PERSONAL PRIVACY ON THE INTERNET: SHOULD IT BE A CYBERSPACE ENTITLEMENT?

BRIAN KEITH GROEMMINGER*

"[N]ever has our ability to shield our affairs from prying eyes been at such a low ebb."[1]

INTRODUCTION

Jane signs onto the Internet, preparing for what most would deem a typical, innocuous Web browsing experience. Jane purchases some clothing for herself and her two- and five-year-old children on an up-scale department store's Web site. She then follows with an extended review of a Web site featuring weight loss plans.

Although most would consider this browsing experience a litany of mundane transactions, a savvy direct marketer with the ability to covertly monitor these activities considers the information obtained priceless. As surprising as it may be to many Web surfers, assembling an alarmingly detailed profile of Jane, without her knowledge or consent, is quite possible with a single browsing activity such as the one previously outlined. Although this scenario requires some inferences, a marketing profile of Jane's transactions might develop as follows: Jane is a mother with two young children, purchases some up-scale goods, and is seriously concerned about her weight and health. Based on her, a merchant or vendor might want to send Jane advertisements, e-mails, banner, advertisements, or pop-up advertisements that offer expensive home exercise equipment. The equipment would allow her to stay at home with her children, aid with her fitness goals, and be affordable based on her observed consumer spending pattern.

An advertisement for exercise equipment may not bother Jane at all. In fact, she may actually be interested in home exercise equipment instead of a different ad that would have been randomly posted on her computer screen as she browsed the Web. However, Jane might be very disturbed by the covert means employed by the merchants to collect, aggregate, use, and/or sell her personal information without asking her for permission or notifying her of their intent to use the information in that manner.

The scenario depicts the rising tension between one's personal privacy and the marketing interests of merchants in the exploding technological megaplex of the Internet.[2] This Note will explore this fragile balance of interests and the

---

* J.D. Candidate 2003, Indiana University School of Law—Indianapolis; B.S., 1992, Indiana State University; M.B.A., 1994, Indiana State University. I would like to thank Professor James Nehf for his insight and guidance throughout the development of this Note.

1. Bernstein v. Dep't of Justice, 176 F.3d 1132, 1146 (9th Cir. 1999).

2. For purposes of this Note, privacy is defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 2, 6

tempestuous debate regarding the appropriate line of demarcation between the collection of personal data and individual privacy rights.

Part I of this Note discusses the technological means employed by Web sites to collect personal information from their Web site visitors. Part II of this Note explores the opposing views regarding cyberspace privacy. Part III discusses the various approaches employed to protect individuals and their privacy rights. Part IV analyzes the current U.S. framework of self-regulation and its implications and results. Part V reviews some current proposed solutions to the Internet privacy dilemma. Finally, Part V proffers a new solution regarding Internet privacy, a market-determined balance between e-commerce interests and individual privacy interests.

I. MONITORING ON THE INTERNET

A. Dissection of an Internet Transaction

Without burrowing too deeply into the technological nuances of Internet architecture, it is important to understand the mechanics involved in a typical Internet transaction in order to understand how one's privacy can be so easily surrendered in cyberspace. Basically, Internet activities are composed of electronic requests for information and subsequent electronic fulfillment of those requests.[3] In other words, a surfer's mouse "click" initiates a submission of an electronic request to view data on a Web site, the site's computer receives the electronic request, and finally, the site sends the requested data to the specific computer making the request.[4] In order to send the information to the correct computer among the millions logged onto the Internet, the Web site must be able to distinguish the computer requesting data from all other online computers. An Internet protocol (IP) address, which is basically a specific machine address assigned by the Web surfer's Internet service provider (ISP) to a user's computer, accomplishes this task.[5] Hence, every time a transaction requesting or sending data occurs on the Web this unique IP address accompanies the data.[6] Furthermore, both the ISP and the Web site typically log these transactions.[7] To the detriment of users' personal privacy and anonymity on the Web, however, the uniqueness of the IP address may allow someone in possession of another user's IP address to find detailed personal facts about the user, such as the user's name, address, birth date, social security number, and e-mail address, within minutes.[8]

(2000) (quoting ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967)).

3. Lawrence Jenab, *Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress*, 49 U. KAN. L. REV. 641, 643 (2001).

4. *Id.* at 643-44.

5. Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 295 (2001). Examples of ISPs include America OnLine (AOL) and Earthlink.

6. *Id.* at 296.

7. Jenab, *supra* note 3, at 644.

8. Jessica J. Thill, *The Cookie Monster: From Sesame Street to Your Hard Drive*, 52 S.C.

B. Cookies and Clickstreams

Another common method of surreptitiously collecting data from users is through the use of small text files commonly known as cookies.[9] Web sites place these files on the computer hard drives of Web site visitors during Internet transactions.[10] A cookie file contains a unique identification number which allows a Web site to recognize and distinguish the user in subsequent visits to the site.[11] Cookies also typically store information such as user preferences, the type of browser software or operating system used, installed plug-ins, and password or login information which allow for easier Web site browsing by the user in future visits.[12] However, cookies have a dual-personality potential because they can abrogate an individual's privacy in cyberspace by collecting information regarding the user and his or her behavior.[13]

Cookies accomplish their darker-sided agenda in several ways. First, a Web site can retrieve cookies at a future time.[14] When the Web site does this, the cookie can disclose a detailed list of all Web sites that a specific computer visited within a particular time frame.[15] Embedded within these cookie files may be telltale information that can identify a user personally, such as a user's name,

---

L. REV. 921, 923 (2001). These transactions are usually invisible to the individual user on the Internet.

9. Helms, *supra* note 5, at 297.

10. According to a Business Week/Harris Poll telephone survey of 1014 adults conducted in March 2000, sixty percent of computer users had never heard of cookies. Heather Green et al., *Business Week/Harris Poll: A Growing Threat* (March 20, 2000), *available at* http://businessweek.com/2000/00_12/b3673006.htm.

11. Anna E. Shimanek, *Do You Want Milk with Those Cookies?: Complying with the Safe Harbor Privacy Principles*, 26 J. CORP. L. 455, 459 (2001).

12. Thill, *supra* note 8, at 923.

13. Rachel K. Zimmerman, *The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-first Century*, 4 N.Y.U. J. LEGIS. & PUB. POL'Y 439, 443 (2000-01). Cookies can be categorized into four basic types: visitor, preference, shopping basket, and tracking. Visitor cookies, also referred to as counters, record the number of times a specific computer visits a Web site. Preference cookies, as their name suggests, save Web page settings chosen by the user, such as specific colors or stocks in a user's personal portfolio. Shopping basket cookies assign the user an identification number in order to maintain a record of items the user selects while shopping at the site. Tracking cookies, the variety that predominantly exhilarate direct marketers and distress privacy advocates, assign an identification value upon an initial visit to a Web site containing a banner advertisement and subsequently track other sites visited by the computer bearing that unique identification value. *See* Nelson A. Boxer, *Are Your Corporation's Cookies Private?*, CORP. COUNS. 1 (May 1999).

14. *See, e.g.*, Zimmerman, *supra* note 13, at 443. For a real-time example of some data a simple cookie file can accumulate, see http://www.junkbusters.com/cgi-bin/privacy (demonstrating that a simple mouse click transmits more information than most surfers realize).

15. *Id.*

password, e-mail address, and other personal information.[16] In the past, only the Web site that placed the cookie could read the file; however, now the use of cookie sharing between sites or the use of placement ads by the same ad agency allows cookies from multiple Web sites to be aggregated to create a comprehensive personal profile of an individual user.[17] Second, some cookies have the capability to record the Web site from which a user came, the links accessed at the site, and any personal information entered at the site.[18] A Web site may also use these types of cookies in concert with a more efficient, and yet more intrusive, technique for gathering personal data known as "clickstreams."[19] A clickstream is basically a recording of all Web sites a user visits during the same session or connection.[20] Clickstream collections not only gather a list of sites visited, but also the duration spent on each site, purchases made, advertisements viewed, and data entered.[21] Internet service providers usually perform clickstream monitoring, because users have essentially rented a line from the provider to connect to the Internet.[22] Lastly, some cookies may be able to identify the IP address of the computer, which could lead to the ultimate disclosure of the location of the computer used to access the site.[23]

II. COMPETING PERSPECTIVES OF CYBERSPACE MONITORING

A. Pro-Business Aspects

The allure of Web-based marketing is threefold: the ability to collect personal information with unprecedented expanse, detail, speed, and ease, the ability to reduce marketing and distribution costs, and the ability for smaller firms to sell products and collect marketing data.[24]

---

16. *Id.*

17. Shimanek, *supra* note 11, at 460. This process is typically achieved through banner ads owned by the same company. Zimmerman, *supra* note 13, at 445.

18. Zimmerman, *supra* note 13, at 443.

19. Shimanek, *supra* note 11, at 460.

20. *Id.* For an example of how cookies and clickstreams operate in concert to develop detailed information regarding the user's Web transactions, see Jenab, *supra* note 3, at 645.

21. Shimanek, *supra* note 11, at 460. This e-surveillance technique is tantamount in the real world to a person secretly following you as you shopped in brick-and-mortar stores, recording what you reviewed, what you bought, and other information about you and your preferences. Andrew Shen, *Request for Participation and Comment from the Electronic Privacy Information Center (EPIC)* 18, *available at* http://www.epic.org/privacy/internet/Online_Profiling_ Workshop.PDF (last visited Feb. 15, 2002).

22. Zimmerman, *supra* note 13, at 446. Due to a provider's position in the electronic channel and the service they provide, clickstream monitoring is accomplished with relative ease. *Id*.

23. *Id.* at 444. The dangerous potential of gathering this type information was discussed in the previous section of this Note.

24. Shaun A. Sparks, *The Direct Marketing Model and Virtual Identity: Why the United States Should Not Create Legislative Controls on the Use of Online Consumer Personal Data*, 18

Using one or a combination of electronic data collection techniques, marketers can capture not only purchase data when Internet users enter information into Web forms to obtain quotes or complete on-line sales transactions, but also invaluable non-purchase "window-shopping" habits of consumers.[25] Also, each subsequent "click" of the mouse may provide the database marketer with further information about the Web surfer. Electronic collection of the information allows Web sites to collect innumerable pieces of individual information with which to develop a solid profile of a particular Web user, and database marketers can run statistical models or other analytical software programs to quickly assemble target lists.[26] What may have taken weeks or months in paper form may take mere seconds or minutes in its electronic counterpart. Thus, what may have been cost and time prohibitive to many marketers is now quick and simple, encouraging a prudent business to leverage the technology to its fullest advantage by acquiring as much data as possible—the better the profile, the better the prospect.

Many of the traditional costs disappear in Web-based transactions, especially costs associated with targeted marketing campaigns. First, the costs of collecting masses of personal data are reduced, as much of the data is voluntarily given or surreptitiously gathered.[27] Second, marketers can develop more precise profiles of potential customers, thereby customizing mailings and developing one-on-one customer relationships.[28] Marketers, armed with this powerful information, can change product mixes or limit the number of mailings to those customers that they deem most profitable or most likely to purchase.[29] A marketer can then use electronic means to communicate to these customers, further reducing the marketing costs to the business.[30] In many cases, an e-mail or banner ad can substitute for a sales catalog or flyer, the number of customer service representatives can be reduced, and the costs associated with low-response blanket mailings can be eliminated.[31] Efficient and effective data collection and profiling allows businesses to better match the right people with the right products, and at the same time reduces efforts and costs associated with both less-targeted mass mailing campaigns and more-targeted campaigns for which

---

DICK. J. INT'L L. 517, 527 (2000).

25. *Id.* at 529.

26. *See id.* at 528-29. Even seemingly pedestrian demographic data can yield strong individual profiles. "Data triangulation" is a process through which small, singular data items on an individual user (e.g., one's date of birth) are matched to a larger, more complete database (e.g., a public records database) to create complete profiles that are then sold to others, such as direct marketers. Letter from Jason Catlett, President, Junkbusters Corp. to Secretary of Federal Trade Commission, *available at* http://www.ftc.gov/bcp/profiling/comments/catlett.htm (last visited Nov. 17, 2002).

27. Jenab, *supra* note 3, at 649.

28. Sparks, *supra* note 24, at 529.

29. *See id.*

30. *Id*. at 530.

31. *Id.*

businesses amass the same information through more laborious and costly collection techniques.[32]

The Internet also allows companies to efficiently deal directly with the ultimate consumer. As a result, a business can remove many or all of the distribution intermediaries from the chain of distribution, thereby reducing distribution costs to the business. One of the greatest cost advantages to businesses from Internet-based commerce is the ability to reduce the number of people who "touch" the product on its way to the consumer.[33] As a result of the elimination of non-value-added distribution intermediaries, consumers will realize lower prices for goods and increased gains for services.[34]

Technological advances have transformed data collection via Web sites into a relatively inexpensive endeavor, providing a more efficient means of data mining and profiling of consumers and their needs.[35] Because of diminished data collection costs, both small and large businesses can afford to engage in targeted marketing efforts that were once within the exclusive province of deep-pocketed companies with substantial capital commitments to data collection activities.[36] With the advent of the Internet, companies selling personal information number in the several thousand.[37] As a result, procuring information and information services, once left to only the largest of firms, can now be afforded by individuals.[38] Hence, small companies can now conduct target marketing on a level equal with larger companies' target marketing, thereby increasing competition, market efficiency, and ultimately lowering costs.

From the perspective of the database marketer, curtailing data collection increases the risk of stifling the explosive growth and ultimate potential of e-commerce on the Internet.[39] In fact, many economic and legal commentaries indicate that "more information is better" and that placing restrictions upon information flow does not maximize social wealth because restrictions inhibit decisionmaking, increase transaction costs, and encourage fraud.[40] Unfortunately, protecting user privacy becomes a vicious cycle that works

---

32. *See* BOB STONE, SUCCESSFUL DIRECT MARKETING METHODS 102-03 (3rd ed. 1986).

33. Sparks, *supra* note 24, at 530-31.

34. *Id*. at 531. In a free market economy, businesses, under pressure from competition, will pass some or all of the distribution savings to consumers in an effort to capture business through lower prices.

35. *Id.* at 528.

36. Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U.S.F. L. REV. 633, 655 (2000).

37. Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1037 (1999).

38. *Id*. at 1037-38.

39. Sparks, *supra* note 24, at 550. The Internet economy is estimated to grow to $2.8 trillion in 2003, nearly tripling in size in two years. Seth Safier, *Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 VA. J.L. & TECH. 6, 8 (2000).

40. Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2382 (1996).

counter to the Internet's direct marketing potential.[41]

Consumers will feel the adverse impact of personal data collection restrictions in other ways. Collection of data at Web sites also allows an expansive offering of free Web sites that are subsidized exclusively through ad banners.[42] Removing or restricting the ability to collect greatly diminishes the value of the ad to the sponsor.[43] Hence, many of these free Web sites will be unable to command a large enough premium from the advertisers to continue operating the site free of charge to visitors.[44]

B. Pro-Privacy Aspects

Although not specifically enumerated as a fundamental right in the Constitution, Justice Louis Brandeis once described privacy as "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[45] However, even though the right has been recognized within the penumbra of the Constitution of the United States, the Court has also stated that the Fourth Amendment does not provide protection of personal information conveyed to third parties for commercial use.[46] In fact, the First Amendment of the Constitution and the Commerce Clause have been used as mighty swords to "strike down state laws concerning Internet privacy legislation."[47]

Nonetheless, measures to protect the privacy of personal information on the Internet offer substantial individual, economic, and societal benefits that must be

---

41. Andrew Leonard, *Your Profile, Please*, SALON NEWSLETTER (June 26, 1997), *at* http://archive.salon.com/june97/21st/article.html. A study commissioned by the Direct Marketing Association indicated direct marketing sales to consumers jumped from $458 billion in 1991 to $630 billion in 1996. In that same period, direct marketing business-to-business sales rose from $349 billion to $540 billion. Safier, *supra* note 39, at 8.

42. Steven R. Bergenson, *E-commerce Privacy and the Black Hole of Cyberspace*, 27 WM. MITCHELL L. REV. 1527, 1553 (2001).

43. *Id.* Ads certainly are posted to market and sell products, but data collection on individuals who click the ad remains critical as well. This data allows marketers to better understand who "clicks" an ad and also allows marketers to provide target advertising of other products or to employ other methods or channels of advertising to those individuals or groups. This data is quite valuable. One author estimates that one individual's data can be worth up to $500. Shimanek, *supra* note 11, at 461.

44. Bergenson, *supra* note 42, at 1553 (citing Erika S. Koster, *Zero Privacy on the Internet*, COMPUTER LAW 7 (May 1999)). Privacy may also potentially stagnate efforts to prosecute those who engage in criminal behavior in cyberspace. If officials are unable to bring culpable parties to justice by analyzing Web sites visited or cookies deposited, not only are law enforcement efforts abrogated, but also the inclination to commit non-traceable Internet crimes could be exacerbated. Helms, *supra* note 5, at 294.

45. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

46. Edward Fenno, *Federal Internet Privacy Law*, S.C. LAW., Jan.-Feb. 2001, at 36, 38 (citing Smith v. Maryland, 442 U.S. 735, 743-44 (1979)).

47. *Id.*

vigorously protected. First, individuals benefit from the protection of privacy in cyberspace by enjoying the right to be left alone.[48] A 1996 poll conducted by Equifax and privacy scholar Alan Westin indicated that "89% of those polled in the United States were either very or somewhat concerned about privacy."[49] Another survey showed ninety-eight percent of respondents felt their privacy was "substantially threatened by advertisers and marketers.[50] When individuals were queried about Internet privacy, the results spoke once again in favor of personal privacy.[51] Surveys reveal that sixty-four percent of Americans are unlikely to trust Web sites, while ninety percent want the right to control the use of their personal information after collection.[52]

In addition to the overwhelming concern for protecting personal information collected on the Internet, lack of privacy may actually stagnate the e-commerce economy.[53] Today, direct marketing is big business. The industry employs over eighteen million people, is utilized by seventy-seven percent of companies, has grown at approximately twice that of the United State's gross national product, and is expected to generate $30 billion dollars in commerce by 2002.[54] Without the ability to choose (or even know) how much privacy will be maintained on a trip into cyberspace, many surfers may be deterred from visiting the Web. In fact, polls reveal that the privacy concern is the top reason why consumers avoid using the Internet.[55]

Finally, intrusive data collection, coupled with the lack of any meaningful choice regarding protection, could lead to avoidance of the Internet as a free-flowing medium of free speech. People may lie to protect their personal data, refuse to answer questions fearing that their answers will become a record in a marketer's database, or avoid the Internet altogether. Privacy protections, therefore, may also protect against untruthful data and self-censorship.[56]

---

48. Nearly four of five respondents in a recent survey "regard privacy as a fundamental right . . . [similar to] life, liberty, and the pursuit of happiness." Sovern, *supra* note 37, at 1057.

49. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1196-97 (1998).

50. Sovern, *supra* note 37, at 1057. Numerous surveys indicate that online users distrust e-businesses' requests for personal information. Often, as much as twenty-five percent of the time, users will enter false information when prompted for personal details. As a result, databases will become increasingly corrupted with worthless information unless privacy concerns are addressed in cyberspace. *See* Leonard, *supra* note 41.

51. Zimmerman, *supra* note 13, at 448.

52. *Id.*

53. *See* Sovern, *supra* note 37, at 1056.

54. *Id*. at 1047.

55. *Id*. at 1056.

56. *See generally* Bartow, *supra* note 36, at 655.

III. THE STATUS QUO OF THE LEGAL ENVIRONMENT

A. U.S. Law on Internet Privacy

Federal laws only offer limited protection to this new electronic threat to consumer privacy. Although Constitutional claims may lie when the government attempts to collect information on individuals from the Internet,[57] the private sector has received relatively little attention. To date, no comprehensive legislation exists regarding Internet privacy pertaining to a private enterprise's ability to collect personal information from the Internet. Congress has poised itself as a reactionary to the problem, rather than as a composed, proactive legislator. The underlying rationale of Congress's approach is to minimally inhibit the inertia of the massive economic engine of the Internet and to deal only with issues related to privacy as advocated at that moment.[58] However, this approach has created fragmented and sparse protections for specific individuals in particular situations, while creating logical inconsistencies across a regulation base without a conceptual infrastructure to fuse them together.[59] For example, the Video Privacy Protection Act of 1988[60] prohibits the disclosure of titles of videos rented, yet book purchases may be monitored with impunity.[61] Other regulations that confine data protection to specific segments of industry include the "Electronic Communications Privacy Act, . . . the Tax Reform Act, the Freedom of Information Act, the Right to Financial Privacy Act, the Telephone Consumer Protection Act, and the Federal Records Act."[62] In October 1998, Congress inched closer to federal regulation of the entire Internet with the passage of the Children's Online Privacy Protection Act (COPPA).[63] Although the government continues to enact legislation protecting the Internet privacy rights of certain segments of commerce and consumers, eventually the government may be forced to succumb to the social outcries for total privacy protection for all Internet constituents and enact an all-encompassing privacy

---

57. *See* U.S. CONST. amend. IV.

58. *See generally* Sparks, *supra* note 24.

59. *See* Zimmerman, *supra* note 13, at 452-53.

60. 18 U.S.C. § 2710 (2000).

61. Zimmerman, *supra* note 13, at 452.

62. *Id.* at 453.

63. 15 U.S.C. §§ 6501-6506 (2000). This Act is the first piece of legislation to protect an entire category of Internet users. COPPA requires Web sites directed towards children and operators with actual knowledge that they are collecting personal information from children to post a notice on their Web site detailing what information is collected and how it is used. The bill also requires that Web site operators gain parental consent, allow for parental review of the information collected, and allow parents to prohibit further use of the information. The Act also requires Web sites and operators to take reasonable steps to protect the confidentiality, security, and integrity of the collected information. Ethan Hayward, *The Federal Government as Cookie Inspector: The Consumer Privacy Protection Act of 2000*, 11 DEPAUL-LCA J. ART & ENT. L. & POL'Y 227, 239 (2001).

statute.[64]

Congress also attempted to protect personal data in telecommunications by passing the Telecommunications Act of 1996. This Act regulates the use of personal information obtained by telecommunications carriers while transacting with and serving their customers.[65] The FCC interpreted the Act to mean that carriers had to "obtain express permission from customers [an 'opt-in' approach] before using any personal data for certain marketing purposes."[66] That interpretation was recently challenged, and ultimately failed to withstand constitutional scrutiny in *U.S. West, Inc. v. FCC*.[67] The court, applying the *Central Hudson* test,[68] stated that when the government attempts to protect personal data, it must show a proper balancing between the costs and the benefits of legislation restricting use of that information.[69] Under the *Central Hudson* test regulations mandating a formal opt-in mechanism may also be deemed an unconstitutional restriction on commercial speech.

The FTC has also commenced federal actions regarding privacy rights on the Internet, but the central focus has involved deceptive collection techniques in violation of section 5(a) of the Telecommunications Act.[70] The FTC first started its Internet privacy enforcement in August 1998 by charging GeoCities with committing deceptive trade practices in violation of section 5(a) of the Act.[71] GeoCities, Inc. was charged with misrepresenting its information collection

---

64. *See* Bergenson, *supra* note 42, at 1545.

65. Telecommunications Act of 1996, 47 U.S.C. § 222 (1994).

66. Sparks, *supra* note 24, at 540. An "opt-in" approach requires a Web site visitor to affirmatively grant the Web site permission before it can collect information on the visitor. An "opt-out" approach allows the Web site to collect information about the Web site visitor unless the visitor affirmatively tells the Web site that he or she does not want his or her personal information collected. Jenab, *supra* note 3, at 667.

67. 182 F.3d 1224, 1234-35 (10th Cir. 1999).

68. The *Central Hudson* test was used to determine whether a particular governmental regulation violated the First Amendment right to free commercial speech. The Court outlined four questions that must be analyzed in a particular governmental regulation:

> Is the commercial speech concerned with lawful activity, and is the speech misleading?
>
> Is there a substantial state interest in regulating the speech in question?
>
> Does the regulation directly and materially advance that interest?
>
> Is the regulation not overly broad in serving that interest?

If the first question is answered affirmatively, then the rights to lawful speech are balanced against the answers found in the remaining three inquiries. *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York, 447 U.S. 557, 566 (1980).

69. *U.S. West, Inc.*, 182 F.3d at 1239.

70. This part of the Telecommunications Act empowers the Federal Trade Commission to prevent unfair or deceptive acts or practices in or affecting commerce. *See* 15 U.S.C. § 45 (2000).

71. Stephen F. Ambrose, Jr. & Joseph W. Gelb, *Survey: Consumer Privacy Regulation and Litigation*, 56 BUS. LAW. 1157, 1166 (2001) (citing Complaint, *In re* GeoCities, Inc., FTC File No. 9823015 (1999), *available at* 1998 WL 473217 (F.T.C.)).

practices in its privacy statement.[72] This misrepresentation occurred when GeoCities allegedly sold third parties certain information that consumers entered in their application forms to GeoCities without the consumers' consent, even though GeoCities' privacy statement claimed it would not do so without first obtaining consumer permission.[73] Although GeoCities denied all charges, the case was settled in February 1999. The consent order outlined revisions to GeoCities' data information and collection practices, including disclosures of "(I) what information is collected; (ii) its intended uses; (iii) third parties to whom information will be disclosed; (iv) consumer's ability to obtain access to such information; (v) consumer's ability to remove information from GeoCities' databases; and (vi) procedures to delete personally identifiable information from GeoCities' databases."[74]

State law invasion of privacy claims regarding unauthorized information collection on the Internet, much like federal actions, have failed to materialize into any meaningful privacy haven for Internet users. Usually unauthorized data collection actions materialize under invasion of privacy claims. A claim for common law invasion of privacy may be based upon one of four theories: intrusion upon seclusion, public disclosure of private facts, misappropriation of name or likeness for commercial purposes, or publicity that places another in false light.[75] However, an invasion of privacy claim arising from Internet data collection usually fails because at least one of the requisite elements of an invasion of privacy claim is missing. Intrusion upon seclusion requires the invasion to be highly offensive to a reasonable person.[76] However, courts have not viewed Internet data collection as such an offensive action, reasoning that an individual could foresee data being collected at a Web site.[77] Public disclosure of private facts usually does not prevail in covert Internet data gathering techniques because the tort also requires that the disclosure be highly offensive, a step courts have not taken in this arena.[78] Claims for misappropriation and false light fall even further from the possible realm of a successful tort claim, because these types of invasions of privacy do not apply neatly to the Internet

---

72. *Id.*

73. *Id.* at 1166-67.

74. *Id.* at 1167.

75. W. PAGE KEETON, PROSSER & KEETON ON TORTS, §117 (5th ed. 1984); RESTATEMENT (SECOND) OF TORTS §§ 652B, 652C, 652D, 652E (1984).

76. KEETON, *supra* note 75, § 117; RESTATEMENT (SECOND) OF TORTS § 652B.

77. Helms, *supra* note 5, at 310. For example, in one case, a group of credit card holders filed a class action suit against the credit card issuer for its alleged intrusion into the cardholders' seclusion. The cardholders' complaint arose because the issuer collected data from the cardholders' use of their credit cards and subsequently rented that information to third parties. The Illinois appellate court dismissed the cardholders' suit based on the fact that the information the issuer had collected and rented was "voluntarily" given and thus the act did not constitute an impermissible intrusion into the cardholder's privacy. Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1353-55 (Ill. Ct. App. 1995).

78. Helms, *supra* note 5, at 311.

data collection issue.[79]

By far, the most publicized state law privacy claim involved DoubleClick, Inc.[80] DoubleClick, a large Internet advertising agency linked to millions of Internet users, announced in January 2000 its plans to merge its non-personally identifiable database information with its Abacus Online database, a database containing enormous amounts of personally identifiable information.[81] This merger would have enabled DoubleClick to link users' names with their clickstream data.[82] Litigation ensued, attacking DoubleClick's use of cookies, clickstream surveillance, and practice of obtaining personal information without consumer consent. Among the state claims filed against DoubleClick were "Trespass to Property, Invasion of Privacy, Violation of Unfair Trade Practices Acts, Unjust Enrichment, and violation of various Consumer Protection Acts."[83] Ultimately, DoubleClick decided against the data merger, and the case was never fully litigated in a court of law.

B. The European Approach to Privacy on the Internet

The European community has been far more progressive than the United States in the protection of personal information in cyberspace, enacting its comprehensive Data Protection Directive ("Directive") in 1995.[84] The Directive, which took effect in October 1998, and binds all fifteen-member nations of the European Union (EU), makes no distinction between on-line and off-line environments.[85] To comply with the Directive, each member state must enact

---

79. A claim for misappropriation would require that the appropriation be for the value of an individual's personal information. The Illinois appellate court, for example, held that the unauthorized sale or use of an individual's personal profile for marketing purposes had value only because it was associated with the other names on the list. The name itself had no intrinsic value, but the list owner created value through the process of list compilation. Thus, the list owner did not deprive the individual of the value of his or her personal data. *Dwyer*, 652 N.E.2d at 1356. Recovery on a false light claim would only be reasonable when the account, if true, would have been actionable as an invasion of privacy. KEETON, *supra* note 75, § 117.

80. Courtenay Youngblood, *A New Millennium Dilemma: Cookie Technology, Consumers, and the Future of the Internet*, 11 DEPAUL-LCA J. ART & ENT. L. & POL'Y 45, 53 (2001).

81. Shen, *supra* note 21, at 17. Abacus Direct Corporation is an offline company which possesses credit card numbers, personal addresses, telephone numbers, information about household incomes, family compositions, and other information on consumer habits. The power of these companies' data gathering capabilities is astounding. For example, in December 1998, DoubleClick placed cookies with forty-eight million Internet surfers in the United States. Abacus held more than eighty-eight million five-year buying profiles. Combining these data stores would have yielded profound knowledge of personally identifiable online behavior. *Id.*

82. Youngblood, *supra* note 80, at 53.

83. *Id.*

84. James T. Sunosky, *Privacy Online: A Primer on the European Union's Directive and United States' Safe Harbor Privacy Principles*, INT'L TRADE L.J. 80, 82 (2000).

85. *Id.* at 82. The European Union (EU) is a union of fifteen independent countries that

legislation that accomplishes the following objectives: the information collector must obtain consent from individuals before personally identifiable information is collected and used; the information collector must obtain consent from the individual before the information is transferred to a third party (opt-out provision); the information collector must disclose the purpose behind the collection of data; the information collector must provide individuals free access to data about themselves; and the information must provide individuals with a mechanism for correcting false information.[86]

IV. ANALYSIS OF THE CURRENT SELF-REGULATION APPROACH

A. A Coasean Perspective on Privacy Rights

In his seminal article, *The Problem of Social Cost*, Ronald Coase argued that in a world with no transaction costs, it does not matter with whom the property right exists, as people will bargain to attain the right if the cost to attain the right does not exceed the bargained-for price.[87] As a result, governmental intervention is unnecessary.[88] If individuals value their privacy but that right is held by the e-businesses, then individuals can purchase the right from e-businesses. However, if the businesses feel the right is worth more than the individuals are willing to pay (i.e., how much they value their privacy), then the businesses will retain the right.[89] The result is an efficient allocation of resources, regardless of who "controls" the property rights to the personal information. In essence, privacy of information is appropriately valued and given its due consideration in the marketplace.

One reason for self-regulation's failure is a lack of information and understanding of what actually transpires during an Internet visit.[90] In general,

---

actively collaborate to enhance the political, social, and economic realms of their countries. Current member include: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, and the United Kingdom of Great Britain and Northern Ireland. *See* European Union Official Web Site, *at* http://www.europa.eu.int./index_en.htm (last visited Nov. 11, 2002).

86. Bartow, *supra* note 36, at 662; Joel R. Reidenberg, *Restoring America's Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 783-84 (1999).

87. One article summarizes the Coase Theorem as follows:

> If the parties to any actual or potential social arrangement could enter into marketplace transactions with no transactional impediments (costs) of any kind, they would always agree to rearrange their respective obligations in a manner that would lead to a net increase in the productive value of their arrangement if such an increase were possible. This would hold true irrespective of any rule of liability in effect at the time.

Michael I. Swygert & Katherine Earle Yanes, *A Primer on the Coase Theorem: Making Law in a World of Zero Transaction Costs*, 11 DEPAUL BUS. L.J. 1, 2 (1998) (footnote omitted).

88. *Id.*

89. Sovern, *supra* note 37, at 1067.

90. Obtaining accurate information on current information collection and privacy practices

the individual Web user is blissfully ignorant of the covert data collection experience and many Web sites offer little or no information regarding their collection practices.[91] Without adequate knowledge, the individual usually operates under the false assumption that his or her privacy is protected. Thus, even if transaction costs were removed from the equation (necessary to perfect Coase's theorem), the unequal knowledge of the true nature of the situation prevents the Coasean irrelevance theory from gaining a foothold.[92] In fact, a Business Week/Harris poll conducted in March 2000 indicates that sixty percent of Internet users have never heard of cookie files.[93] Thus, efficient resource allocations cannot be realized because of the consumer's lack of knowledge regarding the collection practices of most Web sites. Without such knowledge, no bargaining regarding privacy of information ensues, and an efficient balance between data collection and privacy is improbable.

B. An FTC Perspective on Self-Regulation

Currently, the U.S. Congress has treated Internet transactions in a laissez-faire fashion, allowing the Internet economy to flourish and set its own terms regarding the collection of data. Initially, the FTC seemed comfortable with the self-regulatory environment.[94] Over time, however, mounting pressure from the EU and the apparent failure of self-regulation were reflected in the FTC's progress report on the industry. The FTC's 2000 report regarding the Internet and privacy asked Congress for expanded regulatory powers and even suggested a legislative proposal on Internet privacy be made to Congress.[95] Although the proposal was ultimately rejected, it remains clear that the FTC has implicitly announced the failure of self-regulation as a mechanism to balance commerce and privacy interests on the Internet.

C. A European Union Perspective on the Current Self-Regulation Approach

The current absence of data collection standards in the United States, which would afford individuals privacy, may pose a formidable threat to U.S. economic ties to our European brethren. The European Directive, a comprehensive body

---

for every Web site a user may visit would be costly and overly burdensome in today's environment. These high costs work against a private marketplace solution. *See generally* Swygert & Yanes, *supra* note 87, at 11-12.

91. Steven A. Hetcher, *The Emergence of Website Privacy Norms*, 7 MICH. TELECOMM. & TECH. L. REV. 97, 99 (2000-01). The McDonough School of Business at Georgetown University reported the results of its Internet privacy survey in March 1999. The survey found that ninety-three percent of commercial Web sites surveyed collected personal information from consumers, but only sixty-six percent of these Web Sites posted disclosures about their information gathering practices. Charles L. Kerr & Oliver Metzger, *Online Privacy: Changing Exceptions—Changing Rules*, 632 PLI/PAT 147, 156 (2001).

92. Swygert & Yanes, *supra* note 87, at 3-5.

93. Jenab, *supra* note 3, at 647.

94. Bartow, *supra* note 36, at 668.

95. *Id*. at 668; Thill, *supra* note 8, at 930.

of legislation that fiercely protects the privacy rights of the EU's citizenry, makes clear that its member states will not tolerate e-commerce exchanges with countries that could potentially undermine those rights.[96] The result of non-compliance by U.S. Internet businesses could be devastating if they are not permitted to engage in such transactions as transatlantic personal finance transactions, sale of goods, credit checks, and travel reservations.[97] The bottom line is that a staggering $1.5 trillion of transatlantic commerce is at stake.[98]

Fortunately, the United States has convinced the European Union, at least for now, to accept its proposal for a safe harbor provision.[99] The provision, reluctantly adopted by the EU, helps ensure that U.S. organizations satisfy the Directive's standards while maintaining the self-regulatory scheme that U.S. legislators currently prefer.[100] Under the agreement, the U.S. Department of Commerce will establish and maintain a public list of companies and other organizations that publicly declare adherence to the Safe Harbor principles.[101] These principles basically assure other countries that the businesses on the Safe Harbor list afford protection similar to that of the Directive, without the entities' country explicitly adopting the Directive.[102] The continued viability of the Safe Harbor provision will depend upon its success in protecting individual privacy to the EU's satisfaction. Thus, U.S. commerce has dodged the economic bullet for present moment.

---

96. Bergenson, *supra* note 42, at 1551. The Directive is a concerted effort by member states to protect privacy rights of their citizens. Basically, the Directive requires each member state to enact privacy legislation which complies with the Directive's privacy standards, maintain a national supervisory and enforcement authority, and to create a public registration system by requiring entities or individuals processing personal information to notify the member state's supervising authority, prior to any data collection. Sunosky, *supra* note 84, at 82.

97. Bergenson, *supra* note 42, at 1551-52. For a country to be approved under the Safe Harbor provision, its program must adhere to the Directive's basic principles which include:

1) Notice to the Web visitor of data collection practices
2) Ability of a visitor to choose not to partake in the data collection (an opt-out provision)
3) Information collected from a Safe Harbor Web site can only be transferred to a Safe Harbor third party or a contract with the same effect
4) Visitors have access to collected data
5) The visitors have a mechanism to correct inaccurate data, and the Web site business must have a dispute resolution process.

Sunosky, *supra* note 84, at 86-88.

98. *Id.*

99. *Id.* at 84-85. *See also* THE PRIVACY LAW SOURCEBOOK, RECENT DEVELOPMENTS: SAFE HARBOR ARRANGEMENT (EU-US) 517 (2001). A safe harbor is "a provision . . . which gives . . . protection as long as efforts were made to comply with the law." BLACK'S LAW DICTIONARY 1336 (6th ed. 1990).

100. Sunosky, *supra* note 84, at 85.

101. *See* THE PRIVACY LAW SOURCEBOOK, *supra* note 99, at 517.

102. Sunosky, *supra* note 84, at 85.

V. PROPOSED SOLUTIONS

A. Adoption of the EU Directive

One of the proposed solutions to the Internet privacy problem is the adoption of the EU Directive in the United States. Although the adoption of the EU mandate remains a plausible solution to the cyberspace data collection dilemma, it comes at a price that Congress has been hesitant to pay.[103]

In addition, some real-world problems accompany the complete adoption of the EU Directive. First, the Directive contains stringent requirements for businesses to meet and for the government to enforce. These requirements may be too stringent, creating inefficiencies and overburdening e-businesses as the environment changes from under-protection to over-protection of privacy rights. It is questionable whether our personal information is worth that much. Second, although notice and knowledge are key for judicious decisionmaking by consumers and a lynch-pin in the Coasean scheme of efficient economic allocations, e-businesses may provide notice that is beyond a typical consumer's understanding or patience. For example, to avoid litigation, businesses may attempt to cover for every possible contingency with a long and complicated list of notices saturated in legal parlance. Although a business may be in technical compliance with the regulation by giving adequate notice, few Internet users will be able to read and understand the notice. This phenomenon is commonplace in today's world, as casual glance at the back of a hockey ticket, a parking garage slip, or a movie theater pass will demonstrate. Very few people read the notice on the back of a hockey ticket and requiring the notice does not change real world behavior.[104] In these instances, it can hardly be said that users were given knowledge in any meaningful manner.

B. Licensing

Some commentators suggest that personal data should be licensed.[105] Under this proposed solution, individuals would be given property rights in personal data. However, this solution may have a detrimental impact upon commerce by inhibiting transactions, encouraging fraud, and increasing transaction costs.[106] In addition, defining what information is owned by the individual or determining how to deal with information already in databases are additional complexities

---

103. The United States has claimed differences between the judicial systems of the United States and the EU necessitate adoption of the Safe Harbor provision rather than the EU Directive. In the United States, it is easier to bring a successful action in court than it is in European courts. Consequently, the United States' open and flexible court system coupled with moderate legislation, as opposed to comprehensive, heavy-handed legislation, will adequately protect an individual's privacy. *See* THE PRIVACY LAW SOURCEBOOK, *supra* note 99, at 517.

104. Walker, *supra* note 2, at 140.

105. *See generally* Kalinda Basho, *The Licensing of Our Personal Information: Is It A Solution to Internet Privacy?*, 88 CAL. L. REV. 1507 (2000).

106. *Id*. at 1526.

that must be resolved under such a system. Should a person's name, openly published in a phone book, really be information that a business must buy from an individual?

C. Tort Law Expansion

Another solution proposed is to expand state tort law to encompass Internet data collection practices.[107] This could be accomplished, for example, by expanding the "reasonable expectation of privacy" to include transactions over the Internet.[108] However, state regulation creates its own subset of problems in this area. Jurisdictional issues and variations in state laws will cause consumer confusion and inconsistency across cyberspace, a medium that transcends state lines.

D. Technology-based Solutions

Yet another proposed solution is rooted in technology itself. Privacy enhancing techniques (PETs), often based on pseudonyms or remailers to disguise identities of Internet users, rely on technological safeguards to protect against unwanted data collection while surfing the Web.[109] However, reliance upon PETs and similar techniques has shortcomings as well. Since technology is always changing, the extensive use of PETs may engage individuals and businesses in a large-scale cat and mouse game, attempting to gain advantage over the opposing side by inventing techniques that defeat the mechanisms of the other side.[110] Additional burdens may also be placed upon the technology to adapt to new Internet methods and access channels, such as cellular telephones. Buying the initial requisite hardware and software and constantly updating for technological advancements involves costs for both businesses and individuals. Also, keeping apprised of the upgrades needed to protect their personal information may be onerous for individuals. Lastly, PET's would not increase

---

107. *See, e.g.*, Zimmerman, *supra* note 13, at 458.

108. *Id*.

109. *See* Helms, *supra* note 5. Generally, remailers create anonymity for the user by masking or replacing domain names or other identifying information attached to e-mails. For example, remailer technology would change the address "johnsmith@aol.com" to "az3234@remailer.com." Proxy surfing allows a user to surf the Internet through another's server. This server acts as a substitute TCP/IP address, which will be displayed as the user's address to Web sites collecting the data. Thus, the user's true address is cloaked from the prying eyes of the Internet. For an expanded discussion on PETs, *see id.*

110. For example, Intel was contemplating the use of a controversial user identification number embedded within its then upcoming processor chip. However, in April 1999, the company, in the wake of boycotts and denouncements from political leaders (due to the number's ability to decimate privacy), decided against including the identification number feature in its new chip. Declan McCullagh, *Intel Nixes Chip-Tracking ID*, WIRED NEWS, Apr. 27, 2000, *at* http://www.wired.com/news/politics/0,1283,35950,00.html.

a user's knowledge of what and how information is collected and used.[111] Without that knowledge, users will be ill-equipped to decide to whom they wish to give information.

E. Seals

Another proposal to solve the Internet privacy dilemma harnesses optional seals to identify Web sites that adhere to the seal provider's privacy principles.[112] "The most notable examples of such initiatives are TRUSTe, Better Business Bureau Online, and SecureAssure."[113] Participating Web businesses donning a seal assure the site's visitors that the site's privacy policy and practices conform to the privacy policy standards outlined by the seal-sponsoring organization.[114] For example, the privacy policy of the Better Business Bureau's Privacy Program includes "verification, monitoring and review, consumer dispute resolution, a compliance seal, enforcement mechanisms and an educational component."[115] A 1998 poll indicated that twenty-eight percent of respondents who would have originally not provided personal information in order to receive free pamphlets or coupons would be more likely to provide information to a Web site if the site had a privacy policy, and fifty-eight percent said they would be more likely to provide personal information if the site contained both a privacy policy and a seal issued from a reputable organization such as the Better Business Bureau.[116] Seal programs also seem to pass EU muster, because the programs' privacy policies meet the rigorous demands of the Directive.[117]

---

111. As one article noted: "Privacy isn't just about fancy software. It's also about making sure that information is being used in the ways companies had promised. Technology won't protect people from privacy invasions. Only people do that." Green et al., *supra* note 10.

112. Hayward, *supra* note 63, at 232-33.

113. *Id.*

114. *Id.*

115. COUNCIL OF BETTER BUSINESS BUREAU, INC., ABOUT THE PRIVACY PROGRAM, *at* http://www.bbbonline.org/business/privacy/index.html (last visited Oct. 10, 2002).

116. *See generally* Lorrie Faith Cranor et al., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy* (Apr. 14, 1999) *at* http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.html.

117. Shimanek, *supra* note 11, at 468. For example, Principle III of the BBBOnline Code of Online Business Practices suggests that Web sites and online advertisers bearing their privacy seal should:

> [P]ost and adhere to a privacy policy that is open, transparent, and meets generally accepted fair information principles including providing notice to what personal information the online advertiser collects, uses, and discloses; what choices customers have with regard to the business' collection, use and, disclosure of that information; what access customers have to the information; what security measures are taken to protect the information, and what enforcement and redress mechanisms are in place to remedy any violations of the policy. The privacy policy should be easy to find and understand and be available prior to or at the time the customer provides any personally

Unfortunately, voluntary seal programs have faltered as a feasible solution to the privacy issue for several reasons. First, the programs are completely voluntary, thus severely limiting the number of Web sites that fall under the purview of a seal program.[118] Also, in many cases, a seal program's sponsors, who established and fund the seal program, are also seal program participants.[119] In addition, although the seal programs boast of enforcement mechanisms, the only real penalty that the seal issuer can assess against a violator is the revocation of the seal.[120] Lastly, it is difficult to uncover seal participants who violate the privacy policies of a program, which further undermines the effectiveness of the seal programs.[121]

VI. A NEW PROPOSAL

Current seal programs are voluntarily joined, seldomly monitored, and lax in enforcement for non-compliance.[122] However, the underlying concept of seals

---

identifiable information.

COUNCIL OF BETTER BUSINESS BUREAU INC., CODE OF ONLINE BUSINESS PRACTICES FINAL VERSION WORKS, *at* http://www.bbbonline.org/Reliability/Code/principle3.asp (last visited Nov. 10, 2002). Although the European Union publicly declared these seal programs were acceptable when the Web sites complied with the policies of seal providers, it also noted that the discretionary nature of the programs were not adequate to protect privacy interests. Shimanek, *supra* note 11, at 468.

118. *See generally* COUNCIL OF BETTER BUSINESS BUREAU, INC., *supra* note 115.

119. Hayward, *supra* note 63, at 233. Jason Catlett, President of Junkbusters, notes that a seal program's non-profit status is of no import to ensuring privacy and compliance, stating that "[t]he nonprofits are essentially industry-funded PR and lobbying efforts, and they're up front about the fact that their main aim is to stave off legislation." THE INDUSTRY STANDARD: PRIVACY? WHAT'S THAT?, *at* http://www.thestandard.com/article/display/0,1151,17385,00.html [hereinafter THE INDUSTRY STANDARD] (last visited Nov. 10, 2002).

120. Hayward, *supra* note 63, at 233-35.

121. *See generally id.* A survey conducted by AT&T Labs in November 1998 revealed that "[a] joint program of privacy policies and privacy seals seemingly provides a comparable level of user confidence as that provided by privacy laws." The following responses were given by users who were unsure or would not give personal information (such as name and address) to a Web site in order to receive free pamphlets and coupons on hobbies of interest to the user:

1) 48% said they would be more likely to provide it if there was a law that prevented the site from using the information for any purpose other than processing the request.
2) 28% said they would be more likely to provide it if the site had a privacy policy.
3) 58% said they would be more likely to provide it if the site had both a privacy policy and a seal of approval from a well-known organization such as the Better Business Bureau or the AAA.

Cranor et al., *supra* note 116.

122. Zimmerman, *supra* note 13, at 457. In a recent investigation, Interhack, a security and privacy firm, discovered four retailers who, contrary to their privacy policies, shared names, addresses, and other information collected at their sites with a third party marketing company

appears to be a reasonable way of notifying Web visitors of the site's particular collection practices. A modified "seal-type" program may resoundingly answer the cyberspace privacy issue, creating an amendable solution for both e-business and user privacy interests. However, merely codifying an existing seal program is not enough; a new seal-type program must also address the other deficiencies entrenched in current seal programs.[123]

The following is a suggested privacy program for all e-business Web sites. Although the discussion is not exhaustive of the expansive detail necessary to implement such a program, the features listed are the substantive elements of a federal program designed to protect privacy at a market-efficient level.

A. The "Privacy Toolbar"

The nucleus of the proposed privacy program is a graphical user interface[124] coined the "privacy toolbar." This toolbar would be similar in appearance to the visual toolbars of many software applications and operate in a similar fashion. The toolbar would comprise a series of buttons, each containing a picture icon and representing a "core element" of a privacy policy. Thus, the particular buttons that appear on a Web site's privacy toolbar would depend on its treatment of an individual's information. However, every toolbar would derive from the same pool of icons, furthering uniformity and reliability while allowing each toolbar to be custom-fit to the site's data collection practices.[125] The toolbars should also have the same basic construction and be placed in a conspicuous location on the site. Furthermore, the icons should be readily apparent and internationally recognizable, in a similar manner to road signs, and serve the same purpose: imparting information about what lies ahead for the person who utilizes the Web site. As a result, these iconic buttons would serve as visual management guides to an individual visiting a particular Web site.

To be a useful reference for users, however, the toolbar should contain a limited number of buttons.[126] Although the way in which information is collected and used appears limitless, rational categories could be generated to serve as

---

named Coremetrics. Additionally, two of the four retailers carried the TRUSTe seal, that supposedly indicates the site is committed to the practice of fair information collection practices. *See* THE INDUSTRY STANDARD, *supra* note 119.

123. *See* Hayward, *supra* note 63, at 233-35.

124. A graphical user interface is a means of operating a computer by manipulating picture icons and windows with the use of a mouse. CHARLES E. PUFFENBARGER, DICTIONARY OF COMPUTER TERMS (1993).

125. Conversely, under the guise of current seal programs, the same seal can represent differing privacy practices. It would be very difficult to capture the core elements of a site's privacy policy with only one common symbol. The privacy toolbar would use "mass customization" to tailor the toolbar around specific information collection practices, thereby imparting more information than a single seal.

126. If too many buttons are used, the toolbar may become self-defeating, complicating the message to such an extent that it is subsequently disregarded by a large number of users.

definitive guideposts for Web surfers.[127] These categories should revolve around fundamental privacy dimensions: what information is collected/used and how it is collected/used.[128] To disclose what types of data are collected, for example, a button may display a medical cross for medical information. To convey how the information is used, for example, a toolbar may contain a button depicting two persons facing each another to indicate that the site distributes the information it collects to third parties. Another button may display a safety pin, indicating that the site has data security measures in place to protect the data during transfers. Still another site's toolbar may contain a button with a checkmark, indicating that the site allows users to review the data that has been collected about them and make corrections to that data. Ultimately, the buttons on any particular toolbar would change commensurate with the particular Web site's information collection practices.

Of course, the categorization of privacy practices will likely spur the stiffest of challenges. If categories are defined too narrowly, consumer confusion will result from the countless categorizations. Alternatively, if categories are defined too broadly, consumer confusion will ensue as to what a particular site's collection practices really entail. In addition, broad categorizations will inhibit smaller, more innocuous information gatherings on Web sites if they are grouped in the same category as sites that commit greater intrusions into personal privacy.

The privacy toolbar is designed to compress a complex privacy policy into simple icons in order to facilitate a user's understanding of a site's privacy policy. By design, the toolbar should not supplant the posting of a privacy policy in full text. In fact, the toolbar may encourage Web sites to remove layers of complexity that cloak their current privacy policies and create easy-to-read, consumer-friendly textual privacy policies that clearly and fully explains their information collection practices.

Educating the Internet public regarding the meaning of the buttons located on the toolbar may require a formal program that utilizes various media. Thus, successful implementation of the program may require governmental spending to help educate the e-community about the toolbar program, its purpose, and its limitations.[129] In addition to a formal campaign to impart general learning, the toolbar itself should be an indispensable tool for informal self-education. Each button on the toolbar, therefore, should be a functional button. When depressed ("clicked"), the button should link the user to a site that explains the element in

---

127. One possible method of categorizing "core elements" may be via the FCC's Fair Information Practices Principles (FIPPs). The five FIPPs are (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress. Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2049 (2000). Each element or subelement of the FIPPs could be represented by an icon in a button on the privacy toolbar and would be precisely and unambiguously defined.

128. *See* Green et al., *supra* note 10.

129. "[W]hen we asked respondents about online privacy seal programs *without mentioning any specific brand names*, their responses suggest that they do not yet understand how Internet seal programs work." Cranor et al., *supra* note 116.

detail as it pertains to the site and any steps the user may need to take to effectuate that element. In addition, all toolbars would include a help button, which would link to an FTC Web page not only describing in detail the general mechanics and definitions of the toolbar program, but also a place to report suspected violators of the program. Considering the power of the Internet and user familiarity with toolbars, the self-education program may yield successful results without pursuing secondary educational avenues.

B. Notice Before Data Collection

To effectively protect privacy and yet permit businesses to collect information at the first possible moment, the toolbar should be displayed on the Web site's page prior to collecting data. Three alternatives are available to Web sites under this requirement. One possibility is that a Web site will display only a home page privacy toolbar, which will be the uppermost boundary for data collection for other pages associated with that home page. However, this alternative may be susceptible to circumvention of notice if links are used to bypass a Web site's home page. However, a program code may be able to adequately address the issue by first determining from what site the user came, and then posting a dialog box displaying the toolbar for that particular page.[130]

Web sites must also reflect the collection practices of advertisement banners placed on their Web pages. Either the Web site's home page becomes the privacy limit for banners placed on their pages, or the banners themselves must feature a privacy toolbar. Although the process may seem cumbersome at first, the inconvenience should be no more than that posed by current pop-up windows or dialog boxes today.[131]

Alternatively, if different collection practices exist within a Web site, or home page toolbars prove ineffective, then each page must be affixed with a toolbar commensurate with the collection practices of that page. Of course, each page must conform to the toolbar buttons it posts or risk violating the program. This strategy is helpful if the Web site is highly complex, or the Web site wants to show the content of part of its site to entice users to agree to their information collection practices on subsequent pages. Again, the site that has a different collection practice must reflect that practice with an appropriately marked toolbar, and the user must affirmatively "click" past the toolbar before the site starts collecting data at that level.

Finally, if the Web site wishes to collect data when the user accesses the site, then the site must provide the toolbar in a pop-up dialog box prior to entry to the Web site. This would be tantamount to dialog boxes indicating that the individual is leaving a secured site and moving to an unsecured site, and then

---

130. Of course, the information noting from where the user came could be used, but could not be permanently collected unless the user agreed to its collection through the dialog box.

131. Considering the number of people that are concerned about privacy, this should not be an issue. In addition, browsers may be set to allow pages that meet certain privacy conditions to pass through seamlessly without clicking a dialog box every time.

requiring the individual to affirmatively respond by clicking either the "Yes" or "No" button.

Regardless of the approach allowed, the rationale is clear: sites must not collect data prior to the posting of the privacy toolbar, thereby providing, at a minimum, constructive notice of their privacy practices to Web users.[132] Concurrent or post-collection notification frustrates the efficient market valuation of privacy by individuals accessing the site. Individuals must be allowed to determine whether they wish to surrender their privacy before it is actually relinquished. The market must make that value determination.

C. ISP Requirements

Although privacy toolbars end unauthorized Web site data collection methods, ISPs still hold the dangerous "clickstream" surveillance potential.[133] Since the problem lies upstream from Web sites, the issue must be appropriately addressed or risk eviscerating the efficacy of the proposed privacy program. However, the notice rationale used for Web sites and ad banners can be applied to ISPs as well. Hence, ISPs must conspicuously post privacy toolbars (or the icons themselves) in their on-line and off-line subscription agreements, using the same toolbar protocol as posted on Web sites.[134] This approach would possibly allow the customer to choose between his or her privacy rights and lower subscription rates, since ISPs may charge higher rates to compensate for the lost revenues associated with the collection, use, and sale of information.[135]

---

132. This system, however, may be tantamount to a formal opt-in mechanism, and may run afoul of a First Amendment Constitutional challenge. *See supra* note 67 and accompanying text.

133. Helms, *supra* note 5, at 297; Kang, *supra* note 49, at 1224. Prior to the merger of America Online (an ISP) and Time Warner in January 2001, Jerry Berman, Executive Director of the Center for Democracy & Technology, and John Morris, Director of the Broadband Access Project, commented:

> The proposed merger of AOL and Time Warner does highlight both the increased risks for privacy problems as the Internet evolves, and the great potential for self-regulatory efforts to enhance privacy protection. Both AOL and Time Warner have access to significant amounts of personal data about their subscribers. For AOL, this includes for example, information about online service subscribers, AOL.COM portal users, and ICQ and instant messaging users. Time Warner has access to information about ranging from cable subscriber usage to magazine subscriptions. The specter of the merged companies pooling all of their information resources, and then mining those resources for marketing and other purposes, should be cause for concern.

Jerry Berman & John Morris, Prepared Statement Before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Communications (Mar. 2, 2000), *at* http://www.cdt.org/testimony/000302berman.shtml.

134. Although occupying different hierarchical levels in cyberspace, privacy issues challenging Web sites are also present with ISPs.

135. *See generally* Youngblood, *supra* note 80; Shimanek, *supra* note 11. List vending, which is the process of compiling and selling information gathered on individuals to other companies, is

However, the leverage of ISPs versus consumers may be too great, and therefore no ISP of any size would offer the choice of additional privacy.[136]

However, under the privacy toolbar program, ISPs could recover lost revenues from foregoing information collection by offering scaled subscription rates. Under Coasean theory, a consumer that values his or her privacy beyond what the right costs would "buy" the right to keep his or her information private. Hence, ISPs could offer either hierarchical levels of privacy protection at scaled subscription rates[137] or charge a higher rate for access to all subscribers, provided the ISPs do not unfairly charge for elevated levels of privacy to dissuade people from choosing more privacy.[138] If an ISP receives higher subscription rates to compensate for the lack of personal information to sell or use, the ISP's revenue stream will be equivalent, and thus the ISP has no incentive to favor one choice over the other.

D. Mandated Participation

Under a statutory toolbar program, all U.S. businesses would be required to attain certified toolbars for their Web sites reflective of their data collection practices.[139] Each Web site would be issued a specific toolbar, custom-fit to its privacy practices, and this information, including current collection and use of information, would be recorded in a national registry.[140] This registry would be

---

big business. The Direct Marketing Association reports that over fifty percent of direct marketers use the Internet, and forty-eight percent actively mine the membership rosters of online services providers for data on individuals. Safier, *supra* note 39, at 63.

136. ISPs link users and the Internet, and this leverage may inhibit the market from achieving Coasean irrelevance. As such, legislation may be needed to intervene and enact stronger laws in support of privacy. However, as the number of ISPs increase, this risk decreases.

137. This approach provides the clearest notice to a customer about privacy practices because he or she affirmatively chooses the level of privacy in which he or she feels comfortable operating. Thus, the consumer truly chooses the value of his or her privacy in each instance. This approach can be analogized to the "shopper's cards" issued by some grocers. The grocers, in exchange for data collection on consumer purchases, give price discounts to those who use the cards. If privacy is paramount, the same goods are available to the shopper who chooses not to use a card, albeit at higher prices. *See, e.g.*, Consumers Against Supermarket Privacy and Numbering, Kroger: What Savings?, CASPIAN Shoppers Discuss Kroger "Card Savings," *at* http://www.nocards.org/savings/savingsletterskroger.shtml (last visited Nov. 11, 2002).

138. If necessary, the government could require a complete sealing of an ISP's records of an individual's transactions, allowing disclosure only upon a court order. This requirement, however, is more intrusive than the first alternative and only should be used as a secondary alternative if ISPs fail to allow individuals greater privacy protections in any meaningful sense.

139. Jason Catlett, Corporate President of Junkbusters, a New Jersey privacy protection Web site, commented that privacy seals would be more effective when coupled with strong Federal online privacy laws. *See* Catlett, *supra* note 26.

140. This provision parallels the current practice of voluntary seal programs and the registry kept by the Department of Commerce as set forth in the Safe Harbor agreement with the EU. *See*

used as a reference and an enforcement mechanism. If a Web site's data collection practices fail to conform to the policy as registered with the government, the site will be in violation of the program and subject to penalty. Without legally mandating participation and enforcing the program for Internet privacy, consumer trust in e-commerce will continue to wane.[141]

Also, under current seal programs and the European Directive's Safe Harbor provision for the U.S., businesses are required to conform to a set of privacy principles. A privacy toolbar program would be more amenable to businesses, because it would not interfere with their current business models or collection practices. The toolbar program only requires that e-businesses offer simple and true representations of their information collection practices.[142] It will be business as usual for e-businesses under the privacy toolbar program, albeit with an additional notice requirement.

E. FTC Regulated and Enforced

Congress should designate the responsibility of the toolbar program and its enforcement to the FTC. If buttressed with the appropriate legislation, enforcement is best left to the current governmental experts in the field of cyberspace. The FTC currently monitors privacy issues on the Internet and could make any necessary recommendations to Congress, or be given authority to set administrative rules to help assist with efficient execution of the toolbar program and enforcement process.[143] However, considering the ever-expanding juggernaut of e-privacy, more governmental resources will be essential to effectively tackle enforcement procedures. These resources will need to provide for random audits, complaint investigation, and the administrative duties that will accompany a toolbar program.

Another key element of the statutory regulations is enforcement.[144] To be an effective deterrent against violating the program, the program requires an FTC penalty that, multiplied by the probability of getting caught and found guilty, outweighs the value of the illegal activity.[145] In many instances, the chances of

---

discussion *supra* note 99 and accompanying text; *see also* THE PRIVACY LAW SOURCEBOOK, *supra* note 99, at 517.

141. Shen, *supra* note 21, at 19. An October 1998 study revealed that over seventy-two percent of Americans feel that new laws to protect privacy on the Internet should be enacted. GVU's 10th WWW User Surveys, *at* http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/graphs/privacy/q59.htm (last visited Nov. 11, 2002).

142. The EU Directive mandates that its members follow strict privacy guidelines set forth by the EU. *See* discussion *supra* note 96.

143. *See generally* Hetcher, *supra* note 91.

144. Research conducted by Forrester Research found that ninety percent of Web sites fail to comply with basic privacy principles. Basho, *supra* note 105, at 1522.

145. The usual remedy for violators of the FTC Act is injunctive relief. If the injunction is subsequently breached, then the FTC can impose harsher terms. However, if a company posts a privacy policy and collects information contrary to that policy, then the FTC can impose sanctions

getting caught undertaking unlawful collection practices may be minimal because an individual would not readily discover covert collection practices by culpable businesses. Thus, the penalty for unlawful data collection practices must be high enough to account for the smaller probability of getting caught.

VII. BENEFITS OF THE NEW PRIVACY PROGRAM

A. Least Intrusive Legal Alternative

Privacy toolbars impart information and allow market forces to determine the value of privacy rights versus the commercial value of information collection and use.[146] Consumers, without having to "opt-in" or "opt-out" of complex privacy notices, can use privacy toolbars as easy visual management devices, discreetly leaving sites without complex negotiations regarding information collection and use.[147] This process allows capitalistic forces to operate, yet does not force excessive burdens upon the site to contract with Web site visitors, construct complex legal notices, develop mandated "opt-in" or "opt-out" devices, or develop other methods and mechanisms. Rather, the business can continue to use its current methods of collection, but must affix a notification of its conduct conspicuously on the Web site. Again, market forces, not the legislature, will be the ultimate arbiters of the correct balance between privacy and business needs. Legislation should merely serve as a facilitating device.

In addition, the privacy toolbar program is less likely than more comprehensive legislation to impinge upon a business's right to commercial free speech. The toolbars give notice to prospective Web site visitors of information collection practices, but do not inhibit current collection practices. What will ultimately dictate the level of privacy required is the market's acceptance of more invasive data collection practices in exchange for the value proposition of a particular site.[148]

---

for deceptive practices, including statutory damages, attorney's fees, and economic remuneration. Interview with James Nehf, Professor, Indiana University School of Law—Indianapolis (Jan. 20, 2002).

146. As one commentator noted, "when a 'new' problem is identified in cyberspace, we should initially respond with the lowest, most decentralized level of control possible." Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1026 (Summer 1994). He suggests, and this author agrees, starting with the presumption that the lowest level of controls can adequately resolve the problem, and if not, then ascend the ladder of centralized control until satisfactory results manifest. *Id.* Since self-regulation has not proven successful enough to ensure real privacy protections, we must move up the "control" ladder.

147. Many "opt-out" provisions are not clearly displayed on Web sites, thereby providing individuals little meaningful control over their information. Users must delve into the complexities of the "opt-out" provision to determine their rights, and many are unwilling or unable to do so. This is important, because in "opt-out" provisions the user's information will be collected and used unless the individual takes affirmative steps to be excluded from the site's database. Shen, *supra* note 21, at 27.

148. The same conceptual framework can be applied to ISPs and ad banners as well.

B. Uniformity, Clarity, and Reliability

Under a mandatory privacy toolbar program, all sites would adhere to the same iconic system, and thus consumers would have a clearer expectation of the level of privacy offered at every e-business site. Uniform system metrics will not relegate the consumer to sifting through the mire of inconsistent policies and notices.[149] A button on the privacy toolbar will stand for the same core element on one site as it does another, thereby clearly defining and communicating each element uniformly and consistently across the entire Internet. As a result, Web users can rely upon these toolbar icons to understand what the collection practices of a particular Web site entail. Once consumers learn the meanings of the toolbar buttons, they can grasp the basic practices of any U.S.-based Web site. In addition, icon-type programs have already been applied with some success in the market.[150] Market learning has already been accomplished to some extent, and existing technology can support a mandatory toolbar program in the electronic arena.

C. Ease of Use

The toolbar signifies a readily available store of further information regarding privacy, including definitions of buttons, definitions of terms, and details regarding the site's specific practices. The consumer need not locate hard-to-find privacy policies buried deep within a Web site's numerous pages. In addition to its visibility, the most novice of Internet consumers can also understand the toolbars affixed to Web sites, as opposed to potentially drowning in the legalese and complexities of formal notice disclosures, "opt-ins," or "opt-outs."[151] As a result, many of the barriers that cause people not to "opt-out" will be removed, as they can discreetly and nonchalantly exit the site without

---

149. Seal programs were intended to, and have succeeded to a certain extent, establish more comprehensive and uniform methods of Internet data collection practices. *See* Hayward, *supra* note 63, at 232-33. However, sites that display the same privacy seal may provide Internet visitors with widely divergent information collection practices. *Id.* at 235.

150. According to a 2001 Greenfield Online Survey, almost ninety percent of online shoppers would feel more confident shopping on a site that displays BBBOnline's privacy seal. Council of Better Business Bureau, Inc., BBB Online, *at* http://www.bbbonline.org/privacy/ priv_EN.asp (last visited Nov. 11, 2002).

151. *See* Walker, *supra* note 2, at 140. BBBOnLine notes that "displaying the BBBOnLine seal assures customers with just one glance" that the requisite privacy practices are in place. Council of Better Business Bureaus, Inc., *supra* note 150. Today, when a Web site posts a privacy policy, it is usually "vague, legalistic, and provides little useful information." Mary J. Culnan, *The Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission*, *at* http://www.msb.edu/faculty/culnanm/GIPPS/gipps1.PDF (last visited Dec. 15, 2001). Over sixty-five percent of Americans felt that security metrics that rated the security of a Web site would prove useful to consumers. GVU's 10th WWW User Surveys, *supra* note 141.

worry.[152] In addition, browsers could be programmed to identify and authorize threshold toolbar grades, allowing access to only those Web sites that have a collection of buttons meeting standards determined by the user.[153]

D. Equity Across Market Players

Smaller players who may have difficulty in complying with a complex statutory scheme may be placed at a disadvantage to larger, more capitalized Web players. However, a simple privacy toolbar program is affordable to all businesses because it does not require extensive changes to a business's collection techniques or require individual contracts with Internet visitors.

E. Satisfaction of EU Directive Requirements

The privacy toolbar program will afford EU consumers the same or heightened protection level as the Safe Harbor provision under which companies currently operate. The EU could require that certain core elements exist before the Web site may conduct business with the EU. In addition, all Web sites and operators would be under legislative edict to post toolbars, whereas today the Safe Harbor provision is purely voluntarily.[154] Conducting business with U.S.-based sites would become easier, as a quick online visit to the Web site will reveal the broad policies regarding collection activities of businesses.

Of course, any regulation of a previously unregulated industry can cause adverse economic repercussions. However, the toolbar program is a relatively unobtrusive means of formalized governmental regulation. In addition, economic growth must be balanced with the competing value of individual privacy to attain a solution that maximizes the collective social good.

CONCLUSION

The Internet economy is a new frontier for business growth and expansion. However, privacy issues must be resolved in order for the e-economy to realize its true potential as an economic medium. Technology will continue to develop and change the dynamics of the Internet architecture, but personal privacy concerns will remain throughout technological evolution. Self-regulation is currently failing to adequately meet the expectations of online consumers, and as such, may be pulling back the reins of e-commerce growth. Regulation of personal data is an integral part of operating in the Internet environment, and current laws cannot adequately cope with the current deficiencies in consumer privacy protection. Although new regulations are required, they should be

---

152. *See generally* Sovern, *supra* note 37, at 1071-78.

153. This would be similar to Web browsers that can currently be programmed to reject "cookie" files.

154. A posted toolbar does not automatically guarantee that the Directive's requirements have been met. However, the EU will have more assurance that the site is compliant with the policy because stiffer penalties for noncompliance would exist for violators.

drafted to minimally disrupt the current practices of businesses and refrain from impinging upon free commercial speech. A mandatory privacy toolbar program accomplishes both tasks and allows the invisible hand of the market to truly place an accurate value on personal data privacy. As such, the market will attain the efficiencies desired, and e-business will continue to thrive on the market's terms.