privacy Online: A Report to Congress at 6 (July 1999) [hereinafter FTC, Privacy III] ("[S]elf-regulation is the least intrusive and most efficient means to enforce fair information practices, given the rapidly evolving nature of the Internet and computer technology.").

[FN31]. The Clipper Chip was partially such an attempt. See generally A. Michael Froomkin, [It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow,"](#) 1996 U. Chi. Legal F. 15 (discussing federal government's attempt to make the relatively insecure Clipper Chip into an encryption standard); A. Michael Froomkin, [The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution,](#) 143 U. Pa. L. Rev. 709 (1995) (same).

[FN32]. This article will not discuss the obvious points that (i) government has regulated broadcast television and radio, and (ii) dish, cable, and other pay-per-view services may be overpowering the broadcasters.

[FN33]. For example, The New York Times will be happy to give you free on-line access to recent news if, and only if, you share demographic information and do not object to inhabiting a space shared with banner advertisements. You only need to provide your demographic information once because the site remembers you. See The New York Times <http://www.nytimes.com> (visited Aug. 26, 2000). Some information is less costly. Information Please, for example, will let you search for information without answering any personal questions. Its privacy policy says that it is not collecting or selling personal information, but the privacy policy says nothing about who runs the banner advertisements. See Information Please ht-

[tp://www.infoplease.com/privacy.html](http://www.infoplease.com/privacy.html) (visited Aug. 26, 2000). Several firms are willing to provide free dial-up Internet service in order to market advertisements. See David Lake, *It's Not Easy Being Free*, *The Industry Standard*, Sept. 4, 2000, at 127 (providing statistics). Some wonderful sites are completely free. I managed to write an article on the then-pending Collection of Information Anti-Privacy Act before I knew if the bill would pass because of Congress's Internet site <http://www.thomas.loc.gov>. See Malla Pollack, *The [Right to Know?: Delimiting Database Protection at the Juncture of the Commerce Clause, the Intellectual Property Clause, and the First Amendment](#)*, 17 *Cardozo Arts & Ent. L.J.* 47 (1999). In addition to government-run services, which have recently been ordered to stop hidden information retrieval, see OMB, *Privacy Policies and Data Collection on Federal Web Sites* (June 22, 2000), available at <http://www.whitehouse.gov>, one can visit, for example, the San Francisco Fine Art Museum on the Internet. No questions are asked, and no banner advertisements appear. There is also no posted privacy policy. See Fine Art Museums of San Francisco <http://www.famsf.org> (visited Sept. 8, 2000). Some sites may use cookies inadvertently because some Microsoft server products turn on cookie technology by default. See Declan McCullagh, *Fed's Hands Caught in the Cookie Jar Violating White House Order*, *Wired News*, June 20, 2000, at 3. Advertising alone, furthermore, has proven unable to support many on-line content suppliers. See, e.g., Hane C. Lee, *Can Syndication Save Content?*, *The Industry Standard*, Sept. 4, 2000, at 85 ("Last spring's market plunge made it painfully clear to content companies that ad dollars alone cannot sustain a business.").

[FN34]. See, e.g., John Stuart Mill, *On Liberty* 9 (1978) (stating that the basic principle of government is "[t]hat the only purpose for which power can be exercised over any member of a civilized community against his will, is to prevent harm to others"). This argument overlooks the possibility that selling information, like selling votes, may have societal harm. Removing individually targeted advertising, furthermore, does not eliminate advertising. Additionally, one can target advertising without trailing consumers, by considering the host site's content or by paying persons to be "tracked" on-line. E.g., Joshua Hallford, *Web Ratings: Heavy Traffic Ahead*, *The*

Industry Standard, Sept. 25, 2000, at 104 (discussing several web-rating firms that compensate individuals for providing information about their browsing behavior); see also, e.g., Julie E. Cohen, [Examined Lives: Informational Privacy and the Subject as Object](#), 52 *Stan. L. Rev.* 1373, 1374-77 (2000) (arguing that rhetoric of individual freedom masks commercial interests, which desire to treat persons as objects).

[FN35]. See, e.g., Seth F. Kreimer, [Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law](#), 140 *U. Pa. L. Rev.* 1, 6-7 (1991) (stating that First Amendment theory assumes that sharing more information is preferable); The Europeans Take a Hard Line on Data Privacy, *Credit Card News*, Apr. 1996, available at [1996 WL 8385684](#) ("Americans are unnerved by the concept of a national data protection agency ... it would be like setting Big Brother to watch Big Brother .... [S]tudies show that in the U.S., there is a direct correlation between the public's distrust of government and fears about the abuse of confidential information.") (internal quotation marks omitted).

[FN36]. Some state constitutions do include a right to privacy, including Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington. Some of these provisions may create recourse against non-governmental entities. Cf. [Damages for Breaches of Privacy](#), 65 *Fed. Reg.* 45679 (July 19, 2000).

[FN37]. See, e.g., Bernard Bailyn, *The Ideological Origins of the American Revolution* 47-48, 51 (1992) (indicating that American colonials were strongly influenced by the English radicals who "maintain[ed a] vigil against government" showing "extreme solicitude for the individual and an equal hostility to government").

[FN38]. Most constitutional limitations are only applicable to "state action." E.g., [San Francisco Arts & Athletics, Inc. v. United States Olympic Comm.](#), 483 *U.S.* 522, 543-48 (1987) (refusing to reach the USOC's allegedly discriminatory choice of licensees on the ground that the USOC is not a government actor). If a non-governmental entity is watching, it may be willing to sell the

information to the government or even to share the information for free for the sake of governmental goodwill. Regardless of the collector's attitude, if the information exists, the government presumably can order it to be produced under a proper showing.

[FN39]. See Cheskin Research, *Trust in the Wired Americas* 13 (2000), available at <http://www.cheskin.com/think/studies/trust2.html> (using an 11 point scale when 0 means strong disagreement and 10 means strong agreement, and indicating that the government's ability to monitor received a 7.3 and actual monitoring received a 5.9) (page numbers reference the word document of the study available at this URL) [hereinafter Cheskin Research].

[FN40]. See, e.g., Fourth Amendment, 'Sham' Outside Review Concerns Dog FBI's Carnivore E-Mail Snooper, 5 *Electronic Com. & L.* (BNA), No. 35, at 912 (Sept. 13, 2000); see also McCullagh, *supra* note 33 (reporting that federal agencies are not complying with White House order not to use cookies on their websites).

[FN41]. See U.S. GAO, *Internet Privacy: Comparison of Federal Agency Practices with FTC's Fair Information Principles* (Sept. 11, 2000) (on file with the Catholic University Law Review). The Clinton administration termed the GAO's document "seriously misleading." Most Federal Web Sites Fail on Privacy Standards, Report Says, *N.Y. Times*, Sept. 17, 2000, available at [http://www.nytimes.com/2000/09/17/technology/17\\_priv.html](http://www.nytimes.com/2000/09/17/technology/17_priv.html).

[FN42]. See, e.g., William Funk, [Bargaining Toward the New Millennium: Regulatory Negotiation and the Subversion of the Public Interest](#), 46 *Duke L.J.* 1351, 1356 (1997) (arguing that contemporary negotiated rule making subverts agency goal of protecting public interest); Bradford C. Mank, [Superfund Contractors and Regulatory Capture](#), 2 *N.Y.U. Env't'l L.J.* 34, 34 (1993) (arguing that behavior of contractors hired to clean up superfund sites demonstrates agency capture). But see, e.g., Steven P. Croley, [Theories of Regulation Incorporating the Administrative Process](#), 98 *Colum. L. Rev.* 1, 142-46 (1998) (arguing that processes used in agency rule making and adjudication are not well suited to rent seeking by private interests).

[FN43]. See [Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 842-44 \(1984\)](#) (requiring judicial deference to an agency's construction of a statute enforced by that agency). As for trusting the FTC, specifically, while that agency has done some excellent work, it also decided that the cartoon cigarette spokesanimal Joe Camel was not targeting children, despite persuasive evidence otherwise. See FTC News, June 7, 1994, at 1 (announcing no action decision); see generally, e.g., JAMA, Dec. 11, 1999 (reporting several research studies showing strong reaction of children to Joe Camel advertisements). Note that the 1998 Tobacco Settlement includes a commitment for cigarette companies to stop using non-human cartoon characters in advertisements as of May 22, 1999. See Joy Johnson Wilson (National Conference of State Legislators, Director, AFI Health Committee), Summary of the Attorneys General Master Tobacco Settlement Agreement (March 1999), available at <http://www.udayton.edu/~health/syllabi/tobacco/summary.htm> (visited Sept. 13, 2000). The FTC, furthermore, only recently issued its first corrective advertising order in an adjudicated case since 1975. See [69 U.S.L.W. \(BNA\) 1140 \(Sept. 12, 2000\)](#).

[FN44]. In this section, "current" means through the end of the 106th Congress.

[FN45]. [15 U.S.C. §§ 6501-6506 \(West Supp. 2000\)](#). But see [ACLU v. Reno, 217 F.3d 162 \(3rd Cir. 1999\)](#) (affirming preliminary injunction against enforcement of COPPA).

[FN46]. Publ. Law. 106-102, 113 Stat. 1337, Title V (Privacy) (enacted Nov. 12, 1999). The Gramm-Leach-Bliley Act covers consumers' financial information. See *id.*

[FN47]. S. 2606, 106th Cong. §2 (2000).

[FN48]. See 146 Cong. Rec. S4299, S4301 (daily ed. May 23, 2000) (remarks of Senator Hollings).

[FN49]. See Bill Summary & Status for the 106th Congress for S. 2606, available at <http://www.thomas.loc.gov>. The Committee and the FTC cooperated in hearings on Internet pri-

vacancy and on-line profiling. See press announcements and hearing reports for June 13, 2000 and hearings dated May 25, 2000 at the Committee's website. See <http://www.senate.gov/commerce>. One day of hearings was held on S. 2606 on October 3, 2000. The Committee's web site contains some of the testimony. Because the Senate seemingly orchestrated the bill in conjunction with the FTC, the FTC's July 2000 acceptance of new advertising self-regulation principles might have herald the bill's untimely death even though a majority of FTC commissioners still officially supported legislation to fill self-regulation's gaps. See *infra* notes 97-99 and accompanying text (discussing NAI self-regulation); see also *OnLine Profiling Part 2*, *supra* note 17, at 6.

[\[FN50\]](#). S. 2606, at2 (1), (2). A purist might quibble that subsection (1) may imply that a "fundamental right" can be limited to the "appropriate legislation" that manages to get through a pro-business Congress. Additionally, the purist may argue that a fundamental right to privacy should not be limited to the commercial field specified in subsection (2). By the way, does "personal information" include allegedly "anonymous" profiles either kept separate for each browser address or aggregated? Perhaps Congress's drafting experts are frightened by the Supreme Court's recent willingness to strike legislation as beyond Congress's commerce clause power. See [United States v. Morrison, 120 S. Ct. 1740 \(2000\)](#) (finding Violence Against Women Act is void as beyond Congress' Commerce Clause Power); [Seminole Tribe of Florida v. Florida, 517 U.S. 44 \(1996\)](#) (abrogating state sovereign immunity in Indian Gaming Regulation Act is beyond Congress's Commerce Clause Power); [United States v. Lopez, 514 U.S. 549 \(1995\)](#) (enacting Gun-Free School Zone Act is beyond Congress's Commerce Clause power). Perhaps Congress is taking a trick from the framers of the Constitution and writing about positive powers largely to limit those powers. See William W. Crosskey, *Politics and the Constitution in the History of the United States* 486-87 (1953). I would argue that the Internet is an inherently interstate system on which the surfer is performing interstate movement; therefore, the commerce clause should allow federal statutes regulating all web sites.

[FN51]. Id. at 102, 103.

[FN52]. Id. at 102(g), 103(c).

[FN53]. Id. at 601.

[FN54]. Id. at 301-305. Consumers would also retain certain state law remedies. See id. at 306.

[FN55]. I would prefer the much broader term "profiling," or even the slightly broader term "locating" or identifying" in place of the chosen term "contacting."

[FN56]. Id. at 901(6).

[FN57]. See Joel R. Reidenberg & Paul M. Schwartz, Data Protection Law and Online Services: Regulatory Responses, at 23 & n. 89, available at [http://europa.eu.int/comm/internal\\_market/en/media/dataprot/studies/regul.pdf](http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/regul.pdf).

[FN58]. See id. at 23 & n.88.

[FN59]. See id. at 23.

[FN60]. See Statements on Introduced Bills and Joint Resolutions (Senate, May 23, 2000) (remarks of Mr. Hollings introducing S 2606) (asserting that most service providers track their customers, AOL being the main exception), available at <http://www.thomas.gov> (query for Congressional Record pages related to S 2606). AOL, however, does not deserve a presumption of full consumer trust. The click-through contract one accepts when becoming an AOL member is constructed not to be printable for future reference. See e-mail from Alma, AOL Support Employee, to AOL member (Sept. 15, 2000) (on file with Catholic University Law Review) ("I would like to apologize but the agreement is an integral part of the AOL software installation and cannot be printed."). AOL and Netscape, an AOL subsidiary, have been sued for including in SmartDownload (an appliance that downloads computer software from the Internet) a function that reports downloads back to Netscape/AOL. See Amended Class Action Complaint, Specht et

al. v. Netscape Comm. Corp., et al., No. 00 Civ. 4871 (AKH) (S.D.N.Y. 2000) (on file with Catholic University Law Review).

[FN61]. See Reidenberg & Schwartz, *supra* note 57, at 23-43.

[FN62]. See *id.* at 24-28.

[FN63]. See *id.* at 28-35.

[FN64]. See *id.* at 35-40.

[FN65]. See *id.* at 41-43.

[FN66]. 24/7 Media Privacy <http://www.247media.com/privacy.html> (visited Sept. 8, 2000).

[FN67]. It also only reaches sites within Congress's power to regulate under the Commerce Clause. See *id.* at 901(1).

[FN68]. The Act does, however, include government promotion of privacy enhancing computer agents such as P3P. See *infra* note 106 and accompanying text; see also S. 2606, 106th Cong. § 707 (2000) (indicating that the National Institute of Standards and Technology shall "encourage and support the development of [software for Internet access for expressing user's privacy preferences that] automatically execute the program, once activated, without requiring user intervention"). As of Labor Day 2000, several other bills relating to on-line privacy were also sitting in congressional committees. None are as sweeping as the Privacy Act. Considering these bills in chronological order of their introduction, their major on-line thrusts are as follows:

The Online Privacy Protection Act of 1999 requires the FTC to promulgate regulations concerning personally identifiable information collected on line from persons above the age of 13 and to approve industry created programs as "safe harbors." The Children's Online Privacy Protection Act does not protect persons over thirteen. See 15 U.S.C. 6501. Only the FTC and state attorneys general have standing to sue. The Bill does not expressly define IP addresses as PII, but the FTC has some regulatory power over the definition of PII. S. 809,

106th Cong. § 8(8) (1999).

The Electronic Rights for the 21st Century Act provides standards for government access to stored electronic information and lessens government control of strong encryption. S. 854, 106th Cong. § 102 (1999).

The Internet Consumer Information Protection Act requires that web surfers be given notice of information collection, a chance to opt-out of the collection of this data, and the ability to correct personally identifiable data. H.R. 2882, 106th Cong. §§ 1, 2, 5 (1999). The FTC may issue cease and desist orders, and individuals may sue in a civil action for appropriate relief. PII is defined by reference to [47 U.S.C. § 551](#), which merely excludes "any record of aggregate data which does not identify particular persons." [47 U.S.C. §551\(2\)\(A\) \(2001\)](#) (referenced by H.R. 2882 5(3)).

The Online Privacy Protection Act of 2000 is substantively similar to the Online Privacy Act of 1999, described above, including its definition of PII. H.R. 3560, 106th Cong. § 8(8) (2000).

The Privacy Policy Enforcement in Bankruptcy Act of 2000 removes from a debtor's assets any personally identifiable information whose sale would violate the debtor's privacy. The list of PII does not mention computer IP addresses, but does include an expandable provision. S. 2857 Sec. 2(6)(H), 106th Cong. § 2(6)(H) (2000) ("[A]ny other identifier that permits the physical or electronic contacting of a specific individual."). I would prefer the much broader "profiling," or even the slightly boarder "locating" or "identifying" to the chosen "contacting."

The Consumer Internet Privacy Enhancement Act requires detailed, accurate notices of on-line collection of personally identifiable information. The FTC is to approve private seal programs as safe harbors. Only the FTC and state attorneys general have standing to sue. The FTC is to commission a study on privacy by the National Research Council. The definition of PII does not include IP addresses, but it does include "unique identifying information that an Internet service provider or operator of a commercial web site collects and combines with

any information" earlier defined as PII. S. 2928 Sec. 6(5)(F), 106th Cong. § 6(5)(F) (2000).

Only one of these privacy bills was ordered reported out of committee by the end of the 106th Congress, the Privacy Commission Act. H.R. 4049, 106th Cong. (2000). This bill toothlessly creates the Commission for the Comprehensive Study of Privacy Protection and orders the Commission to hold hearings and make a report. Id. § 3 (2000). If this is the sum total of action congressional committees are willing to send to the floor, one can only conclude that tight top-down privacy regulation currently is unlikely in the United States.

My search, furthermore, probably missed relevant material. On September 2, 2000, a search on Thomas (Congress's online database) for pending bills that included the word "privacy" produced 50 hits. See Thomas (visited Sept. 2, 2000) <http://thomas.loc.gov>. Thomas, however, is incapable of displaying over 50 hits. To confirm this limit, I ran a search for all bills including the word "act"; Thomas retrieved only 50 hits. Id. (visited Sept. 25, 2000). My thanks to Jonathan Winer for mentioning this problem with Thomas.

[FN69]. See infra text accompanying notes 73-75.

[FN70]. See Peter Swire, Of [Elephants, Mice, and Privacy: International Choice of Law and the Internet](#), 32 Int'l Law. 991 (1999), available at <http://www.acs.ohio-state.edu/units/law/swire1/elephants.htm> &gt;.

[FN71]. A strong brand name is the biggest boost to Internet consumer confidence. See Cheskin Research, supra note 39, at 7. FTC Commissioner Orson Swindle, on the other hand, argues that government on-line privacy regulations would force small businesses off the Internet and act as artificial barriers to the entry of other small businesses into ecommerce. See FTC, Privacy 5/00, at 24. My suggestion for opt-in government does not have these alleged drawbacks of standard top-down regulation. The percentage of small businesses that sold over the Internet dropped from 29% in 1998 to 26% in 1999; revenues from on-line sales dropped from 12% to 8% of total sales. See Dun & Bradstreet, Small Businesses Skeptical of Internet Impact, NUA Internet Surveys, available at [http://www.nua.net/surveys/?f'vs&art\\_id' 005344816&rel'true](http://www.nua.net/surveys/?f'vs&art_id' 005344816&rel'true).

[FN72]. The 2000 Platform of the Republican Party was enthusiastic about small business:

Small businesses are the underlying essence of our economy. Small businesses create most of the new jobs and keep this country a land of opportunity. They have been the primary engines of economic advance by American women, whose dynamic entry into small business in recent years has accounted for much of the nation's growth. Small businesses generate more than half of the gross domestic product. Their willingness to give people a chance, and their ability to train individuals new to the work force, made welfare reform the success that it is. They deserve far better treatment from government than they have received. We will provide it through many of the initiatives explained elsewhere in this platform: lower tax rates, ending the death tax, cutting through red tape, legal and product liability reform, and the aggressive expansion of overseas markets for their goods and services.

Republican National Committee, *supra* note 8, available at [http:// www.rnc.org/2000/2000 platform2](http://www.rnc.org/2000/2000platform2). The Democratic Platform also took an enthusiastic approach:

Strengthening small business is a vital component of economic innovation, job creation, and supporting entrepreneurship. Small businesses have accounted for more than 90 percent of the 22 million new jobs created with Democratic leadership. The Democratic Party is committed to sustaining and adding to that level of growth of small businesses, including home based businesses. Democrats believe that strengthening small businesses is a vital component of strategies to create opportunity and community economic development. We will build on the tremendous progress of the Clinton-Gore Administration in modernizing the Small Business Administration and improving access to the Federal marketplace. We will fight to reform and strengthen programs to combat discrimination against women and minority entrepreneurs, including federal procurement, because the playing field is still not level.

Democratic National Committee, *supra* note 8, available at [http:// www.democrats.org/hq/ resources/platform/index.html](http://www.democrats.org/hq/resources/platform/index.html). Al Gore is continuing the pro-small business rhetoric:

In the private sector, Democrats believe in supporting the startups, the small businesses, and the entrepreneurs that are making the New Economy go. This means making permanent the

Research and Experimentation tax credit and expanding it to make it partially refundable so that small businesses can use it more easily. It also means keeping cyberspace a duty-free zone so that American companies can sell goods around the world and insist that other countries refrain from actions that impede commerce. To expand technology's worldwide potential as a force for good, Al Gore has advanced a bold vision for a new Global Information Infrastructure—a network of networks that sends messages and images at the speed of light, across every continent—to expand access to phone service and communications, further improve the delivery of education and health care, and create new jobs and industries.

Id. Using niche-marketing techniques, some small businesses have obtained some help from Internet connections. See Leslie Kaufman, *The Opposite of Amazon.com*, N.Y. Times, Sept. 22, 2000, available at <http://www.nytimes.com/2000/09/22/technology/22smal.html>.

[FN73]. See Susannah Fox et. al., *Trust and Privacy Online: Why Americans Want to Rewrite the Rules 10* (Released by the Pew Internet & American Life Project, Aug. 20, 2000), available at <http://www.pewInternet.org> (only 24% of American Internet users reported having given incorrect personal information to a web site). But see Profiling Workshop, *supra* note 17, at 22, 68 ("[M]any studies show that upwards of 70 % of the information that's disclosed is either deliberately or accidentally misleading or inaccurate," remarks of Daniel Jaye, Chief Technology Officer, Engage Technologies, Inc., Internet advertising agency).

[FN74]. Online Profiling Part 1, *supra* note 17, at 2-4.

[FN75]. See *id.* at 2-8; see also Jeff Sovern, [Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information](#), 74 *Wash. L. Rev.* 1033, 1033-45 (1999) (providing some specifics on extent of information collection and compilation); Privacy.net, The Consumer Information Organization From Consumer.net <http://www.privacy.net> (visited Oct. 12, 2000) (providing multiple negative stories). Once an information collection exists, controlling its dissemination raises additional problems. For example, schools generally have logs of web sites accessed from their computers' records, which might provide information about the browsing beha-

violation of specific children. Such logs have been shared with businesses as a type of payment for supplying free Internet hardware and software and with at least one public advocacy group that wished to argue that school filtering software over-limited students' computer use. A New Hampshire parent is currently suing for access to logs from schools without filtering software in order to pressure for the software's installation. See Carl S. Kaplan, *Suit Considers Computer Files*, N.Y. Times, Sept. 28, 2000, available at <http://www.nytimes.com/2000/09/28/technology/29cyberlaw.html>.

[FN76]. "A recent study showed that more than a third of all Fortune 500 companies check medical records before they hire or promote." The White House, *Remarks by the President on Medical Privacy*, <http://www.whitehouse.gov/wh/new/html/1999/1029.html> (visited Oct. 9, 2000). Another recent study showed major and pervasive problems with the content and accuracy of health insurance web sites' privacy policies. See California HealthCare Foundation, *Health Insurance (information collected Feb. through May 2000)*, [Chttp://www.ehealth.chef.org/ind\\_study10/index\\_show.cfm?doc\\_id'162](http://www.ehealth.chef.org/ind_study10/index_show.cfm?doc_id'162) (visited Oct. 13, 2000).

[FN77]. See Lawrence Lessig, *Code and Other Laws of Cyberspace* 152 (1999) (discussing a man who was recorded on a video camera leaving hotel room with an attractive, much younger woman--his daughter).

[FN78]. See *id.* at 152 (arguing that monitoring and recording of behavior collapses borders between normative communities). The Navy, for example, ordered the separation of Senior Chief Petty Officer Timothy R. McVeigh after 17 years of exemplary service, because his AOL file mentioned homosexuality; the Navy board heard no evidence of homosexual words or behavior in any other venue. See [McVeigh v. Cohen, 983 F. Supp. 215 \(D.D.C. 1998\)](#) (enjoining preliminarily the separation because the AOL disclosure was likely to be held a violation of the Electronic Communications Privacy Act). The Navy later settled with McVeigh; he retired early and received \$90,000 to cover legal fees. See *Outed Retired Sailor Says He Is Gay*, *United Press Int'l*, Oct. 2, 1998.

[FN79]. See Pew Internet & American Life Project, Trust and Privacy Online: Why Americans Want To Rewrite the Rules, available at <http://www.pewInternet.org> (reporting that 27% of Internet users consider tracking-allowed advertisements helpful) [hereinafter Pew Project].

[FN80]. Yes, if you are looking for a common fungible item, you may find a store outside the informed group. The need to do so, however, greatly raises search costs. Further, the only available low-priced merchant may lack other desirable attributes, such as a good return policy. Amazon.com recently backed off a test of "dynamic pricing," charging different customers different non-negotiable prices for the same goods; Amazon.com claimed that it had not based the price differences on demographics--despite the rumors to the contrary. See Infoworld.com, [http://www.infoworld.com/articles/hn/xml/00/09/28/000928\\_hnamazondvd.xml](http://www.infoworld.com/articles/hn/xml/00/09/28/000928_hnamazondvd.xml) (visited Oct. 2, 2000).

[FN81]. Businesses already exist to sell demographically organized voter information to candidates. See, e.g., Leslie Wayne, One Consulting Firm Finds Voter Data Is A Hot Property, N.Y. Times, Sept. 9, 2000, available at <http://www.nytimes.com/2000/09/09/technology/09priv.html>. Aristotle International combines voting list information with commercially available databases. The company's services include targeted Internet advertisements. George W. Bush allegedly used the service. Although Al Gore's campaign refused to do so on privacy grounds, Gore's running mate Joseph I. Lieberman is allegedly an AI customer. See *id.* Political advertising in the United States is increasingly like commercial advertising. See generally Ronald K. L. Collins & David M. Skover, *The Death of Discourse* (1996) (discussing effects of advertising and commercialization on politics and political discourse in the United States since the advent of mass broadcast media).

[FN82]. Hirsch's Theory of Internet Reality claims (only partially tongue-in-cheek) that  $R=IT^2$  (reality equals information times speed of information transfer squared). Wide and rapid transfer of information creates the impression that the information is accurate. See David Beckman & David Hirsch, *We Log On, Therefore We Believe*, ABA J., Sept. 2000, at 74. Recall the political

brouhaha over the racist reading of Richard J. Herrnstein & Charles Murray, *The Bell Curve* (1994), which discussed the alleged differences in intelligence among different population groups in the United States. *Intelligence, Genes, & Success: Scientists Respond to The Bell Curve* at v- vi (ed. Bernie Devlin, et. al. 1997 paperback ed.) asserts that the 1994 publication of *The Bell Curve* "quickly produced an engaged public response ... colored by political perspectives" and that "[m]any of the harshest criticisms appear to come from those who scarcely refer to statements and claims actually found in the book!" See Robert L. Hayman, Jr., *The Smart Culture: Society, Intelligence, and Law* 8-10 (1998), which attacks both *The Bell Curve*'s science and others' political use of *The Bell Curve*).

[FN83]. In this section, "current" means through September 2000.

[FN84]. See, e.g., FTC, *Privacy* 5/00, at 6-7 (discussing seal organizations).

[FN85]. See *Online Profiling Part 2*, supra note 17, at 4; see also NAI, *Self-Regulatory Principles for OnLine Preference Marketing by Network Advertisers*, available at <http://www.ftc.gov/os/2000/07/index.htm#27> (supplying the final text of the NAI policy in a PDF document indexed under July 27, 2000) [hereinafter *NAI Final*]. Experts disagree emphatically on the likelihood that non-personally identifiable information can (or will) be correlated with personally identifiable information. Compare *Profiling Workshop*, supra note 17, at 22, 68 ("The standard is not that we won't violate privacy or we won't figure out who the consumer is; our standard is that we can't. Literally, if you go through our database, we can't figure out who you are.") (remarks of Daniel Jaye, Chief Technology Officer, Engage Technologies, Inc., Internet advertising agency), with *id.* at 43, 61 (remarks of Richard Smith, independent Internet security consultant), and *id.* at 43-44, 78 (stating that cookies track persons across domains and 'do become universal Ids') (remarks of Eric Winger, Assistant Attorney General in New York's Internet Bureau). Double-Click, another Internet advertising giant, however, recently purchased a large off-line database; the company seemingly intended to merge this acquisition with its on-line data. See *Profiling Workshop*, supra note 17, at 177-78.

[FN86]. See Online Profiling Part 2, *supra* note 17, at 6.

[FN87]. See *id.* ("[T]he NAI principles present a solid self-regulatory scheme."); *id.* at 9 ("Simply stated, we do not have a market failure here that requires legislative solution ... I oppose imposing burdensome regulation on an entire industry to address the 10% of advertisers who are not members of NAI ....") (quoting Commissioner Swindle).

[FN88]. See Pew Project, *supra* note 79, at 5.

[FN89]. The game industry's self-regulation standards ban targeting children in advertising of violent games, but the FTC recently reported wide spread violations. See FTC Violence, *supra* note 5, at 53.

[FN90]. See Online Profiling Part 2, *supra* note 17, at 6 (calling for legislation because of these shortfalls). Drop out had already begun when I first wrote this article. For example, between the June FTC announcement and early September, NAI lost both Avenue A and L90. NAI gained Adsmart and Real Media. The membership list also started listing two subparts of other members: B Flycast and NetGravity (respectively part of Engage and DoubleClick). Compare FTC, Prepared Statement of the FTC, Online Profiling: Benefits and Concerns before the Senate Comm. on Commerce, Science, and Transportation (June 13, 2000), at 5, available at <http://www.ftc.gov/os2000/06/onlineprofile.htm>, with NAI, Our Members, <http://www.networkadvertising.org/> (visited Oct. 11, 2000). As of April 18, 2001, NAI included AdForce, Avenue A, Double Click, Engage Inc., L90, MatchLogic Inc., and 24/7 Media. See *id.* (last visited Apr. 18, 2001).

[FN91]. The difference between opt-in and opt-out is easy to overstate. 'Opt-in' screens can be presented with the opt-in box already checked. Opt-in, however, has the potential to short-circuit business' attempts to externalize costs onto consumers. See, e.g., Sovern, *supra* note 75, at 1106.

[FN92]. See FTC, Privacy II, *supra* note 17, at 24-26; see also EPIC, Surfer Beware III: Privacy

Policies without Privacy Protection ("We also found that the privacy policies available at many websites are typically confusing, incomplete, and inconsistent.") <http://www.epic.org/reports/surfer-beware3.html> (visited Aug. 27, 2000).

[FN93]. Information collectors are using transaction costs to lower rates of consumer opt-out. See *Sovern*, *supra* note 75, at 1081-94; see also *Lessig*, *supra* note 77, at 160 ("No one has the time or patience to read through cumbersome documents describing obscure rules for controlling data.").

[FN94]. Compare, e.g., World Wide Web Consortium, Platform for Privacy Preferences (P3P) Project <http://www.w3.org/P3P> (visited Aug. 10, 2000) (P3P is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit), with, e.g., Karen Coyle, P3P: Pretty Poor Privacy?: A Social Analysis of the Platform for Privacy Preferences (P3P) <http://www.kcoyle.net/pep.html> (P3P "is designed not to protect data privacy but to facilitate the gathering of data by web sites.") (visited Aug. 10, 2000). EPIC is a good starting point for surfers interested in pro-privacy technologies. See EPIC, EPIC Online Guide to Practical Privacy Tools <http://www.epic.org/privacy/tools.html> (providing links to many privacy providers) (visited Oct. 2, 2000).

[FN95]. The vast majority of consumers are not even ready to handle secure e-mail. See William Spernow, Commentary, *N.Y. Times*, Aug. 25, 2000, available at [http://www.nytimes.com/cnet/CNET\\_0\\_4\\_2613005\\_00.html](http://www.nytimes.com/cnet/CNET_0_4_2613005_00.html)&gt;. Besides fearing the loss of a new technological breach in your privacy wall, many computer users may have a fear of inadvertently harming their own data. Even technologically sophisticated computer users may inadvertently harm their computer databases when attempting to install privacy-protection systems. See, e.g., *Profiling Workshop*, *supra* note 17, at 44, 86-87 (remarks of Danny Wetzner, Technology and Society Domain Leader for the World Wide Web Consortium admitting that he wiped most of his computer while trying to install a privacy system).

[FN96]. See Online Profiling Part I, *supra* note 17, at i-ii.

[FN97]. Profiling Workshop, *supra*note 17 (providing transcript).

[FN98]. See FTC, Online Profiling: Benefits and Concerns before the Senate Comm. on Commerce, Science, and Transportation (June 13, 2000), at 5, available at <http://www.ftc.gov/os/2000/06/onlineprofile.htm>.

[FN99]. See NAI Final, *supra* note 85.

[FN100]. *Id.* VI, at 12.

[FN101]. *Id.*

[FN102]. *Id.* VIII, at 12. This provision may be the reason why certain large entities are members themselves, as well as containing member subsidiaries. For example, Flycast and AdKnowledge are parts of Engage. See *infra* notes 118-20 and accompanying text. NetGravity is identified on the membership list as part of DoubleClick. See NAI [http:// www.networkadvertising.org](http://www.networkadvertising.org) (visited Oct. 11, 2000).

[FN103]. See NAI <http://www.networkadvertising.org> (visited Oct. 11, 2000). NAI's members include 24/7, Burst!Media, DoubleClick, Engage, Flycast, MatchLogic, NetGravity (a division of DoubleClick), and Real Media. See *id.*

[FN104]. As of April 2001, the NAI site has an opt-out spot, where a visitor may check separate boxes to opt-out of non-PII collection by Adforce, Avenue A, Double Click, Engage, L90, MatchLogic, and 24/7 Media. Enforcement by Arthur Andersen LLP is allegedly forthcoming. See *id.*

[FN105]. See NAI Final IV.B.2(a), (b), *supra*note 85.

[FN106]. See *id.*

[\[FN107\]](#). See supra note 51 and accompanying text.

[\[FN108\]](#). The OPA (Online Privacy Alliance) guidelines are also the NAI rules on collection of PII. See NAI Final III, supra note 85, at 3. The OPA is an industry group, not a consumer organization, and it requires notice and choice in the vast majority of circumstances as to undefined PII. The guidelines do not apply to "proprietary" information. See OPA, Guidelines for Online Privacy Policies available at <http://www.privacyalliance.org/resources/ppguidelines.shtml> (last visited Sept. 9, 2000).

[\[FN109\]](#). See NAI Final IV.A.4, supra note 85, at 3-4 (emphasis added).

[\[FN110\]](#). See, e.g., Profiling Workshop, supra note 17, at 61 (remarks of Richard Smith, independent Internet security consultant).

[\[FN111\]](#). As author Thomas Sterns Eliot stated:

We are the hollow men  
We are the stuffed men  
Leaning together  
Headpiece filled with straw. Alas!  
....  
This is the way the world ends  
This is the way the world ends  
This is the way the world ends  
Not with a bang but a whimper.  
Eliot, supra note 1, at 542.

[\[FN112\]](#). See NAI Final IV.B.1.(d), (e), (g), supra note 85, at 5, 8, 11.

[\[FN113\]](#). See DMA Interactive <http://www.the-dma.org> (visited Aug. 22, 2000). "[DMA] is the oldest and largest trade association for users and suppliers in the direct, database and interactive

marketing fields." Id. EPIC's 1998 privacy report asserted that DMA's members were not following the then-current DMA privacy policy. See EPIC, EPIC Online Guide to Practical Privacy Tools <http://www.epic.org/privacy/tools.html> (visited Oct. 2, 2000).

[FN114]. See Online Profiling Part 2, *supra* note 17.

[FN115]. DMA, Privacy Policy <http://www.the-dma.org/privacy.shtml> (visited Aug. 22-23, 2000). Since September, 2000, DMA has changed its privacy policy to state that DMA "place[s] cookies on visitors [sic] hard drives to collect aggregate generic information about the number of visitors." Id. (last visited May 17, 2001).

[FN116]. DMA, Privacy Policy <http://www.the-dma.org/privacy.shtml> (visited Aug. 22-23, 2000) at 2.

[FN117]. "URL" stands for "universal resource locator," the address on the Internet, which is the letter string keyed into a web browser's control line to reach a desired site. See Mark A. Lemely, et. al., *Software and Internet Law* 1099 (2000).

[FN118]. "Linking" or "hyperlinking" by using "links" or "hyperlinks" refers to clicking a computer mouse on icons or underlined text (commonly colored blue or red on computer screens) that take the user directly to another page or document on the Internet. See *id.* At 1093-94. This process works through the scientific magic of "HTML" (hypertext markup language), which is the lingua franca of web pages. See *id.*

[FN119]. The DMA's use of an outdated URL appears misleading. The business and advertising community has raised a tremendous fuss about the allocation of domain names on the theory that the public expects a domain name to match a firm's trade name. See, e.g., [15 U.S.C. 1125\(d\)](#) (creating a cause of action for "cyberpiracy" of domain name similar to a trademark); ICANN, Uniform Domain-Name Dispute-Resolution Policy, available at <http://www.wcann.org/udrp/udrp.htm> (providing a means to resolve disputes between trademark holds

and unaffiliated holders of allegedly confusing domain names). Does the DMA have some reason for wanting visitors to think its advertisements are not part of the Engage empire? Again, no one is quite telling a lie. Flycast Communications is one of several smaller firms that were integrated into Engage. See Engage.com, About Engage Media [http://www.engage.com/engagemedia/about\\_us](http://www.engage.com/engagemedia/about_us) (visited Aug. 23, 2000). Engage.com is now part of NASDAQ-traded CMGI, Inc., "the largest, most diverse network of Internet companies in the world." See Engage.com < [www.engage.com/company/parentino\\_company.cfm](http://www.engage.com/company/parentino_company.cfm) > (visited Aug. 23 2000). My suspicions, perhaps unjustified, were further aroused when I visited the privacy page of GeoCities, which is now part of Yahoo! An early FTC privacy invasion case targeted GeoCities. See Federal Trade Commission <http://www.ftc.gov/opa/1998/9808/geocitie.htm> (visited Aug. 23, 2000) (announcing FTC's first on-line privacy consent decree); see also Federal Trade Commission <http://www.ftc.gov/os/1998/9808;index.htm> (providing links to multiple FTC documents in File No. 982 3051, In re GeoCities).

[\[FN120\]](#). A reference to Flycast can be found by running a site search at Engage.com, but my attempts also retrieved many items in which I could find no mention of Flycast.

[\[FN121\]](#). See OnLine Profiling Part 1, *supra* note 17, at 22.

[\[FN122\]](#). See Engage.com <http://www.engage.com>.

[\[FN123\]](#). The "Privacy On This Site" link advises the user to send an e-mail to deal with information collected at the Engage site. A user must link to "Opt Out Options" to block Engage's advertising service cookies. See Engage.com, Privacy <http://www.engage.com/privacy> (visited Aug. 22, 2000).

[\[FN124\]](#). DMA, Privacy Policy <http://www.the-dma.org/privacy.shtml> (visited Aug. 22-23, 2000).

[\[FN125\]](#). See Engage.com, Privacy <http://www.engage.com/privacy> (visited Aug. 22, 2000)

[FN126]. See Welcome to Engage Media <http://www.engage.com/engagemedia> (visited Aug. 22, 2000).

[FN127]. See Profiling Workshop, *supra* note 17, at 67-68 (remarks of Daniel Jaye, Chief Technology Officer, Engage Technologies, Inc. & Jason Catlett, President of JunkBusters).

[FN128]. See Online Profiling 1, *supra* note 17, at 12-13 (explaining why many persons are against anonymous profiling). A 1997 Georgia Tech study reported that 87% of American Internet users believed they should have complete control over their demographic information. See Profiling Workshop, *supra* note 17, at 210, 276 (remarks of Andrew Shen, Policy Analyst, Electronic Privacy Information Center).

[FN129]. See Online Profiling 1, *supra* note 17, at 15.

[FN130]. Profiling Workshop, *supra* note 17, at 43, 61 (stating that identifying someone who was the subject of "anonymous profiling" is "very, very easy"). "[A]ll you do is send out an e-mail message that sends back both the e-mail address and the cookie." *Id.* (remarks of Richard Smith, Internet security consultant).

[FN131]. See Profiling Workshop, *supra* note 17, at 124 (quoting Jonathan Shapiro of DoubleClick).

[W]e are only ever going to capture that personally identifiable information in places where the user is given notice, and as part of that notice they will be given the choice to participate or not. If they choose not to participate, if they opt out of the DoubleClick cookie, then there's no way for me to link that personally identifiable information with their online behavior. I can't technically do it.

*Id.* at 178.

[FN132]. In September 2000, DoubleClick's privacy notice informed surfers that one unnamed DoubleClick client was combining DoubleClick--provided anonymous data with personally

identifiable information obtained elsewhere. DoubleClick allegedly had requested the client to disclose this information on its own web site. DoubleClick did not name the offending client. See DoubleClick, Privacy Policy <http://www.doubleclick.com/us/corporate/privacy/> (visited Sept. 2000).

[FN133]. FTC, Privacy II, *supra* note 17, at 9-10. "A weighted analysis figure reflects the likelihood that a consumer will visit a site that follows that practice." *Id.* at 8.

[FN134]. Toysmart Privacy Policy, Ex. 1 to FTC's First Amended Complaint, *FTC v. Toysmart.com* (D. Mass., Civ. No. 00-11341-RGS), <http://www.ftc.gov/opa/2000/07/toysmart2.htm> (visited Aug. 18, 2000). The attorneys general of forty-four states also filed objections to the data sale. See Bytes in Brief, Sept. 2000, at 3 (Bytes in Brief is a monthly, free cyber law update service available from Sensei Enterprises, Inc., e-mail "senseient.com; <http://www.senseisent.com>).

[FN135]. Several FTC Commissioners dissented or entered statements mentioning concerns on this point. See Statement of Commissioner Anthony; Statement of Commissioner Thompson; Dissenting Statement of Commissioner Swindle, <http://www.ftc.gov/opa/2000/07/toysmart2.htm> (visited Aug. 18, 2000).

[FN136]. Exhibit A: Stipulation and Order Establishing Conditions on Sale of Customer Information, Filed in United States Bankruptcy Court for the District of Massachusetts, Eastern Division 2 (Chapter 11 Case No. 00-13995-CJK), <http://www.ftc.gov/opa/2000/07/toysmart2.htm> (visited Aug. 18, 2000).

[FN137]. Michael Brick, Judge Overturns Deal on Sale of Online Customer Database, *N.Y. Times*, Aug. 18, 2000, available at <http://www.nytimes.com>.

[FN138]. JunkBusters, What's News at JunkBusters <http://junkbusters.com/ht/en/new.html> (visited Aug. 18, 2000).

[FN139]. See *id.*

[FN140]. See Brick, *supra*note 137.

[FN141]. Two bills were pending at the close of the 106th Congress. See Consumer Privacy Protection Act, S. 2606, 106th Cong. (2000); Privacy Policy Enforcement in Bankruptcy Act of 200, S.2857, 106th Cong. (2000). TRUSTe filed an objection to the proposed FTC/Toysmart.com settlement with the Bankruptcy court and hails the court's ruling as a victory, despite the still unclear fate of the consumer information. See TRUSTe, TRUSTe Files Objection to Federal Trade Commission Consent Agreement with Toysmart.com [http://www.truste.org/users/users\\_toysmart\\_objection.html](http://www.truste.org/users/users_toysmart_objection.html) (visited Oct. 8, 2000); TRUSTe, TRUSTe Applauds Bankruptcy Court Decision Regarding Toysmart.com, [http://www.truste.org/users/users\\_toysmart\\_adv.html](http://www.truste.org/users/users_toysmart_adv.html) (visited Sept. 8, 2000).

[FN142]. Yahoo! has "the largest global audience on the Web." Cory Johnson, Yahoo "Ads" It Up, *The Industry Standard*, Sept. 11, 2000, at 79; see also Steve Lawrence & C. Lee Giles, Accessibility of Information on the Web, 400 *Nature* 107, 177 (July 1999) (indicating that Yahoo! is the site with the highest advertising revenue).

[FN143]. See Yahoo! Privacy Center, <http://privacy.yahoo.com/privacy/us/print.htm> (visited Sept. 31, 2000). Yahoo! also may use or share the information if ordered to do so by a court or if you violate its terms of service. See *id.*

[FN144]. Yahoo!, Privacy <<http://privacy.yahoo.com/privacy/us/adserver/details.html>> (visited Sept. 3, 2000) (emphasis added).

[FN145]. *Id.* (emphasis added).

[FN146]. 24/7 Media <http://www.247media.com> (visited Sept. 12, 2000).

[FN147]. See 24/7 Media, Privacy <http://www.247media.com/privacy.html> (visited Sept. 12, 2000).

[FN148]. When I first visited the site on Sept. 3, 2000, I had a different experience. The link was to a privacy statement headed by a notice that about August 31, 2000 the site would post a new policy with "more robust notice and choice regarding 24/7 Media's privacy and data collection practices." The policy I saw rambled on for five pages starting with 24/7's membership in TRUSTe. I was told how to opt out of information collection at 24/7.com and other sites owned by 24/7, but I saw no mention of opting out of the firm's data collection through advertisements it services on others' web sites. I was told (three pages into the policy) that I could e-mail a given address to remove my name from 24/7's database of personally identifiable information. Why should I bother, however, if the information would just reappear next time I browsed?

[FN149]. 24/7 Media, Privacy <http://www.247media.com/privacy.html> (visited Sept. 12, 2000).

[FN150]. Id.

[FN151]. Id.

[FN152]. Id.

[FN153]. Id.

[FN154]. Id.

[FN155]. See AdForce <http://www.adforce.com> (visited Sept. 12, 2000).

[FN156]. See AdForce, AdForce and Privacy <http://www.adforce.com/company/privacy/addeliveryprivacy.asp> (visited Sept. 12, 2000).

[FN157]. Id.

[FN158]. Id.

[FN159]. Id.

[FN160]. Id.

[\[FN161\]](#). Be Free <http://www.befree.com> (visited Mar. 2, 2001).

[\[FN162\]](#). See Be Free, Privacy Information [http:// www.befree.com/docs/includes/privacy.html](http://www.befree.com/docs/includes/privacy.html) (visited Sept., 2000).

[\[FN163\]](#). Id.

[\[FN164\]](#). Id. ("[U]sers [can] opt out of personalization entirely.").

[\[FN165\]](#). Id.

[\[FN166\]](#). Id.

[\[FN167\]](#). Id.

[\[FN168\]](#). Matchlogic.com <http://www.matchlogic.com> (visited Sept. 8, 2000).

[\[FN169\]](#). See Matchlogic.com, Privacy Policy [http://www.matchlogic.com/ privacy/privacy\\_policy.asp](http://www.matchlogic.com/privacy/privacy_policy.asp). The three services are registration data collection, on-line ad servicing, and e-mail marketing. See id. A "cookie opt-out" and a "cookie opt-in" are also available. Id.

[\[FN170\]](#). Id. The policy indicates that such information will be shared with third parties only if the on-line registrant agreed. See id. The policy also states that it will stop using the PII if a user so request. See id.

[\[FN171\]](#). See id.

[\[FN172\]](#). See <http://www.mediaplex.com/mp/privacy/privacy.html>.

[\[FN173\]](#). See Mediaples.com, Privacy Policy, [http://www.mediaplex.com/mp/ privacy/privacy.html](http://www.mediaplex.com/mp/privacy/privacy.html) (visited Sept. 8, 2000).

[\[FN174\]](#). See id.

[\[FN175\]](#). Id.

[FN176]. Sabela.com <http://www.us.sabela.com> (visited Sept. 8, 2000).

[FN177]. See id. Setting a cookie on a user's hard drive "allows [[Sabela] to deliver ads that are more relevant to [the user] and avoid delivering the same ads too many times." Id.

[FN178]. See id.

[FN179]. See id.

[FN180]. Vitabella <http://www.track-star.com/privacy.html> (visited Sept. 8, 2000).

[FN181]. See Vitabella, Privacy <http://www.track-star.com/privacy.html>.

[FN182]. Id.

[FN183]. See id.

[FN184]. WebConnect <http://www.webconnect.com> (visited Sept. 8, 2000).

[FN185]. See Webconnect, Privacy Pledge <http://www.webconnect.com/NewMedia/Privacy.html> (visited Sept. 8, 2000).

[FN186]. Id.

[FN187]. WebConnect, What We Do <http://www.webconnect.com/site4/WhatWeDo.asp> (visited Sept. 8, 2000).

[FN188]. Id.

[FN189]. Id.

[FN190]. See, e.g., Donna L. Hoffman, et al., Building Consumer Trust in OnLine Environments: The Case for Information Privacy, Vand. U. eLab (1998), available at <http://www2000.ogsm.vanderbilt.edu/papers.html> (consumers do not trust merchants and will not do so until they have opt-in power over information collection).

[FN191]. See FTC, Privacy II, *supra* note 17, at i-ii. The FTC's 1998 survey found that about 92% of Web sites collected personal information but that only 14% disclosed anything about their information practices. The 1999 Georgetown Internet Privacy Policy Survey found that 10% of sites posted some disclosure that at least touched on the four basic information practice principles (notice, choice, access, and security). See *id.* at i.

[FN192]. See Online Profiling Part I, *supra* note 17, at 7-10.

[FN193]. See FTC, Privacy II, *supra* note 17, at 12.

[FN194]. See *id.* at 13. For more details, see *id.* at 7-28, Appendix A-C.

[FN195]. See *id.* at 15. The FTC gave credit for any principle if the site followed that principle as to at least some information. See *id.* at 23.

[FN196]. See *id.* at 21. The weighted analysis figures are that 69% of sites a surfer will visit have third party cookies and that only 41% of the cookie sites the surfer visits will disclose their existence. See *id.*

[FN197]. See Online Profiling Part 1, *supra* note 17, at 10.

[FN198]. See FTC, Privacy II, *supra* note 17, at ii.

[FN199]. BBOnLine, How the Privacy Program Works <http://www.bbbonline.org/privacy/index.asp> (visited Sept. 27, 2000). On Sept. 7, 2000, however, the home page of the BBOnLine web site said the privacy program had 497 "participating web sites." *Id.* (visited 9/7/00). I sent an email asking for clarification on September 7, 2000, but received no response.

[FN200]. TRUSTe Awards 1000th Privacy Seal! <http://www.truste.org/> (visited Aug. 27, 2000). Privacybot does not give membership figures at its web site. See Privacybot, <http://www.privacybot.com> (visited Aug. 27, 2000). On August 27, 2000, I emailed Privacybot for

more information; I received no response'.

[FN201]. E-mail from Dave Steer, TRUSTe, to author (Aug. 27, 2000) (on file with Catholic University Law Review).

[FN202]. See Lawrence & Giles, *supra* note 142, at 107. If the same material was accessible at multiple servers, the study only counted one address. See *id.* As for amount of content, a recent report claims 1.2 billion documents theoretically reachable with technology now used in most commercial web browsers and another 550 billion documents which would be available with improved technology. See Elinor Abreu, *Diving into the Deep Web*, *The Industry Standard*, Sept. 11, 2000, at 119. Search engine Google, supposedly, has only indexed some 600 million pages so far. See *id.*

[FN203]. Seal organizations may not be trustworthy. See, e.g., Ann Bartow, [Our Data Ourselves: Privacy, Propertization, and Gender](#), *34 U.S.F. L. Rev.* 633 (2000) (questioning whether TRUSTe or BBBOOnline has shown willingness to stand up for privacy against their customers, the web sites desiring seals); Bob Tedeschi, *Sellers Hire Auditors to Verify Privacy Policies and Increase Trust*, *N.Y. Times*, Sept. 18, 2000 (e-commerce report), available at <http://www.nytimes.com/2000/09/18/technology/18ECOMMERCE.html> (reporting that TRUSTe lost reputational clout when it failed to penalize Microsoft, a TRUSTe investor and member, for collecting hardware identification numbers from PC users without notifying or consulting the users). The EU is concerned about consumer confusion among seal organizations and has, therefore, begun work on member states accrediting seal issuing groups that require a set of core principles. See Commissioner Byrne, *Cyberspace and Consumer Confidence* speech to the Annual Conference of the Kangaroo Group of MEP's) [http://europa.eu.int/comm/dgs/health\\_consumer/library/speeches/speech55\\_en.html](http://europa.eu.int/comm/dgs/health_consumer/library/speeches/speech55_en.html) (visited Sept. 9, 2000).

[FN204]. One 2000 survey reported that 92% of on-line households do not trust companies to

protect private information despite contrary promises. See Tedeschi, *supra*note 203, available at <http://www.nytimes.com/2000/09/18/technology/18ECONOMMERCE.html>.

[FN205]. BBBOOnline posts statistics on use of the dispute resolution service that is a required part of its privacy seal. From January 1, 2000 through March 31, 2000, the program received only six eligible complaints and fifteen ineligible complaints; it decided three cases. From October 1, 1999 through December 31, 1999, the service received eleven eligible complaints and 13 ineligible complaints; no cases were decided. From July 1, 1999 through September 30, 1999, BBBOOnline received one eligible and three ineligible complaints; no cases were decided. The figures for the earliest reported period, March 17, 1999 through June 30, 1999, are one eligible and three ineligible complaints received and no cases decided. See BBBOOnline, Dispute Resolution <http://www.bbbonline.org/reliability/dr.asp> (visited Sept. 8, 2000). All of these BBBOOnline statistical summaries mentioned hundreds of "inquiries" unrelated to the privacy program. TRUSTe claims it has "helped thousands of Web users resolve their privacy complaints." TRUSTe, [http://www.truste.org/users/users\\_watchdog\\_intro.html](http://www.truste.org/users/users_watchdog_intro.html) (visited Sept. 7, 2000). I could not, however, find any statistical breakdown on types of "help" provided, even though TRUSTe had promised to post statistical summaries twice a year. See TRUSTe, Privacy Seal Program Watchdog Compliance and Escalation Process Part 7 [http://www.truste.org/users\\_watchdog\\_intro.html](http://www.truste.org/users_watchdog_intro.html) (visited Sept. 7, 2000). On Sept. 7, 2000, I emailed TRUSTe for clarification; I received no response. The dispute resolution information page only lists a handful of resolutions for privacy problems brought to TRUSTe's attention.

[FN206]. See Nielsen/NetRatings <http://209.249.142.27/nnpm/owa/NRpublicreports.topadvertisermonthly> (visited Aug. 28, 2000); Nielsen/NetRatings <http://209.249.142.27/nnpm/owa/NRpublicreports.topadvertiserweekly> (visited Aug. 28, 2000).

[FN207]. See, e.g., List-Advertising.com, Email List Advertising Terminology <http://www.list-advertising.com/terms/> (visited Sept. 2, 2000). In Internet jargon, an "impression" is a "log entry recorded by a web server of the successful exit of the HTML ad string from the server." Me-

diaplex, Privacy Policy <http://www.mediaplex.com/mp/privacy/privacy.html> (visited Sept. 3, 2000).

[FN208]. Webster's New Universal Unabridged Dictionary 962 (1996). Again, no one is telling an untruth. The possibly misleading advertising term is an outgrowth of the printing industry's use of "impression" for the number of times printing plates have been used to "impress" the same image on different pieces of paper. *Id.*

[FN209]. See, e.g., Donna L. Hoffman & Thomas P. Novak, When Exposure-Based Advertising Stops Making Sense (And What CDNOW Did About It) *Vand. U. eLab* (2000), available at <http://www2000.osgm.vanderbilt.edu/papers.html> (explaining that Internet allows consumers to interact with the advertisement, thus enabling measurement of valuable, active consumer response as opposed to unimportant, passive consumer exposure to the content).

[FN210]. TRUSTe, TRUSTe Ranked as the Most Trusted Symbol on the Web, [http://www.truste.org/about/about\\_cheskin.html](http://www.truste.org/about/about_cheskin.html) (visited Sept. 7, 2000). Please note that while I disagree with TRUSTe about the import of the Cheskin study, I am not claiming that TRUSTe has made any factually incorrect statements in its press release.

[FN211]. See Cheskin Research, *supra* note 39.

[FN212]. Although Cheskin is a for-profit research company, this study was an in-house project that was not financed by any specific client. See e-mail from Denise Klarquist, to author (Sept. 9, 2000) (explaining the nature of Cheskin and the study) (on file with Catholic University Law Review).

[FN213]. One public advocacy group reported that an unfair trade practice complaint had been filed against TRUSTe and AOL. The complaint supposedly alleges that the TRUSTe seal posted at AOL.com deceives AOL members. Allegedly, AOL members are in a separate "members" portion of AOL that is not covered by the TRUSTe approved privacy policy posted at AOL.com.

See Privacy.Net, Unfair Trade Practices Complaint Filed Against Truste/AOL <http://www.privacy.net/truste.asp> (visited Sept. 12, 2000).

[FN214]. Average income of participants was over \$40,000, average age was 38, 61% of the those sampled spend more than 10 hours a week on-line, and 75% had made at least one purchase on line. According to the U.S. Census Bureau's 1999 figures, less than 50% of Americans 18 or older have any Internet access, and those with access are more likely than the general population to be employed full time and to have attended college. Almost 60% of Americans over 18 have household incomes under \$50,000, and only 32% of Americans over 18 with Internet access have household incomes under \$50,000. United States Census Bureau, 1999 Statistical Abstract of the United States, available at <http://www.census.gov/statab/freq/99s0923.txt>.

[FN215]. Cheskin Research, *supranote 39*, at 7.

[FN216]. *Id.* But see Hoffman, et al., *supranote 209* (arguing that only opt-in information policies will produce consumer trust). "A whopping 87% of Web users think that they should have "complete control" over the demographic information Web sites capture and over 71% believe there should be new laws to protect their privacy online." *Id.* at 3.

[FN217]. This claim is supported by statistics showing that the leaders in on-line income are well established, well known firms, as opposed to start up companies. See Mark Roberti & Eileen Buckley, Hey, Profits!, *The Industry Standard*, Sept. 11, 2000, at 58. An older study was somewhat more supportive of seal organizations. See Lorrie Faith Cranor, Joseph Reagle, & Mark S. Ackerman, Beyond Concern: Understanding Net Users' Attitudes About Online Privacy (AT&T Labs-Research Technical Report TR 99.4.3; issued April 1999), available at <http://www.research.att.com/resources/trs/TRs/99/99.4/99..4.3/report.htm>. This AT&T study involved questionnaires filled out during November 1998 by less than 400 heavy Internet users. See *id.* at 2. Taken separately, known firm names were much more important to the privacy-interested than were seals or posted privacy policies; however, a site that had both a posted privacy

policy and a seal (from a very well known organization) was rated about as trustworthy as one covered by a privacy statute. See *id.* at 10-11, 15.

[FN218]. VeriSign, Inc., headquartered in California, specializes in secure electronic payment and verification systems. See VeriSign, Inc., Corporate Overview <http://www.verisign.com/investor/overview.html> (visited Sept. 8, 2000). Along with the American Institute of Public Accountants, VeriSign provides eligible web sites with the WebTrust seal. This seal is only partially related to privacy issues; seal holders must pay for CPAs to audit their compliance with posted business policies including billing, fulfillment, and privacy integrity. No sign is issued solely upon privacy procedures. See VeriSign, VeriSign Secure Server Ids for the WebTrust Program, <http://www.verisign.com/webtrust/overview.html> (visited Sept. 8, 2000).

[FN219]. Cheskin Research, *supra*note 39, at 19-20.

[FN220]. See *id.* at 20 (indicating percentages of participants who actually read the different companies' privacy statements: Visa 27%; TRUSTe 25%, VeriSign 21%, MasterCard 15%, BBOnLine 10%).

[FN221]. See *id.* at 21. The 1999 figures in the United States were VeriSign 25%, BBOnLine 16%, MasterCard 13%, Visa 11%, and TRUSTe 9%. *Id.*

[FN222]. These two figures are for the entire study that included South America. The study did not break out figures for the United States. *Id.* at 29.

[FN223]. *Id.*

[FN224]. BBOnLine, How the Privacy Program Works <http://www.bbbonline.org/businesses/privacy/self-regulation.html> (visited Aug. 10 2000).

[FN225]. See BBOnLine, Privacy Program Dispute Resolution Processes Procedures, Privacy Policy Review Service and Privacy Review Appeals Board, available at <http://www.bbbonline.org> (visited Aug. 10, 2000).

[FN226]. See PrivacyBot.com, About PrivacyBot [http:// www.privacybot.com/about.shtm](http://www.privacybot.com/about.shtm) (visited Aug. 27, 2000). PrivacyBot uses non-binding mediation in its dispute resolution service. See *id.*; see also TRUSTe, Frequently Asked Questions: How Does TRUSTe ensure that Web Sites Stick to Their Privacy Polices? [http://www.truste.org/users/users\\_faqs.html](http://www.truste.org/users/users_faqs.html) (visited Sept. 7, 2000).

[FN227]. "Sanctions must be sufficiently rigorous to ensure compliance by organizations" but damages are only required "where the applicable law or private sector initiatives so provide." U.S. Dept. of Commerce, Safe Harbor Privacy Principles (July 21, 2000), available at <http://www.ita.doc.gov/td/ecom/shprinciplesfinal.thm>.

[FN228]. EC Directive, Chapter III, art. 24.

[FN229]. Asked to choose only one from a list of possible penalties for an Internet company that used personal information in ways that it said it would not, 11% of respondents wanted the company's owners put in jail, 27% wanted the company's owners fined, 26% wanted the site shut down, and 30% wanted the site placed on a list of fraudulent sites. See Pew Project, *supra* note 79, at 29 (Aug. 20, 2000).

[FN230]. See, e.g., Profiling Workshop, *supra* note 17, at 123, 167 (remarks of Dan Jaffee, Association of National Advertisers, that government should want self-regulation because the FTC and the Department of Commerce have insufficient staff to control industry behavior).

[FN231]. Only 43% of American Internet users know what a cookie is, only 51% of American Internet users who have clicked on an ad know what a cookie is, and only 56% of American Internet users who have bought a product on-line know what a cookies is. See Pew Project, *supra* note 79, at 8. Only 75% of people who have heard of cookies have even a "basic" understanding of how they work. See Online Profiling Part 2, *supra* note 17, at 11-12.

[FN232]. See Hoffman, et al., *supra*note 209, at 3.

[FN233]. See Pew Project, *supra*note 79, at 2.

[FN234]. See *id.*

[FN235]. *Id.* at 97-98.

[FN236]. See Profiling Workshop, *supra* note 17, at 104-05.

[FN237]. *Id.* at 118-19. The subjects were presumably unaware that ad-targeting profiles include psychological factors involving emotional vulnerabilities. See *id.* at 122-23, 127 (remarks of Jeff Chester, Executive Director of the Center for Media Education, referring to the Navient Company's self-description).

[FN238]. *Id.* at 110.

[FN239]. See *id.* at 112-13.

[FN240]. See Hoffman, et al., *supra*note 209, at 4 ("[C]onsumers do not view their personal data in the context of an economic exchange for information, as many commercial Web providers believe." (emphasis in original)).

[FN241]. Letter from James Madison to W.T. Berry (Aug. 4, 1822), reprinted in James Madison, *The Complete Madison* 337 (Saul K. Padover, ed., 1953).

[FN242]. See Harlan Lebo, *UCLA Report Finds Internet Surpasses Television as Key Information Source* (Aug. 15, 2000) available at, <http://www.uclanews.ucla.edu/docs/lshl.379.html> (visited Aug. 26 2000).

[FN243]. Several entities provide "anonymous" searching of various kinds. See, e.g., Anonymizer <http://www.anonymizer.com> (visited Sept. 29, 2000); Topclick <http://www.topclick.com> (visited Sept. 29, 2000).

[FN244]. The FTC has a set of very cute pages discussing "kidz" privacy issues. See FTC

<<http://www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html>> (visited Sept. 8, 2000). Seamlessly linked to the FTC material, and marked with the FTC's kidzprivacy cartoon, is a "kidz" search engine page. See Lycoszone <http://www.lycoszone.com/parentszn.html> (visited Sept. 8, 2000). The search engine is actually a commercially-run page and is not subject to the FTC privacy policy. See e-mail from FTC webmaster to author (Sept. 3, 2000) (on file with author).

[FN245]. My browser reported no active URL at [privatesearch.gov](http://privatesearch.gov) or [privatesearch.org](http://privatesearch.org). A consumer activist site lives at Privacy.net. Privacy.net: The Consumer Information Organization <http://www.privacy.net> (visited Sept. 8, 2000).

[FN246]. This proposal is not based on some pre-Nixon trust in government honesty, but only government action seems capable of producing such a private spot. Private causes of action, furthermore, would help police the privacy police. A non-profit foundation would be a second-best host: an entity with a relatively high profile and presumptive honesty. Enforcement, however, would still be a problem. I thank David E. Sorkin for this suggestion.

[FN247]. Telephone interview with industry source (Sept. 7, 2000).

[FN248]. Privacy Commission Act, H.R. 4049 § 9(a) (2000).

[FN249]. [U.S. Const. art. 1, § 8, cl. 8](#) (the Intellectual Property Clause).

[FN250]. See [Diamond v. Chakrabarty, 447 U.S. 303, 307 \(1980\)](#) (stating that patent power is intended to encourage a positive effect on society).

[FN251]. The PTO is entirely funded by fees and routinely collects more than the federal budget allows it to spend. See, e.g., 1999 USPTO Annual Report 4, 28 available at <http://www.uspto.gov/web/offices/com/annual/1999/> [hereinafter USPTO Report]. Budget projections for 2001 are that the PTO will collect \$1.2 billion, however, they will only be allowed to spend seventy-five percent of this sum. See Letter from Q. Todd Dickinson (Undersecretary of Commerce for Intellectual Property and Director of the U.S. PTO) to Hon. Howard Coble and

Howard Berman (ranking members of the House Subcommittee on Courts and Intellectual Property) (June 9, 2000), available at <http://www.uspto.gov/2001budget.html>.

[FN252]. See The Federal Search Foundation <http://www.fed-search.org/> (visited Sept. 12, 2000). The search engine will give access to 20,000 government web sites involving 27 million pages. See Spenser Hsu, *New Site Streamlines Online Government: Powerful Search Engine Links Thousands of Internet Pates in One Location*, Wash. Post, Sept. 23, 2000. The engine will be able to handle over 100 million queries each day. See *id.* The government has procured a three-year maintenance contract for \$4.1 million dollars. See *id.* and *Washington Post Correction*, Sept. 26, 2000.

[FN253]. Only publicly available documents will be used in this search, and there will be no tracking of personal user information of any kind. Aggregate web site metrics, such as traffic loads and bandwidth measurements, will be used to improve the quality of both the search experience and the overall user experience. See *The Federal Search Foundation: The Engine Behind E-Government: Most Often Asked Questions and Answers at Q.7* (Sept. 22, 2000 briefing material provided to author by Christina Peterson, Federal Search Foundation). This site was in operation at <http://www.firstgov.gov> when this article went to press. See <http://www.firstgov.gov> (visited Apr. 18, 2001). The site's privacy policy, however, collects allegedly non-PII to which I object-- visitors' IP addresses and the page from which you linked. See *id.*

[FN254]. See *id.* at Q.9. Linking entities, called certified partners, must also promise to respect the data's integrity, attribute the information to the government, provide free access, not associate "inappropriate" material, and establish methods for "user feedback." *Id.*

[FN255]. Alternatively, the engine could discard all located sites that lacked a certificate or token issued by the government entity running PrivateSearch.gov.

[FN256]. Class actions for statutory damages might be expressly allowed, and whistle blower protection would also be helpful.

[FN257]. The Yahoo! fee is about \$199. See James Fallows, *Searching for Revenue The Industry Standard*, Sept. 4, 2000, at 51, 52. Yahoo! also markets higher visibility on its portal. See, e.g., David D. Kirkpatrick, *Bookseller and Yahoo to Announce Pact*, N.Y. Times, Sept. 19, 2000, available at <<http://www.nytimes.com/2000/09/19/technology/19book.html>> (discussing contracts between Yahoo and Barnesandnoble.com, Amazon.com, Costco, Spiegel.com, and Kmart Corporation's Bluelight.com). Some of these contracts involve free Internet service for consumers. See *id.*

[FN258]. Trademark registrations have been electronically filable since 1998. See USPTO Report, *supranote 251*, at 5.

[FN259]. Some businesses have hired auditing firms to certify compliance with posted privacy policies, but this is quite expensive. For example, the travel site Expedia.com allegedly paid PricewaterhouseCoopers a six-figure fee. See *Tedeschi, supranote 203*, at 2. Apparently, only some 200 companies have gone this route. See *id.* at 3.

[FN260]. PlumbingWorld.com guarantees absolute privacy; however, it does not post a privacy seal. Plumbingworld.com <http://www.plumbingworld.com> (visited Sept. 3, 2000).

END OF DOCUMENT