An Assessment of the Costs of Proposed Online Privacy Legislation

Robert W. Hahn

May 7, 2001

Mr. Hahn is Director of the AEI-Brookings Joint Center for Regulatory Studies, a Resident Scholar at the American Enterprise Institute, and a Research Associate at Harvard University. This work was supported by the Association for Competitive Technology. He would like to thank Anne Layne-Farrar and Kirstyn Walton for their research support. The views expressed in this document reflect those of the author and do not necessarily reflect the views of the institutions with which he is affiliated. See Appendix A for Mr. Hahn's vita.

Executive Summary

This study estimates the costs of various aspects of proposed online privacy legislation. Using what I believe to be fairly conservative assumptions, I find that these costs easily could be in the billions, if not tens of billions of dollars. This fact alone suggests that proposed regulations that would flow from these laws could have a substantial economic impact on consumers and businesses.

I argue that further regulation of online privacy is premature for three reasons. First, the costs could be substantial. Second, I am not aware of any good quantitative estimates of the benefits of such regulation. Third, the market is reacting to ensure that at least some of the consumer concerns related to online privacy are being addressed.

An Assessment of the Costs of Proposed Online Privacy Legislation

Robert W. Hahn

I. INTRODUCTION

Consumers, government agencies and businesses are all making greater use of the Internet. This trend is expected to continue. As use increases, some scholars have called for regulation of various aspects of the Internet.[1] Other scholars have suggested that very little regulation is needed.[2] The merits of regulating the Internet depend on the benefits and costs of proposed legislation. This study, commissioned by the Association for Competitive Technology (ACT), a non-profit trade association of the information technology (IT) industry, estimates some of the potential costs associated with proposed legislation of online privacy.[3]

After defining the focus of the paper below, Section II reviews several of the privacy laws already enacted. This section also summarizes the currently proposed online privacy bills. Section III accesses the costs of complying with proposed online privacy legislation. Conclusions and recommendations are presented in Section IV.

A. Scope of the Analysis

1. The Theoretical Background for the Privacy Debate

A fundamental issue in the privacy debate relates to the ownership of information. Does a company have the right to take and use personally identifiable information (PII) from a consumer and use that information for profit? Note that both a consumer and a company could benefit from sharing that information. For example, if I were interested in golf and I signed

---

[1] Swire, Peter and Robert Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, Washington D.C.: Brookings Institution Press, 1998; Lessig, Lawrence, *Code and Other Laws of Cyberspace*, New York: Basic Books, 1999; Litan, Robert, *Law and Policy in the Age of the Internet*, 50 DUKE L.J. 4, 1045 (2001).

[2] Litan, Robert and William A. Niskanen, *Going Digital!:A Guide to Policy in the Digital Age*, Washington, D.C.: Brookings Institution Press, 1998.

[3] ACT represents over 12,000 U.S. companies and IT professionals in the computer and communications industries. Members include software consultants, systems integrators, consulting firms, and IT training services.

onto a golf website that sent me updates on the latest golf clubs to buy, I could find that useful in improving my golf game.

Issues arise as to how and when such personally identifiable information should be used. One way of addressing those issues is to ask how different kinds of rules and regulations could affect the well being of both consumers and producers. Does it matter, for example, whether consumers are given the right to "opt-in" to receive certain kinds of notices or ads on the Internet, or whether they are required to "opt-out"? If it were costless to opt-in and opt-out, it might not matter. Of course, it is not costless and it does matter for economic efficiency as well as other concerns, such as the distribution of benefits and costs.[4]

A substantial academic literature concerning the privacy debate currently exists.[5] Most of this literature focuses on theoretical issues or particular anecdotes related to the allocation of property rights and appropriate regulations.[6] Unfortunately, there are very few empirical studies that attempt to measure the costs and/or benefits of online privacy regulation.[7]

2. The Scope of the Study

This study focuses on measurable costs associated with legislative proposals.[8] I do not provide a full analysis of all of the proposed online privacy laws, nor do I weigh all benefits against all costs. In fact, I do not consider potential benefits at all. Instead, the focus is on the narrower question of what the proposed legislation would cost Internet companies faced with complying with the new laws.

---

[4] This is the familiar Coase Theorem applied to PII. Absent any negotiation costs the initial allocation of legal rights does not matter from an efficiency perspective so long as they can be exchanged in a perfectly competitive market. Coase, R.H., *The Problem of Social Cost*, 3 J.L. & ECON. 1, 6-8 (1980).

[5] See, for example, Cate, Fred, *Privacy in the Information Age*, Washington D.C.: Brookings Institution Press, 1997

[6] For example, see Kang, Jerry, *Information Privacy in Cyberspace Transactions*, STANFORD L. REV. (1998); and Lessig, Lawrence, *Code and Other Laws of Cyberspace*, New York: Basic Books, 1999.

[7] A notable exception is *Privacy and the Commercial Use of Personal Information*, Emory University (mimeo), 2001, by Paul Rubin.

[8] Numbers in this paper are generally reported to two significant digits. In some cases, I round to one significant digit.

I limit the analysis here to the costs of legislative proposals whose impact can be quantified. Based on popular provisions of various proposed online privacy bills, I consider only those costs that would fall directly upon businesses that collect PII for marketing and advertising purposes and businesses that sell or distribute advertising space on websites.

The difficulty in quantifying these costs lies in the nascent nature of the industry. For example, the potential decline in PII-targeted advertising revenue could be substantial, even though the current size of this market is small. Instead of speculating about future impacts, this study focuses on hard dollar costs for current Internet sites to comply with proposed online privacy legislation, limiting the analysis to estimated professional labor costs. [9]

I estimate how much a website would need to spend in order to comply with the proposed laws. I then estimate how many operators the proposed laws would affect. Combining the two numbers provides an estimate of the compliance costs for the U.S. commercial Internet industry as a whole. Just focusing on this one area, the analysis below illustrates that compliance costs could reach billions of dollars and therefore warrant careful consideration before any of the proposed bills become law.

II. SUMMARY OF PRIVACY LEGISLATION

A. Enacted Privacy Legislation

Thus far, no single federal statute has attempted to broadly protect the privacy of consumers. However, there are a number of laws that have privacy components, including: the Telephone Consumer Protection Act, the Electronic Communications Privacy Act, Customer Proprietary Network Information rules, the Cable Communications Policy Act, the Financial Services Modernization Act (frequently referred to as the Gramm-Leach-Bliley Act), and the Children's Online Privacy Protection Act. [10]

---

[9] Several costs are not considered here. For example, one potentially large cost is the loss of targeted advertising and email marketing that has helped to support much of the free Internet content.

[10] To review the Telephone Consumer Protection Act of 1991, see http://www.jmls.edu/cyber/statutes/email/tcpa.html. To review the Electronic Communications Privacy Act of 1986, see http://www4.law.cornell.edu/uscode/18/ch119.html. For a link to the FCC order regarding Customer Proprietary Network Information, see http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1998/fcc98027.txt .

Privacy provisions in existing federal laws were designed to increase the protection of information that companies collect about consumers. The Telephone Consumer Protection Act is narrowly focused to restrict communications between firms and consumers – telemarketing, for example. The Electronic Communications Privacy Act, on the other hand, protects the exchange of information from interception by or disclosure to unauthorized third parties, including law enforcement agencies. Customer Proprietary Network Information rules restrict the use of customer information by telephone companies, both internally and via disclosure to third parties. The Cable Communications Policy Act requires detailed, annual privacy disclosures to customers and imposes restrictions on disclosures to third parties, but provides flexibility for a cable operator to use information internally.

The Financial Services Modernization Act contains the most comprehensive financial privacy provisions. The law requires financial institutions to provide every customer with a clear and conspicuous statement of policies and practices for protecting the privacy of customer information. In addition, each financial institution must provide its customers with notice, and an opportunity to prohibit, or opt-out of, disclosures to nonaffiliated third parties.[11]

Legislation aimed specifically at protecting children's privacy on the Internet first appeared in the Children's Online Privacy Protection Act. The Act applies to operators of commercial websites and online services targeted to children under the age of 13, where personal information is collected. The rule also applies to operators of any general interest site that has actual knowledge that it is collecting information from children under 13 years old.[12]

Sites covered by COPPA must: 1) post a privacy policy and links to that policy; 2) notify parents of its information practices; 3) with certain exceptions, obtain verifiable parental

---

Financial Services Modernization Act, 15 U.S.C. § 6801-6827, Title V (1999), available at http://www.ftc.gov/privacy/glbact/glbsub1.htm, http://www.ftc.gov/privacy/glbact/glbsub2.htm. The Children's Online Privacy Protection Act, 15 U.S.C. § 6501 *et. seq.*, Title XIII (1998), available at http://www.ftc.gov/ogc/coppa1.pdf.

[11] Under regulations promulgated by several federal and state agencies, the Gramm-Leach-Bliley Act requirements become fully effective in July of 2001. Financial institution customers are just now beginning to receive paper and email privacy notices mandated under this law. These notices will present consumers with a variety of options dictating how financial institutions may share their information with third parties.

[12] For example, chat rooms and bulletin boards designed for general audiences.

consent before collecting, using or disclosing personal information from children; and (4) provide parental access to their children's information, plus the capability to delete such information and to opt-out of future collection.

B. Unintended Consequences of Privacy Legislation

COPPA became effective in April 2000. Under this law, the Federal Trade Commission (FTC) has specific authority over online privacy issues affecting children. While the Act will help to weed-out bad actors, an unintended consequence is the curtailment of online services that provided legitimate educational and entertainment experiences for children.

For example, Zeeks.com, an award-winning games and entertainment website for kids ages 6 to 13, announced plans to remove all of its interactive elements, from e-mail to chat rooms, because of COPPA compliance costs.[13] Zeeks CEO Steven G. Bryan said the $200,000 per year it costs Zeeks to employ chat room supervisors, monitor phone lines to answer parents' questions and process COPPA permission forms was "the straw that broke the camel's back." To comply with COPPA, Bryan said the company had to employ about a dozen chat room monitors to oversee activity in a pair of chat rooms available 12 hours a day.

Microsoft's free Hotmail service reported a surge in complaints from customers because of the company's compliance with COPPA.[14] Hotmail is not targeted at children under 13, but some children use it and therefore it has to follow the rules regarding parental consent. Some users had entered a false birth date for privacy reasons, but were forced by the Act to reveal information they had chosen to keep private in the past. Many Hotmail users balked at having to provide a credit card number to prove age and identity in order to re-gain access to their account. In all, Microsoft received over 15,000 complaints from users of its free email service during April and May of 2000, compared with an average of 600 complaints in the months just before COPPA implementation.

---

[13] Information in this paragraph based on Charney, Ben, "The cost of COPPA: Kids' site stops talking," *ZDNet News*, September 13, 2000, available at http://www.zdnet.com/zdnn/stories/news/0%2C4586%2C2627742%2C00.html.

[14] Information in this paragraph provided by Diane McDade, Privacy Product Manager for MSN.com, in an interview conducted by Steve DelBianco on April 20, 2001.

These two examples do not negate the intended benefits of COPPA in protecting children, but they should caution policy makers to consider all of the potential impacts of proposed online privacy legislation.

C. Proposed Online Privacy Legislation

1. Common Features of Online Privacy Protection

Each of the proposed laws contains at least one of the following five basic principles[15]:

- **Notice** to the consumer regarding collection, use and disclosure to third parties of PII obtained from a user. PII are data used to identify, contact, or locate a person, including name, address, telephone number, or E-mail address. Some legislative proposals require website operators to notify all users of any change in information policy or breach of policy.

- **Consumer choice** either to opt-out or opt-in for use or disclosure of PII to third parties. Some legislative proposals require choice for PII use in internal marketing and for disclosures to affiliates; some proposals exempt internal uses.[16]

- **Access** by a consumer to his or her PII and an opportunity to correct inaccurate information. Some bills would require access to names and addresses of every affiliate or third party using a consumer's PII.

- **Security** adequate to protect the information from unauthorized disclosure.

---

[15] The FTC also defines these principles as the foundation for privacy legislation. *See* "Privacy Online: Fair Information Practices in the Electronic Market place, A Report to Congress," Federal Trade Commission, May 2000, available at http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf.

[16] Consumer choice entails two basic mechanisms: opt-out and opt-in. In opt-out, the default is that the individual allows the website visitor to share her PII. For example, when Jane Doe visits Amazon.com and clicks on the privacy notice, she pulls up a description of the types of information Amazon collects and what it does with that information. At the bottom of the screen is a link that allows Ms. Doe to change her choice to prevent Amazon from sharing any PII that she might fill out in the course of ordering a book from the website. Unless she changes her choice, the default will allow Amazon to share her PII with its affiliates in the ways described by its privacy policy. When websites use an opt-in mechanism, the default is for the website not to share any PII collected. In this case, Ms. Doe would need to actively change her choice to allow PII sharing.

- **Enforcement** of applicable privacy obligations, including penalties for violations.

2. A Selected Review of Proposed Privacy Laws

a. Consumer Privacy Protection Act (S. 2606)

Legislation was introduced in the 106th Congress (and likely will be reintroduced in the 107th) giving consumers a fundamental ownership interest in their personal information and the right to access and control how that information is collected, used or transferred. This concept is codified in S. 2606, introduced by Sen. Hollings (D-SC).[17] The bill requires opt-in consent for collection and disclosure of PII. If the Web operator changes its distribution policy, it is prohibited from using or collecting PII until the user consents to the new policy. Consent or denial remains in effect until changed by the user. Non-PII information is subject to an opt-out requirement. The Hollings bill also creates new private rights of action by authorizing civil suits seeking recovery of damages. Websites may need to track both the choices made and any uses of PII to prove compliance in defense against private plaintiffs.[18]

b. Consumer Internet Privacy Enhancement Act (H.R. 237 & S. 2928)

In the 107th Congress, Representatives Eshoo (D-CA) and Cannon (R-UT) introduced a privacy bill covering all consumers who use the Internet. This bill closely matches S. 2928, introduced by Senators McCain (R-AZ) and Kerry (D-MA) in the 106th Congress.

According to these bills, a user may opt-out of PII collection and transfer for marketing purposes. A website must disclose whether a user is required to provide PII, but does not require the website to provide users with service if they opt-out of providing PII.

Both bills require a website operator to provide clear and conspicuous notice of information practices, including a description of how PII is collected and used, and

---

[17] All of the proposed online privacy bills discussed below may be found at http://thomas.loc.gov/home/c106query.html.

[18] Section 303(a) and (b) of proposed Senate bill 2606. Fines start at $5,000 per violation with an additional fee of up to $50,000 for a willful or knowing violation.

identification of third parties who may collect information from the website's users. They further require that consumers have simple methods to restrict the use and disclosure of PII to third parties. Website operators must provide their address, telephone number, and an electronic means of contact so that consumers may inquire about the site's information practices.

The FTC would be empowered to fine violators of the provision with civil penalties ranging from $22,000 to $500,000 per violation. H.R. 237, however, provides a safe harbor for any website that complies with self-regulation policies approved by the Federal Trade Commission.[19]

c. Consumer Online Privacy and Disclosure Act (H.R. 347)

Introduced by Rep. Green (D-TX), this bill would require the FTC to promulgate regulations requiring website operators to provide clear privacy policy notice and the opportunity for users to opt-out of disclosure of PII for purposes not related to why it was originally obtained. In other words, if the privacy policy states that the PII is obtained to track performance of a website, it could not be used for marketing purposes. The bill also requires disclosure of the PII that is provided to third parties.

Section 2(a)(2) states that no operator of a website or online service may allow any third party to attach a "cookie"[20] as a means of developing a personal profile of an individual, unless the operator clearly discloses such practices and obtains the user's permission. That is, consumers can prevent the use of the information for any activity other than the intended transaction.[21]

---

[19] The bill calls for the FTC to conduct a study with recommendations for self-regulation.

[20] A cookie is an information file placed on the user's computer by a website that collects data on the user and the Internet sites he or she visits. Each cookie contains a list of website addresses with which a browser may share cookie information. By storing a user's ID for a particular website in a cookie, the user no longer needs to re-enter identifying information when returning to the site. See Appendix C for a brief glossary of technical terms.

[21] In its May 2000 report to Congress, the FTC specifically asked Congress for authority to require choice encompassing "both internal secondary uses (such as marketing back to consumers) and external secondary uses." *See* "Privacy Online: Fair Information Practices in the Electronic Market place, A Report to Congress," Federal Trade Commission, May 2000, p. 36 available at http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf.

d. Spyware Control and Privacy Protection Act of 2001 (S. 197 & H.R. 112)

Some legislators have grown concerned about software and websites that include a method to collect information about the computer on which the software is installed. Two bills, H.R. 112 (Rep Holt, R- NJ) and S. 197 (Sen. Edwards, D- NC) were introduced to address this issue.[22] The bills classify "spyware" as encrypted codes that monitor the activities of computer users and that share the personal information with advertisers, telemarketers, or other businesses. The definition of spyware could include third party software that is used to collect information about which Web pages are visited and how a software product is used. The bills proposed would require prior notice of the capability of a software application to transmit PII, a description of the PII collected, contact information for PII recipients, and clear and conspicuous instructions on how to stop the collection without affecting the software's performance. Collected PII could only be used for the purposes for which it was collected, and would therefore require site operators to track where data are used. Individuals would have the right to access their data for inspection and to correct errors or omissions. The spyware bills provide enforcement through the FTC; Senate bill 197 also allows private rights of action with penalties ranging from $2,500 to $500,000 for each violation.[23]

D. Online vs. Offline Privacy

While a distinction is often drawn between the online and offline collection of information, focusing on the type and use of information is far more productive. Some information is used solely for marketing purposes while other information is used to actually make a decision about a consumer, such as a mortgage approval. While I have a choice as to which online bookstore to use – perhaps even based upon their relative privacy policies – once I decide to purchase a book online, I do not have the choice of whether to provide my credit card number.[24] It makes sense to provide some sort of consumer assurances and protection

---

[22] See http://thomas.loc.gov/home/c107query.html.

[23] "Willful and knowing" violations could push fines up to $1.5 million.

[24] "Information about an individual's use of a credit card may be used to determine the advertising inserts placed in their monthly billing statement, just as information about the actions of a computer browser may be used to determine the advertising placed on the next page the browser visits." *See* "Final Report of the FTC Advisory

where the submission of information is necessary or involuntary, especially when that information is sensitive.

All but one of the enacted privacy bills discussed earlier attempt to protect privacy in the offline world. With the exception of COPPA (which applies to children's privacy on the Internet and is similar to the online bills discussed directly above), the enacted bills address the first two basic principles, notice and choice, but are much weaker on the principle of consumer access to PII. For example, the Video Privacy Act requires access to personal information for government entities holding court orders, but unlike proposed Senate bill 2606, gives customers no right to access or correct their own records.[25]

Discrepancies between offline and online privacy legislation could lead to problems for companies with business in both worlds. Consider, for example, a clothing retailer with brick-and-mortar stores, catalogs, and a website. This retailer collects marketing information from its customers at all three points of sale, as well as from information brokers.[26] However, instead of creating a uniform database from all sources for use in its market research and marketing efforts, the retailer would have to keep PII collected online separately. Otherwise, the retailer could not comply, or prove compliance, with the access provisions in the proposed laws. In other words, it would be forced to treat the same kinds of information in very different ways, based solely on how that information was collected.[27] Sensible regulation of personal

---

Committee on Online Access and Security," Federal Trade Commission, May 15, 2000, p. 5, available at http://www.ftc.gov/acoas/papers/finalreport.htm.

[25] Video Privacy Protection Act, 18 U.S.C. § 2703, ch 121 (1988), available at http://www.usdoj.gov/criminal/cybercrime/usc2703.htm.

[26] As described in the FTC Advisory Committee report, "A business may purchase information about its existing customers from another business or it can purchase a list containing information about individuals it would like to attract as customers, such as a mailing list. Similarly, a business may purchase data that is used to enhance the information that it has about its own customers" ("Final Report of the FTC Advisory Committee on Online Access and Security," Federal Trade Commission, May 15, 2000, p. 5, available at http://www.ftc.gov/acoas/papers/finalreport.htm).

[27] Regarding the discrepancies between online and offline privacy regulation, the FTC May 2000 study states "The Commission's review of privacy has mainly focused on online issues because the Commission believes privacy is a critical component in the development of electronic commerce. However, the FTC Act and most other statutes enforced by the Commission apply equally in the offline and online worlds." *See* "Privacy Online: Fair Information Practices in the Electronic Market place, A Report to Congress," Federal Trade Commission, May 2000, ft. 23, available at http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf.

information usage should address the use of information across the economy, regardless of the technology used to collect it.

III. ESTIMATING THE COST OF PROPOSED ONLINE PRIVACY LEGISLATION

In this section, I consider the implications of three of the five basic privacy provisions: notice, choice, and access. Of these three, access appears to entail the most costly compliance and is therefore the primary focus of the cost estimates developed below.

A. Notice

Over the last few years, awareness of privacy issues among Internet businesses has increased substantially. In 1998, the FTC found that only 14% of 1400 randomly sampled commercial websites provided any kind of notice about its information practices.[28] By February 2000, a survey of 30,000 websites found that around 23% were posting some sort of privacy policy.[29] From among the top 1,000 websites, defined by the number of unique visitors to the site, 84% had a privacy notice of some sort.[30] In the summer of 2000, the FTC conducted an update of their 1998 study.[31] "The 2000 Survey results show that there has been continued improvement in the percent of websites that post at least one privacy disclosure (88% in the Random Sample and 100% in the Most Popular Group)."[32]

The statistics on privacy policy notification illustrate a growing trend of Internet self-regulation. There are clear incentives for this trend to continue. Just as with traditional

---

[28] Statistics as of March 1998. *See* "Privacy Online: A Report to Congress," Federal Trade Commission, June 1998.

[29] *See* "Internet Privacy: A summary of privacy ratings research by enonymous.com," April 2000, available at http://www.enonymous.com/study1.doc (site visited on April 24, 2001). Note that this statistic (23%) does not include sites that do not collect any PII. Moreover, the 30,000 sites in the survey included non-commercial sites, like dot-org, dot-net, dot-edu, and dot-gov. The dot-org, dot-net, and dot-edu sites all had smaller percentages of privacy policy notification. Among the dot-coms, around 25% had some kind of policy posted.

[30] According to a January 2000 review of websites by enonymous.com. *See* "Internet Privacy: A summary of privacy ratings research by enonymous.com," April 2000, available at http://www.enonymous.com/study1.doc (site visited on April 24, 2001).

[31] *See* "Privacy Online: Fair Information Practices in the Electronic Market place, A Report to Congress." Federal Trade Commission, May 2000, available at http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf.

[32] The Random Sample studied 335 websites; the Most Popular Group studied 91 of the 100 busiest sites (measured by number of unique visitors to the site).

industries, self-regulation on the Internet is a means to avoid the costs and rigidities of government legislation. Moreover, users are likely to be more comfortable using websites that have a clear information policy, a reputation for adhering to that policy, and offer users a means to opt-out of information sharing.

One of the primary outcomes of increased self-regulation on the Internet has been the creation of privacy seal programs. Programs like TRUSTe, BBB*OnLine* Privacy Seal, SAFEcertified.com, and enonymous.com rate the privacy policies of websites, providing sites that post protective policies a seal of approval and making it easier for consumers to be well informed.[33] Informed consumers demanding clear privacy policies and a means by which to opt-out of the information stream make self-regulation customer driven. According to the FTC, "if widely adopted, they promise an efficient way to alert consumers to licensees' information practices and to demonstrate licensees' compliance with program requirements."[34]

B. Choice

A large majority of sites provide information on their privacy policies, but a much smaller percentage of U.S. commercial websites offer visitors a means to prevent the use of PII. In its 2000 Survey, the FTC found that "only 41% of the sites in the Random Sample and 60% of the sites in the Most Popular Group meet the basic Notice and Choice standards."[35] The percentage is considerably smaller in the enonymous.com 2000 survey: about 6% of the 30,000 websites surveyed provide a consent mechanism at the point of PII collection. In other words, among the same commercial websites that are posting a privacy policy notice, many do not provide consumers a choice when it comes to sharing PII.

---

[33] *See* http://www.etrust.com/, http://www.safecertified.com, http://www.enonymous.com/, and http://www.bbbonline.org.

[34] *See* "Privacy Online: Fair Information Practices in the Electronic Market place, A Report to Congress," Federal Trade Commission, May 2000, p. 6 available at http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf. Note that the FTC does not feel seal programs have yet to establish a significant presence on the Web. They go on to say, "industry efforts alone have not been sufficient" (p. *ii*) and recommend that, while a "major role for industry self-regulation" exists (p. *iii*), Congress should enact online privacy protection legislation.

[35] *See* "Privacy Online: Fair Information Practices in the Electronic Market place, A Report to Congress," Federal Trade Commission, May 2000, available at http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf.

One key aspect of consumer choice provisions in the proposed legislation is the distinction between opt-out and opt-in rules. Because of simple inertia, the choice of default is likely to lead to very different results. Many, perhaps most, people will simply let the default stand rather than make an explicit choice. As a result, for sites with an opt-out mechanism, many people will share their PII; for sites with an opt-in mechanism, many people will not share their PII.

To gain a better understanding of the effect the choice mechanism could have, consider a study of the Financial Services Modernization Act conducted by Ernst & Young.[36] One survey question asked financial institutions to estimate the response rate under opt-out and opt-in regimes.[37] "While there was considerable variation in the responses, the majority of respondents indicated that the response rate under either system would be 10 percent or less."[38] That is, under opt-in 10% of website visitors share their PII while under opt-out 90% share their PII.[39]

In considering the choice mechanism, it is important to keep in mind that many major websites (such as Yahoo! and Yellowpages.com) depend primarily on advertising and marketing revenues to finance their services. If opt-in requirements limit the PII that free websites share with advertisers and marketers, then revenues would fall. If revenues fell

---

[36] "Customer Benefits from Current Information Sharing by Financial Services Companies" (conducted for The Financial Services Roundtable by Ernst & Young LLP), December 2000, available at http://www.privacyalliance.org/resources/glassman.pdf.

[37] I am not aware of any formal empirical study that looks at how opt-in and opt-out work in practice, as opposed to a hypothetical survey question.

[38] "Customer Benefits from Current Information Sharing by Financial Services Companies" (conducted for The Financial Services Roundtable by Ernst & Young LLP), December 2000, p. 25, available at http://www.privacyalliance.org/resources/glassman.pdf.

[39] Clearly, the choice mechanism imposed can have serious repercussions for websites. Currently, online advertising services earn less than $10 million on ads targeted with third-party cookies, but this figure is expected to grow rapidly over the next few years. (Based on interviews conducted by Steve DelBianco, Vice President, ACT, with Chief Privacy Officers and Marketing Directors at DoubleClick and 24/7 Media, two firms offering Internet marketing and advertising consulting services for website operators. See www.networkadvertising.org/aboutnai_members.asp for additional information on the companies). If opt-in mechanisms are required, the amount of PII collected by a site could decline substantially. With fewer customer profiles, websites may be unable to attract third party targeted advertising, resulting in potentially large revenue losses.

dramatically, many sites offering free services today would be forced to charge users a subscription fee or go out of business.

C. Access

In general, the access provisions in proposed legislation require service providers to allow users to see their PII and correct the information, as they deem necessary.[40] If access must be online, the proposed laws could require outside entrance to website databases. A database that is accessible only through the company is relatively more secure. The more people allowed entrance to a database with sensitive information, the more prone to abuse is that database. Thus, there is a natural trade-off between access and security.[41]

D. The Costs of Complying

1. The Implications of Complying

Beyond security issues, complying with and being able to prove compliance with choice and access provisions has several implications for websites. If they choose to store PII, website operators would also need to store information for which they currently have no use. For example, if a user, after originally allowing PII to be shared, changed her mind and decided to opt-out, all third party email services to whom her information had been sent would need to be notified. If new legislation requires consumer choice for the use of third-party cookies, all third-party ad services would need to be notified, probably requiring each ad server to immediately execute an opt-out script to prevent its advertisements from reading or placing cookies.[42] This implies that websites need to track all third parties receiving PII on each user.[43]

---

[40] See, for instance, the access provision in Senate bill 2606, the Consumer Privacy Protection Act, http://thomas.loc.gov/home/c106query.html.

[41] As noted in the Advisory Committee Report to the FTC, "privacy is lost if a security failure results in access being granted to the wrong person." *See* "Final Report of the FTC Advisory Committee on Online Access and Security," Federal Trade Commission, May 15, 2000, p. 15, available at http://www.ftc.gov/acoas/papers/finalreport.htm.

[42] See, for example, "Network Advertising Initiative homepage," available at http://www.networkadvertising.org/optout_howwedoit.asp.

[43] See Appendix D for a diagram illustrating the flows of PII between the user, the website, and third parties. This diagram was not part of the survey supplied to respondents and is presented here to clarify the implications of tracking PII choices and uses.

Moreover, to prove compliance, they would also need to maintain records of changes in each user's PII sharing preferences, along with an indication of the website's privacy policy in place at the time of the change.[44]

Relaxing the assumption that prior third party vendors need to be notified if a user changes his or her preferences does not necessarily reduce tracking costs. Assume that instead of purging third-party databases of users who changed their sharing preferences, the proposed laws simply require changes in choice to apply to information shared on a going forward basis; that is, websites could not share the PII with anyone new. Under this interpretation, a website would no longer need to notify third parties who had received past PII. However, the access provision in some of the pending bills (such as the spyware bills discussed above) requires websites to track all third-party uses of PII for consumer review. To prove compliance with these bills, websites would still need to track users' PII sharing preferences over time, as well as all third parties receiving PII on each user.[45]

2. Quantifying the Costs of Compliance

To obtain quantitative estimates of the cost, I requested that ACT collect estimates on the initial costs of modifying systems to allow a website to track the types of information discussed above. Then I estimated how many websites the proposed laws would affect. Finally, I multiplied the software cost by the number of affected sites to obtain an estimate of the industry-level cost to compliance.

---

[44] As a further complication, consider consumer Jane Doe. Ms. Doe visits websites A and B, both of which collect PII and sell that information to retailer X. At site A, Ms. Doe opts-out of information sharing, but she neglects to opt-out at site B. Retailer X then purchases the PII on Ms. Doe from site B and sends her a targeted offer via email. First, how is Ms. Doe to know how retailer X got her information? Will the proposed legislation compel company X to provide the source of its marketing information? Is X liable in any way? If Ms. Doe were to wrongly assume that X got her PII from website A, A would need some mechanism to prove compliance. This example also illustrates the complexity of guarding PII. PII comes from many sources, not just the Internet.

[45] The FTC Advisory Committee noted in its report "[f]or businesses, this approach [access to all PII] would lead to a substantial increase in costs, including, among others, the costs of required modifications or new design requirements placed on existing systems, new storage costs, new personnel costs, new legal costs and losses due to the disclosure of internal practices and proprietary information, and this approach would affect the confidentiality of procedures companies use to make decisions and assumptions about user data." *See* "Final Report of the FTC Advisory Committee on Online Access and Security," Federal Trade Commission, May 15, 2000, p. 9, available at http://www.ftc.gov/acoas/papers/finalreport.htm.

Quantifying the unit costs and the number of affected websites is a difficult task. First, since very few websites have needed software to track PII and its uses, little is known about much it would cost. Second, there are several estimates of the number of World Wide Web domains, but little data on how many of those are unique, U.S.-based, commercially viable sites, that collect and share PII, and would continue to do so if the proposed bills become law.

To help with the first piece of information, the software cost, I asked ACT to collect information from information technology consulting firms (consultants) on the costs of building server-side software that complies with several provisions in proposed online privacy laws.[46] I assume that most small to mid-sized Internet service providers would need to outsource a project of this scale and complexity.

Consultants were asked to assume that their client (the website operator) was already complying with basic notice and choice provisions. In particular, consultants were asked to make the following assumptions:

1. The client already has a website that includes privacy policy pages.[47]
2. The client already has a database of 100,000 users, indicating name, address, email address, age, sex, date of registration, and several personal preferences, including an indicator to opt-out of sharing this PII with third parties. The database design should scale up to 10 million users.
3. The client already has Web pages to allow users to review and update their basic PII and preferences.[48]
4. All source code developed would become the unrestricted property of the client.

---

[46] ACT sent surveys to 25 information technology consultants from across the United States (see Appendix B for a copy of the survey and the responses). The 25 consultants were selected to represent geographic and technological diversity.

[47] Recall from above that the FTC found over 80% of U.S. commercial sites had some sort of notice.

[48] Note that, while not currently prevalent among commercial websites, according to several consultants responding to the survey, adding an opt-out mechanism represents an insignificant one-time cost. I therefore assume that sites are already providing an opt-out mechanism.

5. All components and database tables must be secured against infiltration from unauthorized users. Identification and password are required for user access to PII.

6. Since the client already has a functioning website with user registration, the estimate for design, testing, and implementation need not include those costs, but it should include the cost of integrating the new components with the existing code and database.

According to the respondents, integration (point 6 above) is probably the most costly element of the compliance software. Websites that are currently collecting PII already have in place working systems, software and databases. Making new software work with existing software is often a difficult and time-consuming task, implying that off-the-shelf solutions are frequently not a viable option. Programming for the user interface and services is also a costly component of the software, but one that will likely become cheaper over time as consultants gain expertise with access compliance software.[49]

The consultants were asked to ensure that the new tracking software would have the following capabilities.[50]

1. The website (client) may need to do a broadcast email to all users in the database whenever there is a change in privacy policies or to report a breach of any privacy policy. Each instance of the email must be logged to a tracking database, including the date sent, the recipient's email address, the message text, and an indication of whether the email is delivered successfully. The software should automatically save any emails returned as undeliverable, and update the user database to indicate the return date and reason for non-delivery.

---

[49] One consultant estimated that the economies of scale for developing software of this kind would "likely not exceed a 15% reduction in cost." See Appendix B for a complete set of the consultants' estimates and comments.

[50] See Appendix B for the actual technical specifications. The six points listed here provide less technical interpretations of those specs.

2. Whenever the website shares or transfers PII to a third party for mailing or marketing purposes, the system must create a tracking record that indicates user name, third party, date, and all PII known at the time. Some transfers may be mail-merge transactions, where the third party requests email addresses for all users that match given characteristics. These merge transfers must also be tracked as PII sharing, since the third party implicitly knows the characteristics of any user that meet its selection criteria.

3. Website registered users may request access to a Web page that displays all instances where their PII has been transferred or shared with third parties (described in (2) above). This display should include the date the PII was shared, third party name and address, and the information that was transferred.

4. When users change their PII or their sharing preferences, the system should create a tracking record indicating user, date of change, nature of the change, and version of the client's privacy policy in effect at time of the change.

5. Any user change to PII or preferences must be forwarded to all third parties that are in the process of using the user's previous PII, whether as mail-merge or for extraction and transfer of information. Any change to a user's PII should generate transaction messages to each third party known to be using PII for that user (tracked per item 2 above).

6. The client's website may display banner ads that are served by third-party network advertising companies.[51] Before linking to any third-party site, the client's website should inform the user and request their permission to allow the link. Users should also be asked whether their preference for third party ad links should be stored and followed for all subsequent visits.

[51] Network advertising companies manage and deliver ads for multiple advertisers. For example, a user visiting www.yellowpages.com might see banner ads served by DoubleClick (a network advertiser). In this example, DoubleClick is a third party advertiser. Some third-party ads might read or place information files (e.g., cookies) on users' computers in order to track the user's preferences and characteristics so that future ads matching the user's interests may be shown.

Given these six software capabilities and the website (client) assumptions above, ACT asked the consultants to estimate the cost of building PII tracking software. The components of their cost estimates included design and data modeling, programming, project management, integration and testing. Each consultant provided the assumed number of labor hours, out-of-pocket expenses, and hardware expenses needed to complete the project.[52] Assuming that interpretations of the law do not change over time, these estimates represent one-time costs of complying, and being able to prove compliance for the consultant's first client. Because of the learning process, providing similar software to additional websites would likely cost less, although an off-the-shelf product may not be realistic given that the new system has to be integrated into the website operator's current Internet platform.[53] Table 1 below summarizes the estimates.

[52] See appendix B for a complete set of the survey questions and cost estimates.

[53] It is my understanding that the PII collection capabilities of affected websites are typically tightly integrated with unique website server software and the website operator's back-end systems for services like customer relationship management, inventory, shipping, and credit. For example, both Amazon.com and BarnesAndNoble.com are booksellers that collect PII, but each has a fundamentally different system architecture that has adapted to their distinct business models. It is possible that some software consultant will create privacy-compliant packaged solutions attractive to businesses that are building their website from scratch. I focus here, however, on existing businesses that already collect online PII and are therefore more likely to require custom solutions

Table 1: Estimated Costs of Designing and Implementing Compliance Systems

Consultant	Paid Labor Hours	Average Labor Cost/Hour	Total Labor Cost	Hardware and Expenses	Total Estimated Cost
1	260	$140	$36,000	$10,000	$46,000
2	270	$120	$32,300	$25,000	$57,300
3	440	$180	$79,900	NA	$79,900
4	570	$70*	$40,000	$4,000	$44,000
5	610	$180	$110,000	$7,500	$110,000
6	640	$170	$110,000	$16,000	$130,000
7	780	$190	$150,000	$27,000	$180,000
8	780	$130	$100,000	$14,000	$120,000
9	790	$150	$120,000	$30,000	$150,000
10	940	$130	$120,000	$110,000	$230,000
11	960	$170	$160,000	NA	$160,000
12	1,000	$130	$130,000	$50,000	$180,000
13	1,300	$90	$120,000	$250	$120,000
14	2,000	$130	$250,000	$70,000	$320,000
15	2,200	$120	$260,000	$75,000	$330,000
16	2,400	$110	$270,000	NA	$270,000
17	3,000	$230	$670,000	NA	$670,000
Mean**	1,100	$150	$160,000	$34,000	$190,000
Median	790	$140	$120,000	$25,000	$150,000
Std. dev.	800	$40	$150,000	$34,000	$150,000

Notes: NA indicates Not Available. *Labor costs represent government rates.**All figures are reported to two significant digits. Std. Dev. denotes Standard Deviation.

The labor costs per hour listed above are fairly similar, despite the various geographic locations of the consultants. The estimated labor hours, however, vary substantially. As is typical with custom solutions, different consulting firms with different resources and methodologies provided varying cost estimates, and some ignored hardware cost altogether. Based on the above survey results, I rely on labor costs and take $100,000 as the cost of custom software that tracks compliance with online privacy access provisions.[54]

3. Industry Impact

How, then, does this expense translate to the community of website operators? First, I estimate the number of U.S. commercial websites, which constitute the majority of sites affected by the proposed laws. In the face of legislation, some portion of the commercial website operators may decide that collecting and sharing PII is not worth the cost. If the benefits that these operators receive from sharing collected PII are less than the cost of the compliance tracking software, then sharing PII and complying with legislation is not profitable.[55] In this case, some websites will either shutdown operations, forgo collecting any PII, continue to collect PII but forgo all information sharing, or decide not to comply with the legislation and risk fines instead.[56]

a. The Number of Affected Websites

The eCommerce: B2B Report for February 2001 reports the number of active, purposeful U.S.-based websites in 2001 as 3,700,000.[57] The eCommerce study breaks the

---

[54] The costs in Table 1 represent the initial cost of implementing a tracking system. They do not include ongoing maintenance or end user support.

[55] Because the costs represent a one-time fee, the net present value of benefits of collecting PII would need to exceed the total cost in order for the website operator to find it profitable to continue collecting PII.

[56] Most provisions only require access if the information is shared, either internally or externally. Therefore, if websites follow a policy of not sharing PII with anyone for any purpose, they would only need to comply with the notice provision.

[57] The report was prepared by eMarketer, a company providing Internet statistics. They define commercially viable in the following way. An "active, purposeful" website provides at least one of the following: interactive customer service or support, a meaningful display of the firm's products or services, and/or regularly updated information. *See* "The eCommerce: B2B Report," *e*Marketer, February 2001, description available at http://www.emarketer.com/ereports/ecommerce_b2b/welcome.html. A second published source, by Netcraft, reports a somewhat higher estimate. They count only sites with distinct content, no matter how many domain and hostnames point at the site. The June 2000 "normal" by-hostname survey found slightly over 17 million

number down further by the size of the website operator: 94,000 of the sites are run by medium to large companies, while small companies run the remaining 3,600,000 sites.[58]

According to the FTC, around 97% of commercial websites collect PII, so the proposed laws could affect as many as 3.6 million sites.[59] However, this number surely includes a great many websites that would choose to stop sharing PII if faced with a $100,000 bill for compliance tracking software. Since I have no way of actually knowing the number of website operators that might stop sharing PII, I calculate three conservative estimates starting with the figures in the eCommerce report. I first assume that only 10% of these websites will need compliance-tracking software. This results in around 360,000 companies. For the second calculation, I assume that only 5% will need the software, for a total of around 180,000 companies. For the third and final calculation, I assume that only the medium and large sites continue to collect and share PII. Under this scenario, the legislation would only apply to 94,000 companies.[60]

b. Industry-Level Costs

Table 2 summarizes the three industry-level cost calculations based on the figures discussed above.

---

sites. Nearly 10 million of these sites are removed from the survey by applying their active sites methodology, which found 7.5 million active sites on 3.4 million IP addresses. *See* "Netcraft Web Server Survey," available at http://www.netcraft.com/survey/index-200007.html#active . For further corroboration, Steve DelBianco spoke with Craig Silverstein, Director of Technology at Google.com, an Internet search engine. (Interview conducted on April 26, 2001). Google determined that there are around 4.5 million commercial websites in the U.S. by visiting actual dot-com sites. The Google estimate does not limit sites to "active and purposeful."

[58] eMarketer defines a small business as having less than 100 employees (not including home offices). A medium business has between 100 to 500 employees, and a large business has greater than 500 employees.

[59] Per the FTC May 2000 study, 97% of U.S.-based commercial websites collect PII. *See* "Privacy Online: Fair Information Practices in the Electronic Market place, A Report to Congress," Federal Trade Commission, May 2000, available at http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf.

[60] It is very difficult to estimate the impact of the proposed legislation on small businesses alone. The eCommerce report highlights the fact that the vast majority of U.S. websites are run by small companies; they represent over 3.6 million of a total 3.7 million websites. To my knowledge, no research has been conducted on which of these small companies will continue share PII if privacy legislation is enacted. Nonetheless, even if I make the extremely conservative assumption that online privacy laws will affect only 1% of websites run by small businesses, the cost to those companies could easily exceed $3 billion (3.6 million websites multiplied by 1%, multiplied by $100,000).

Table 2: Industry-Level Cost Estimates

Assumption	Number of Affected Websites	Industry-Level Compliance Cost (with $100,000 software cost)
10% of commercial sites	361,000	$36 billion
5% of commercial sites	180,000	$18 billion
Medium & large sites	94,000	$9 billion

Because of uncertainties in the both the cost and the number of affected websites, I consider a few sensitivity calculations. First, if hardware cost were included, then the cost for the industry would increase by around 15-30%. Some of the software cost estimates in Table 1 could be high; once the consultants begin to actually write the programs, they may discover the process is easier than anticipated. If the minimum total cost from Table 1 (about $44,000) is used instead of $100,000, the industry impact is reduced by around 50%. On the other hand, if the costs in Table 1 omitted some key, unforeseen requirement, they could understate the cost of compliance software. Using a higher estimate in Table 1 could double the industry-level costs calculated in Table 2.

Based on these conservative approaches, I reach estimates that are, by most standards, quite large. Using several different calculations, the estimates range from $9 billion to $36 billion. This is a wide range but even the lower bound underscores the need for a serious evaluation of both the costs and the benefits of online privacy regulation.

IV. CONCLUSIONS

This study has attempted to provide estimates of the costs of various aspects of proposed online privacy legislation. I found that these costs could be significant, especially for requirements related to access provisions. In particular, having to track how customers' personally identifiable information is shared with other online parties is likely to prove an

expensive undertaking. Using what I believe to be fairly conservative assumptions, I found that these costs easily could be in the billions if not tens of billions of dollars. This fact alone suggests that the regulations that would flow from proposed laws could have a substantial economic impact on consumers and businesses. Based on this analysis I would make the following two recommendations:

Recommendation 1: More information should be obtained on the benefits and costs of proposed online privacy laws prior to passing regulations.

Recommendation 2: That information should be used to determine whether such regulations are warranted.

On the basis of what we know now, I think further regulation of online privacy is premature for three reasons. First, the costs could be substantial. Second, we do not have any good quantitative estimates of the benefits of such regulation. Third, the market is reacting to ensure that at least some of the consumer concerns related to online privacy are being addressed.

Appendix A

Robert Hahn is director of the AEI-Brookings Joint Center for Regulatory Studies, a resident scholar at the American Enterprise Institute, and a research associate at Harvard University. Previously, he served as a senior staff member of the President's Council of Economic Advisers. Mr. Hahn frequently contributes to general-interest periodicals and leading scholarly journals, including the *New York Times*, *Wall Street Journal*, *American Economic Review*, *Science* and *Yale Law Journal*. Most recently, he is the author of *Reviving Regulatory Reform: A Global Perspective* (AEI-Brookings Joint Center, 2000). In addition, Mr. Hahn is cofounder of the Community Preparatory School—an inner-city middle school in Providence, Rhode Island, that provides opportunities for disadvantaged youth to achieve their full potential.

EDUCATION

1977-81 California Institute of Technology, Pasadena, California
M.S., 1979, Ph.D., Economics, 1981

1976-77 Stanford Graduate School of Business, Stanford, California

1971-75 Brown University, Providence, Rhode Island
B.A., Mathematical Economics, 1975
M.A., Economics, 1975
Languages: Spanish
Honors: Phi Beta Kappa

EMPLOYMENT

1998-01 Director, AEI-Brookings Joint Center for Regulatory Studies
1989-01 Resident Scholar, American Enterprise Institute, Washington, D.C.
1997-01 Research Associate, Harvard University, Cambridge, Massachusetts
1990-01 Adjunct Professor of Economics, Carnegie Mellon, Pittsburgh, Pennsylvania
1991-94 Adjunct Research Faculty, Harvard University, Cambridge, Massachusetts
1987-89 Senior Staff Economist, Council of Economic Advisers, Washington, D.C.
1985-90 Associate Professor of Economics, Carnegie Mellon, Pittsburgh, PA
1982-85 Assistant Professor of Economics, Carnegie Mellon, Pittsburgh, PA
1981-82 Research Fellow, California Institute of Technology, Pasadena, California
1981 Instructor, Pitzer College, Claremont, California
1978 Economist, Council on Environmental Quality, Washington, D.C. (summer)
1976 Economist, World Bank, Washington, D.C. (summer)
1975-76 Division Staff, MITRE Corporation, McLean, Virginia
1973-75 Math Teacher, Transitional High School, Providence, Rhode Island

Appendix B
Cost Estimate Survey Results

Survey Respondents:

Company Name	Location	Platform
Active Designs, LLC	Fairfax, VA	Microsoft
Aegis Consulting	McLean, VA	Sun/Oracle/Netscape
Clarity Consulting	Chicago, IL	Microsoft
Compuware	Farmington Hills, MI	Microsoft / Oracle
Crosstier	Fairfax, VA	Microsoft
DevX	Palo Alto, CA	Microsoft
i3 Solutions, Inc.	Sterling, VA	Microsoft
Information Strategies	Washington, DC	Microsoft
IXL	Richmond, VA	Sun/Oracle/Netscape
Mariner	Charlotte, NC	Microsoft
MetroSharp	Dallas, TX	Microsoft
Online Consulting	Wilmington, DE	Microsoft
Progressive Systems Consulting, Inc.	New York, NY	Microsoft
Proxicom	Reston, VA	Unix
Rocketworks, Inc.	Gaithersburg, MD	Microsoft
Rubicon Technologies	Raleigh, NC	Microsoft
WebBranch	Houston, TX	Linux

The individual responses are provided below. To avoid placing the above responding companies at a competitive advantage, the company name associated with each response is redacted. In addition to filling out the survey questions on labor hours and cost estimates, many respondents wrote specific comments on the complexities involved in developing and implementing a PII tracking system.

The Questionnaire Sent to Respondents:

4/16/01

ACT is working with nationally-known economists to analyze costs of compliance with selected privacy laws now proposed in Congress. One element of regulatory impact is the cost to design and implement website software components to comply with regulations and avoid --and prepare for--litigation risks.

That's where you come in. We need several IT systems developers to estimate the cost of building server-side software that meets some of the proposed new privacy laws affecting websites that collect personally identifiable information (PII) from their site visitors.

Please make these assumptions in preparing your estimate:

1. The client already has a website that includes privacy policy pages.
2. The client already has a database of 100,000 users, indicating name, mailing address, email address, date of registration, plus several personal preferences, including an indicator to opt-out of sharing this PII with 3rd parties. Your database design should scale up to 10 million users.
3. The client already has Web pages to allow users to review and update their basic PII and preferences.
4. All source code you develop would become the unrestricted property of the client.
5. All components and database tables must be secured against infiltration from unauthorized users. ID and password is required for user access to PII.
6. Since the client already has a functioning website with user registration, your estimate for design, testing, and implementation should include the effort to integrate new components with existing code and database design.

High-level functional specifications for your new/modified software components:

1. We need to do broadcast email to all users in the database (when client changes privacy policy or has to report a breach of their policy to all users). Each instance of the email must be logged to the tracking database, incl date, user, message text, and indication of whether the email is delivered successfully. Automatically save any emails returned as undeliverable, and update the user database with undeliverable status and date.
2. Whenever we transfer PII to a 3rd party for mailing or marketing purposes, create a tracking record that indicates user, 3rd party, date, and all PII known at the time. Some transfers are mail-merge transactions, where the 3rd party requests email addresses for all users that match given characteristics. These merge transfers must also be tracked as PII sharing, since the 3rd party implicitly knows the characteristics of any user that meet their selection criteria.
3. Users may request an on-line display of all instances where their PII was transferred to 3rd parties (described above). Display should include date, 3rd party name, and the PII transferred.
4. When users change their PII or preferences, write a tracking record indicating user, date of change, nature of the change, and version of privacy policy in effect at time of the change.

5. Any user change to PII or preferences must cascade to all 3rd parties that are in the process of using the previous PII, whether as mail-merge or for extraction and transfer of information. Any change to a user's PII should generate transactions (messages) to each 3rd party known to be using PII for that user (tracked per item 2 above).
6. Our website displays ads that are served by third-party websites, some of which might place cookies on users' computers. Before linking to the ad-server site, we should display a modal response window allowing user to decline the ad link. The window should also allow user to store their preference for 3rd party-cookies for all future visits.

We're just looking for a total cost estimate, but use the itemized table below if it's more convenient.

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model		
Database migration/conversion		
Programming interface and services		
Unit testing		
Integration testing (incl. security tests)		
Procedures for backup and archive		
Project management		
Out-of-pocket expenses		
Storage and server hardware costs		
Total Estimated Cost		

Preferred Operating System	
Preferred Server software (DBMS, web server, etc.)	
Other relevant assumptions you made in preparing your estimate	

Responses Received:

Response 1

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model	80	14000
Database migration/conversion	120	21000
Programming interface and services	150	26250
Unit testing	40	7000
Integration testing (incl. security tests)	120	21000
Procedures for backup and archive	20	3500
Project management	80	13912.5
Out-of-pocket expenses		5000
Storage and server hardware costs		2500
Total Estimated Cost		114162.5

Preferred Operating System	Windows 2000
Preferred Server software (DBMS, web server, etc.)	SQL Server 2000
Other relevant assumptions you made in preparing your estimate	

Response 2

I would still maintain that the cost of implementing the specifications will vary with the number of data elements involved. There's going to be more effort involved in organizations that have 100,000 or 1,000,000 users compared to those that have 1,000 or 10,000. Additionally, organizations that have capabilities in-house to do email blasts and do sell their lists are likely to be in a better position to support any infrastructure changes that may be required.

Upon rereading the specs it occurs to me that items 3 & 5 may be particularly difficult to implement. In many cases, list rentals occur through brokers. When we rent the eWeek subscriber list we get it from a list broker who manages a copy of the eWeek list for such purposes. eWeek itself probably doesn't know that we are using the list. So the system would somehow have to handle data transfers between list brokers and list providers in order to enable on-line viewing of instances of PII transferred to 3rd parties to satisfy spec #3.

Spec #5 doesn't provide a time-frame in which preference must cascade to third parties. My guess is that the eWeek list that the broker rents is only updated a couple of times a year if that. If I'm an eWeek subscriber and I change my PII how will that change get to the list broker and in what time frame?

Here's a breakdown:

Design	100 hrs	$15,000
Convert	40 hrs	$ 5,000
Program	300 hrs	$37,500
Unit Test	80 hrs	$10,000
Integration Test	80 hrs	$10,000
Backup	40 hrs	$ 5,000
Project Management	150 hrs	$28,000
Expenses		$ 5,000
Hardware		$25,000
		======
Total		$145,500

O/S Windows 2000
Server SQL 2000, IIS 5.0

Response 3

Components of your estimate:	**Estimated Man Hours**
Design, technical specifications, data model	280
Database migration/conversion	280
Programming interface and services	840
Unit testing	280
Integration testing (incl. security tests)	280
Procedures for backup and archive	140
Project management	60
Out-of-pocket expenses	0
Total Estimated Man Hours	2,160
Hourly Rate	$120
Estimated Development Cost	$259,000
Hardware (1 x Prod/Test/Dev Servers)	$75,000
Total Estimated Cost	$334,000

Preferred Operating System	**Windows 2000**
Preferred Server software (DBMS, web server, etc.)	SQL Server 2000
Other relevant assumptions you made in preparing your estimate	Site is built using a scripting technology (i.e. JSP, ASP – not ISAPI, CGI) for HTML generation

Assumed Client base: Single client. There would be some economies of scale if we were to do this for multiple clients, but it would not likely exceed a 15% reduction in cost.

Response 4

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model	80	7,200.00
Database migration/conversion	40	3,600.00
Programming interface and services	1060	95,400.00
Unit testing	Inc	
Integration testing (incl. security tests)	160	14,400.00
Procedures for backup and archive	Inc	
Project management	NA	NA
Out-of-pocket expenses		250.00
Storage and server hardware costs		3rd Party
Total Estimated Cost		$120,850.00

Preferred Operating System	Windows 2000 Advanced Server SP1
Preferred Server software (DBMS, web server, etc.)	Microsoft SQL Server 2000
Other relevant assumptions you made in preparing your estimate	1. We do not sell or resell hardware, though we make recommendations for the requirements. Hardware should be purchased through DELL or other manufacturer. 2. The project is not tangible, so estimation could be higher or lower. Assumption is made on past experience. 3. The project is based on Net30 billing, standard rates. A Net7 would receive a 25% discount on hourly rates. Other Net payments are available as well. 4. We assume that the project would have been written in ASP running on IIS5 (Windows 2000). Should this project have been written on MAC OS X, Linux or other non Microsoft Platform or should the project have been written in JSP, Cold Fusion or other the conversion to ASP on Windows would also be required, raising the price dramatically. We work only with Windows 2000 and XP platform for web development and only uses ASP and ASP.Net (ASPX) technology.

Response 5

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model	125	$15,625
Database migration/conversion	25	$3,125
Programming interface and services	625	$78,125
Unit testing	50	$6,250
Integration testing (incl. security tests)	100	$12,500
Procedures for backup and archive	25	$3,125
Project management	50	$6,250
Out-of-pocket expenses	-	0?
Storage and server hardware costs	-	$50,000? (depends on implemented number of users)
Total Estimated Cost		$175,000

Preferred Operating System	Windows 2000 Server (Possibly Advanced Server)
Preferred Server software (DBMS, web server, etc.)	Microsoft SQL Server 2000, Microsoft IIS 5.0, Microsoft Exchange Server 2000
Other relevant assumptions made in preparing estimate	1. Hardware solution for Firewall 2. Multiple servers necessary to scale to 10 million users, assuming 2 million user capacity to start for hardware requirements

Response 6

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model	233	$43,105
Database migration/conversion	38	7,030
Programming interface and services	194	35,890
Unit testing	137	25,345
Integration testing (incl. security tests)	47	8,695
Procedures for backup and archive	7	1,295
Project management	120	26,400
Out-of-pocket expenses		7,300
Storage and server hardware costs		20,000
Total Estimated Cost		$175,060.00

Preferred Operating System	SUN Solaris
Preferred Server software (DBMS, web server, etc.)	Oracle 8.1.7 Netscape iPlanet Webserver Toplink
Other relevant assumptions you made in preparing your estimate	Assumed that three potential outside entities were involved who received information from our site and would require updates when PII changes. Each additional entity would be assumed to require approximately 150 hours effort and $29,000 to implement.

Response 7

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model		
Database migration/conversion		
Programming interface and services		
Unit testing		
Integration testing (incl. security tests)		
Procedures for backup and archive		
Project management		
Out-of-pocket expenses		
Storage and server hardware costs		
Total Estimated Cost	2400	270,000

Preferred Operating System	Solaris / NT
Preferred Server software (DBMS, web server, etc.)	Oracle DBMS, Netscape Web Server, Sybase EAServer
Other relevant assumptions you made in preparing your estimate	Development: ($180,000) Around 3 months (15 weeks) / 3 people = 1800 hours Bill rate of $100/hr Project Manager/Test Coordinator: ($90,000) Around 3 months (15 weeks) = 600 hours Bill rate of $150/hr Travel expenses not factored in. Assumption: All existing HW could handle the requirements and SMTP server software licenses and setup were already in place. All other existing software licenses were also adequate for the project.

Response 8

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model	40 (@ $248/hr)	$9,920
Database migration/conversion	40 (@$175/hr)	$7,000
Programming interface and services	160 (@$175/hr)	$28,000
Unit testing	24 (@$175/hr)	$4,200
Integration testing (incl. security tests)	40 (@$175/hr)	$7,000
Procedures for backup and archive	16 (@$175/hr)	$2,800
Project management	120 (@$175/hr)	$21,000
Out-of-pocket expenses	?	?
Storage and server hardware costs	Should not impact existing hardware configuration.	Should not impact existing hardware configuration.
Total Estimated Cost	440	$79,920

Preferred Operating System	Windows 2000 Advanced Server
Preferred Server software (DBMS, web server, etc.)	SQL Server 2000 Enterprise Edition; IIS 5.0; Exchange 2000
Other relevant assumptions you made in preparing your estimate	The existing system already has email capability. If not, this would impact the hardware configuration, as an SMTP/POP3 server also would be required for handling distribution and storage of email messages.

Response 9

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model	100@$90/hr	9000.00
Database migration/conversion	30@80/hr	2400.00
Programming interface and services	200@$75/hr	15000.00
Unit testing	40@$60/hr	2400.00
Integration testing (incl. security tests)	80@$60/hr	4800.00
Procedures for backup and archive	80@$40/hr	3200.00
Project management	20@$100/hr	2000.00
Configuration Management	20@50/hr	1000.00
Out-of-pocket expenses		2000.00
Storage and server hardware costs		2000.00
Total Estimated Cost		**$43, 800.00**

Preferred Operating System	Windows NT 4.0 w/ SP5
Preferred Server software (DBMS, web server, etc.)	MS IIS 4.0 / Apache Oracle 7.3.x or higher
Other relevant assumptions you made in preparing your estimate	1. All the rates are calculated based on 2001 dollars and are assumed to be good for 90 days. Subsequent to the 90 day period, inflation and market fluctuations need to factored in. 2. All the rates are un-burdened rates. 3. All the personnel are familiar with the system. 4. All the skills are readily available at hand. 5. No downtime for administrative changes is assumed. 6. No server down time is assumed as a result of any unforeseen outages. 7. Other Direct Costs (ODCs) are assumed to be in the range of 15-20% of the project costs. 8. No software licenses cost is included.

Response 10

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model	150	$20250
Database migration/conversion	150	20250
Programming interface and services	320	43200
Unit testing	40	5400
Integration testing (incl. security tests)	40	5400
Procedures for backup and archive	20	2700
Project management	60	8100
Out-of-pocket expenses		3500
Storage and server hardware costs		10000
Total Estimated Cost		$118800

Preferred Operating System	Windows 2000
Preferred Server software (DBMS, web server, etc.)	SQL Server, IIS

Response 11

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model	~40	~ $4,800
Database migration/conversion	~12	~ $1,500
Programming interface and services	~120	~ $15,000
Unit testing	~24	~ $2,500
Integration testing (incl. security tests)	~24	~ $2,500
Procedures for backup and archive	~16	~ $2,000
Project management	~32	~ $4,000
Out-of-pocket expenses		
Storage and server hardware costs		$25,000
Total Estimated Cost	268 hrs	$57,300

Preferred Operating System	Windows 2000
Preferred Server software (DBMS, web server, etc.)	MS SQL Server 2000, IIS
Other relevant assumptions you made in preparing your estimate	Storage and server hardware line item includes system software (OS, RDBMS, other commercial components).

Response 12

I appreciate the opportunity to contribute to your study as I believe this is a very serious matter. In fact, as I reviewed the specs for the 3rd time the very severity of compliance really was brought to bear. I don't find this matter trivial at all. There is a significant amount of tracking required and the onus on business sounds substantial. (To that end, I included a new field to accommodate the legal oversight necessary to ensure data model/execution compliance.)

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model	48	7200
Database migration/conversion	48	7200
Programming interface and services	36	5400
Unit testing	16	2400
Integration testing (incl. security tests)	16	2400
Procedures for backup and archive	12	1800
Project management	48	7200
Out-of-pocket expenses		1000
Storage and server hardware costs	20	9000
Legal	12	2400
Total Estimated Cost		**46000**

Preferred Operating System	NT (or Linux)
Preferred Server software (DBMS, web server, etc.)	MS SQL (or MySQL)
Other relevant assumptions you made in preparing your estimate	1.) Contractual arrangements with the third parties and adjustment of system to comply with other legal requirements necessitated by the comprehensive tracking system and debugging. US$200/hr 2.) Implementation timeline too quick for in-house. At the time such laws are enacted, we would be forced to out source in order to comply within a reasonable period of adoption. US$150/hr. 3.) Independent data storage required to preserve data integrity. Requires installation and configuration. 4.) Out of pocket expenses are miscellaneous and unknown.

Response 13

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model	160	
Database migration/conversion	60	
Programming interface and services	360	
Unit testing	90	
Integration testing (incl. security tests)	130	
Procedures for backup and archive	20	
Project management	120	
Out-of-pocket expenses		$12K
Storage and server hardware costs		$100K
Total Estimated Cost	940	$232,000

Preferred Operating System	Windows 2000 Advanced Server
Preferred Server software (DBMS, web server, etc.)	SQL Server 2000 for database, IIS 5.0 for web server
Other relevant assumptions you made in preparing your estimate	Clustering will be used to scale hardware to accommodate concurrent user loads in multiples of 125. Initial hardware and storage assumes one 2-way box for the web server, one 2-way-box for the application server and one 4-way box for the database. Expenses include travel for requirements gathering, meeting with focus group and deployment and testing. Integration testing includes usability and user acceptance testing. Project management includes time for conducting focus group.

Response 14

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model	40	6000
Database migration/conversion	80	12000
Programming interface and services	240	36000
Unit testing	80	12000
Integration testing (incl. security tests)	120	18000
Procedures for backup and archive	20	3000
Project management	60	9000
Out-of-pocket expenses		1200
Storage and server hardware costs		15000
Total Estimated Cost		127200

Preferred Operating System	Windows NT/2000
Preferred Server software (DBMS, web server, etc.)	SQL, IIS, MTS, Exchange
Other relevant assumptions you made in preparing your estimate	

Response 15

We actually provided this functionality to one of our clients 3 months ago. The changes were deployed on 36 live NT 4.0 production servers. I have limited the costing to the functionality that is in the spec.

Effort:	960 Hrs
Average Billing Rate:	$165.00
Total cost:	$158,400

Response 16

Components of your estimate:	**Estimated Labor Hours**	**Estimated Cost**
Design, technical specifications, data model	298	37,350
Database migration/conversion	298	37,350
Programming interface and services	697	87,150
Unit testing	99	12,450
Integration testing (incl. security tests)	249	31,125
Procedures for backup and archive	49	6,225
Project management	298	37,350
Out-of-pocket expenses		
Storage and server hardware costs		70,000
Total Estimated Cost	1988	319,000

Preferred Operating System	Windows 2000
Preferred Server software (DBMS, web server, etc.)	SQL Server 2000, IIS, ASP.NET, LSMTP, ListServer HPO
Other relevant assumptions you made in preparing your estimate	Does not include costs of software licenses. Hardware may need to be scaled up based on mailing volumes. Assumes database in place.

Response 17

PHASE/ SEGMENT/	TASK	DESCRIPTION	PH/SEG TOTAL	NOTES
1.1		**PLAN PHASE**	**9**	
1.1.1		**DISCOVER PROJECT OBJECTIVES**	**3**	
	1.1.1.1	Conduct Kick-Off Workout		
	1.1.1.2	Define High-level Requirements		
1.1.2		**PREPARE PROJECT PLAN**	**3**	
	1.1.2.1	Validate Effort Estimate		
	1.1.2.2	Plan Effort		
1.1.3		**PREPARE FOR PROJECT LAUNCH**	**3**	
	1.1.3.1	Create Define Phase SOW		
	1.1.3.2	Organize Effort		
1.2		**DEFINE PHASE**	**30**	
1.2.1		**DEFINE BUSINESS REQUIREMENTS**	**24**	
	1.2.1.1	Conduct Business Area Workouts		
	1.2.1.2	Model Business Events and Processes		
	1.2.1.3	Develop Conceptual Data Model		
	1.2.1.4	Develop Business Requirements Document		
1.2.2		**DEFINE TECHNICAL REQUIREMENTS**	**6**	
	1.2.2.1	Conduct Technology Workout		
	1.2.2.1	Research Architecture Options		
	1.2.2.3	Develop Technical Requirements Document		
1.2.3		**DEFINE CREATIVE REQUIREMENTS**		
	1.2.3.1	Conduct Creative Workout		
	1.2.3.2	Develop Creative Brief		
1.3		**DESIGN PHASE**	**69**	
1.3.1		**DESIGN SITE ORGANIZATION**	**0**	
	1.3.1.1	Design Functional Site Flow		
1.3.2		**DESIGN CREATIVE SITE COMPONENTS**		
	1.3.2.1	Design Preliminary Wireframes (for Comps)		
	1.3.2.2	Develop Comp Alternatives		
	1.3.2.2	Select / Refine Comp		
1.3.3		**DEFINE FUNCTIONAL SPECIFICATION**	**15**	
	1.3.3.1	Develop Page Wireframes		
	1.3.3.2	Develop Page Specifications		
	1.3.3.3	Specify Additional Functions (Non-UI)		
	1.3.3.4	Specify Reports		
	1.3.3.5	Complete Functional Specification Document		

Response 17 Continued

1.3.4		**DESIGN TECHNICAL ARCHITECTURE**	**14**	
	1.3.4.1	Research / Design Technical Architecture		
	1.3.4.2	Procure Development Environment Components		
1.3.5		**DESIGN SOFTWARE COMPONENTS**	**41**	
	1.3.5.1	Design Interfaces		
	1.3.5.2	Design Common Architecture Services		
	1.3.5.3	Design/Prototype Difficult Data Structures		
	1.3.5.4	Design/Prototype Straightforward Data Structures		
	1.3.5.5	Design/Prototype Difficult Application Modules		
	1.3.5.6	Design/Prototype Straightforward App Modules		
1.4		**DEVELOP PHASE**	**132**	
1.4.1		**DEVELOP UI PROTOTYPE / TEMPLATES**	**0**	
	1.4.1.1	Develop HTML Page Templates		
	1.4.1.2	Develop Report Templates		
	1.4.1.3	Develop Site Graphics		
	1.4.1.4	QA/Revise Prototype Design		
1.4.2		**IMPLEMENT ARCHITECTURE COMPONENTS**	**32**	
	1.4.2.1	Install and Set up Development Environment		
	1.4.2.2	Implement and Test Common Services		
	1.4.2.3	Implement and Maintain Development Database		
	1.4.2.4	Maintain Software Configuration		
1.4.3		**IMPLEMENT SOFTWARE COMPONENTS**	**56**	
	1.4.3.1	Code Straightforward Modules		
	1.4.3.2	Code Difficult Modules		
	1.4.3.3	Code Interfaces		
	1.4.3.4	Code Reports		
	1.4.3.5	Manipulate & Load Static Content		
	1.4.3.6	Perform Unit Test		
1.4.4		**PROVIDE FUNCTIONAL DESIGN SUPPORT**	**11**	
	1.4.4.1	Resolve Functional Design Questions/Issues		
	1.4.4.2	Revise Functional Specification		
1.4.5		**DEVELOP TEST PLAN**	**6**	
	1.4.5.1	Develop Integration and System Test Plan		
	1.4.5.2	Prepare and Load Test Data		
1.4.6		**PERFORM INTEGRATION TEST**	**25**	
	1.4.6.1	Conduct Integration Test		
	1.4.6.2	Fix Integration Test Defects		
1.4.7		**DEFINE PRODUCTION ENVIRONMENT**	**3**	
	1.4.7.1	Define Operational Requirements *(Scheduling, Backups, etc.)*		
	1.4.7.2	Specify Production Environment		

Response 17 (continued)

1.5		**DEPLOY PHASE**	**20**	
1.5.1		**MIGRATE TO PRODUCTION TES T**	**5**	
	1.5.1.1	Install Production Code to Production Test Environment		
	1.5.1.2	Convert / Migrate Application Data to Test Environment		
1.5.2		**CONDUCT SYSTEMS / ACCEPTANCE TEST**	**5**	
1.5.3		**PRODUCTION MIGRATION**	**10**	
	1.5.3.1	Migrate Site to Production		
	1.5.3.2	Convert / Migrate Application Data to Test Environment		
	1.5.3.3	Support Production Launch		
		SUB - TOTAL DAYS	**260**	
1.6.1		**MANAGE PROJECT**	**52**	
		TOTAL DAYS	**312**	
1.6.2		**CONTINGENCY**	**62**	days
		TOTAL DAYS WITH CONTINGENCY	**374**	days
		BASE COST ESTIMATE (In $1000s)	**$673**	,000

Appendix C
Glossary of Technical Terms

B2B (Business to Business) Describes transactions between and among businesses.

Browser An application program that lets a user interact with information resources on the Internet, or World Wide Web.

Cookie Information file placed on the user's computer by a website that collects data about the user and the Internet sites visited. Each cookie contains a list of website addresses with which a browser may share cookie information. By storing a user's ID for a particular website in a cookie, the user no longer needs to re-enter identifying information when returning to the site.

IP Address (Internet Protocol Address) Identifier for a particular network and device on the Internet. The identifier is a unique string of numbers, usually shown in groups separated by periods. (e.g., 123.123.23.2) All resources on the Internet must have an IP address

P3P (The Platform for Privacy Preferences Project) A technical protocol enabling a user's Web interaction software to automatically determine the privacy policies of a website, and warn or block access if the site's policy does not match the user's preferences.

PII (Personally Identifiable Information) Any data used to identify, contact, or locate a person, including name, address, telephone number, or E-mail address.

Third Party An Internet resource other than the first party (the user) or the second party (the Internet website requested). Advertising services and email marketing vendors are considered third parties in this context.

URL (Uniform Resource Locator) The address of a resource accessible on the Internet. Each URL includes the protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and a location for a specific file. The resource can be an HTML page, an image file, a program, or any other file supported by the protocol.

Web Beacon (also referred to as a "Web Bug") An image embedded on a Web page or in an email message that is designed to monitor whether a computer is accessing a particular Web page or email message. A Web Beacon can be as small as 1-by-1 pixel in size, usually having no color. Information collected might include the IP address of the user's computer, the URL of the page the Web Beacon came from, and the time it was viewed.

Appendix D

Diagram for Websites Sharing PII