ROBERT GELLMAN
Privacy and Information Policy Consultant **202-543-7923**
419 Fifth Street SE **Fax: 202-547-8287**
Washington, DC 20003 **rgellman@cais.com**

Privacy, Consumers, and Costs

How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete

Robert Gellman
Privacy and Information Policy Consultant
<rgellman@cais.com>

March 2002

Privacy, Consumers, and Costs

How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete

Table of Contents

Support for this paper came from the Digital Media Forum. The Digital Media Forum is a project of the Ford Foundation to encourage collaboration among its grantees in the area of media policy. This paper reflects the views of the author, not necessarily the views of the Ford Foundation, Digital Media Forum, or participants in the Digital Media Forum.

Copies of this paper can be accessed at:
<http://www.epic.org/reports/dmfprivacy.html>
<http://www.epic.org/reports/dmfprivacy.pdf>
<http://www.cdt.org/publications/dmfprivacy.shtml>
<http://www.cdt.org/publications/dmfprivacy.pdf>

Privacy, Consumers, and Costs

How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete

Executive Summary

Privacy is an elusive, value-laden concept, and it is hard to reach consensus on a definition. In recent, self-serving studies, the business community seized upon this lack of clarity to distort debates about the true costs of privacy – costs to individuals, society and to the business community itself. These studies have led to a mainly one-sided public discussion of privacy, overstating the costs to businesses, ignoring the costs consumers incur to protect their privacy, and understating the benefits that privacy offers to commerce and to society.

The cost of privacy is a legitimate issue, but the studies and the conclusions drawn from them have serious flaws. They suggest that:

- consumers' demands for privacy are irrational and that consumers do not know what is in their own interest,
- unrestricted trafficking in personal information – the very thing that business wants – always benefits individuals and
- privacy can be evaluated only on the basis of monetary costs and benefits.

In fact, the costs incurred by both business and individuals due to incomplete or insufficient privacy protections reach tens of billions of dollars every year.

Shortcomings with Business Studies

The privacy cost studies sponsored by the business community suffer from a variety of defects. Studies of the credit reporting system seek to prove that the free flow of credit records benefits consumers while ignoring the benefits of legislation that gives consumers a wide range of privacy protections and legal remedies. These policies demonstrate how privacy can be compatible with business success in the marketplace.

Some studies, offered as objective but written by trade association employees, rely on old business models that assume that past information-intensive marketing methods are the only way to do business in the future. New ways to find consumers are ignored, as is the amount of business lost under current practices because of privacy concerns.

Calculating consumer benefits is the basis for some cost/benefit estimates. However, the definition of consumer benefits is so broad as to include the nonconsensual sale and exploitation of consumer information that most, if not all, consumers would reject, if given an informed choice.

Costs to Business of Not Protecting Privacy

The *absence* of privacy rules imposes expenses on businesses that many industry-sponsored studies ignore when calculating the costs of privacy. For example, consumers routinely abandon shopping carts on websites because of demands for too much personal information. Analysts estimate that Internet retail sales lost due to privacy concerns may be as much as ***$18 billion***.

Attempts by business to show losses from privacy protections often reflect only traditional models of marketing that may be less effective than privacy-friendly approaches. Relationship marketing – based on the use of large amounts of personal information – may not be as effective as permission marketing, where consumers select what advertising they want to see.

Because many other countries have comprehensive privacy laws, the United States is significantly behind international privacy standards. The European Union limits the export of data to organizations in countries that do not have adequate privacy protections. The result is lost opportunities for U.S. businesses and higher costs when providing privacy protections for imported personal data. Better U.S. privacy protections could expand international business opportunities and reduce costs.

Accumulated personal data is increasingly attractive to law enforcement agencies, other businesses, and private litigants. Businesses are spending more and more time and money responding to subpoenas for their compilations of personal data.

Investors lost hundreds of billions of dollars in companies with business models based on exploiting personal information obtained from Internet users. The lack of privacy protections led many to believe wrongly that personal data could be exploited without limit.

The Costs Consumers Incur When Privacy Is Not Protected

When laws and practices do not provide adequate protections for personal information, individuals act to protect themselves and their privacy. The costs incurred by individuals to protect themselves from unwanted view or intrusion constitute a *privacy toll* paid in both dollars and time. The privacy toll includes costs associated with higher prices, stopping junk mail and telemarketing calls, avoiding identity theft and protecting privacy on the Internet. **A privacy sensitive family could spend between $200 and $300 and many hours annually to protect their privacy.**

Supermarket frequent shopper cards and other registration and monitoring programs coerce consumers to sell their personal information for lower prices at the cash register. Customers unaware of or unwilling to sign up for these programs often pay more.

Traditional junk mail is a longstanding consequence of the inability of individuals to control the collection, compilation, and sale of their personal information. The average person receives more than ten pieces of junk mail each week, of which nearly half is discarded unopened and unread. Opting out of junk mail often requires writing multiple letters, which is a small expense, but still a significant barrier for most individuals.

About 80% of Americans strongly object to receiving unsolicited sales calls and, to prevent or deter these telemarketing calls, many households buy services such as Caller ID, call waiting, answering machines or voice mail, and unlisted or unpublished numbers. Some estimate that 25% of households pay an average of $1.50/ month to be unlisted. The total price that telephone subscribers pay for privacy-protecting services is more than ***$400 million/year***.

Identity theft is a growing threat that creates financial and other hardships for hundreds of thousands of individuals each year. Identity theft results in part from the ready availability of personal information and the lack of protections that would give individuals more control over that information. It can take years of hard work and hundreds or thousands of dollars in out-of-pocket expense before all vestiges of identify theft are removed from a victim's record. In the interim, a victim of identity theft may be unable to obtain a job, purchase a car, or qualify for a mortgage. Government agencies advise individuals seeking protection against identity theft to purchase copies of credit reports annually or to subscribe to credit watch services. Annual costs for a family can easily exceed one hundred dollars annually while estimates of losses for financial institutions appear to be in the ***hundreds of millions***. Identity theft undermines consumer confidence, deters the growth of electronic commerce, and increases costs that may be passed on to consumers.

Unwanted commercial electronic mail, often called spam, imposes costs on Internet users who cannot control the collection and sale of their email addresses. Users spend hours each year downloading and deleting spam. Spam also raises costs for Internet providers, delays service to users, and undermines the vitality of the Internet as a means of open communications. Estimates are that worldwide costs of spam range from ***$8-10 billion***.

Broader effects of the lack of privacy cannot be measured in dollars. The effects on individuals and institutions due to the evolving "dossier society" are significant and often unwelcome. Non-economic interests protected by privacy policy and laws include avoiding solicitations, the exercise of First Amendment rights, and protection of children.

Introduction: What Do We Mean by Privacy?

Privacy is an elusive, value-laden concept, and it is hard to reach consensus on a definition. Academic literature includes contributions from many different disciplines addressing the real meaning of privacy. The definitional problem will not be solved in this paper.

However, an international consensus does exist for those elements of privacy that relate to the collection, maintenance, use, disclosure, and processing of personal information. In the last twenty years, *fair information practices* have become an international standard for privacy. Virtually all privacy laws enacted around the world in recent years are an implementation of fair information practices.

Fair information practices include these elements:

> 1) Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> 2) Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
>
> 3) Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
>
> 4) Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except: a) with the consent of the data subject; or b) by the authority of law.
>
> 5) Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
>
> 6) Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
>
> 7) Individual Participation Principle: An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data

> relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
>
> 8) Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.[1]

Trade associations and others often restate the elements of fair information practices and simply leave out inconvenient elements. The Federal Trade Commission is guilty of this. For example, some of these restatements have a principle of *choice*. That represents a considerable watering down of the principles of use limitation and purpose specification. Fair information practices call for personal information to be used in clearly defined ways identified in advance. The notion of *choice* is a distortion because it allows any use of data as long as the data subject has been offered some opportunity, no matter how difficult or remote, to object.

In analyzing the costs of privacy for personal information, some elements of fair information practices may be low in cost or in marginal cost. For example, maintaining high quality, accurate health records is essential to the practice of medicine, and it is something routinely done by health care providers. The marginal outlays from a privacy perspective may be zero because the health care system already requires high quality data. In any event, the benefits of high quality health data exceed the cost. The same may be true for other elements of fair information practices. Security offers another good example. In the absence of good security, a website may fail entirely due to thieves, hackers, and lack of customer confidence. In these circumstances, privacy is not a luxury or an irrelevancy. Privacy can be an essential component of a successful business.

Accounting for privacy costs can be just as tricky as defining privacy. Some activities that serve privacy also serve other objectives. The marginal cost for privacy may be zero or low. In other cases, a cost accounting methodology for sharing costs between overlapping objectives may be appropriate. Most of the cost "studies" to date include no cost accounting or refuse to recognize the benefits that result from privacy protections.

---

[1] Organization for Economic Cooperation and Development, *Council Recommendations Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 20 I.L.M. 422 (1981), O.E.C.D. Doc. C (80) 58 (Final) (Oct. 1, 1980), at <http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM>.

I. Selected Shortcomings of Business Studies

Elements of the business community argue that privacy rules would cost consumers through higher prices, greater burdens, and fewer opportunities. This argument has been put forward in part through a series of commissioned "studies" written or sponsored by the Financial Services Roundtable, the Direct Marketing Association, the Association for Competitive Technology, and others.[2] The cost of privacy is a legitimate issue, but the studies and the conclusions drawn from them have serious flaws, poor definitions, and questionable methodology.

The business studies include:

- A study about the benefits from the availability of consumer credit information that shows the credit system produces consumer benefits. More important, but unmentioned in the study, is its demonstration that the marketplace for consumer credit information can operate to the benefit of both businesses and consumers under a federal privacy law that gives consumers real privacy rights and remedies.
- In-house work done by a trade association whose members profit greatly from the existing unregulated market in personal information.
- Identified "consumer benefits" resulting from the use of personal information that few consumers would find beneficial.
- Cost estimates for implementation of privacy requirements that have little credibility because the requirements were selectively chosen to be costly, because the estimators had no incentive to reduce costs, because no attempt was made to collect real information about real world costs for existing privacy laws and practices, and because the study ignored the benefits that would result from privacy.

The studies suggest that consumer demands for privacy are irrational and that consumers do not know what is in their own interest. They suggest that unrestricted trafficking in personal information – the very thing that business wants – actually benefits data subjects. They suggest that privacy can be evaluated only based on monetary costs and benefits. It is hard to accept these suggestions or the notion that the business community can fairly represent consumer privacy interests.

In some circumstances, it is surely true that the availability of personal information increases the efficiency of markets in a way that benefits both consumers and businesses. Implementing privacy policies also has some associated costs. It is easy, however, to overstate the case by cherry-picking the costs and consequences on one side while ignoring the other side of the issue. For example, automobiles appear to be even more beneficial as modes of transportation when you ignore the cost of pollution and accidents.

In the privacy arena too, most business studies simply ignore a major side to the debate. Unrestricted trafficking in personal information has negative consequences for consumers and

[2] Many of these papers are available at <http://www.privacyalliance.org/resources/research.shtml>.

imposes significant costs on them. Consumers pay for unlisted numbers, buy credit reports to look for evidence of identity theft, and spend time and effort evading, wading through, or disposing of through junk mail and spam. The costs to individuals resulting from a lack of privacy protections constitute a *privacy toll* measured in dollars and in hours. The lack of privacy also has effects on society at large and not just on individuals. Existing institutions and policies, as well as the growth of the Internet as a communications medium, have been adversely affected by the lack of privacy.

A. The Credit Reporting System Shows that Privacy Can Be Compatible With Profits

Some industry-supported studies argue that the free flow of credit records benefits consumers. For example, one study concludes:

> Credit bureau data has brought consumers lower prices, more equitable treatment, and more credit products to millions of households who would have been turned down as too risky just a generation ago. The U.S. credit reporting system also has made consumers (and workers) more mobile by reducing the cost of severing established financial relationships and seeking better opportunities elsewhere.[3]

Undoubtedly, there is much truth in these conclusions about the benefits to consumers. Looked at from another perspective, the credit study proves that business and consumer benefits can be provided in an environment that respects the privacy of data subjects.

Credit data and marketing data are different for many reasons. In a privacy context, the principal difference is that credit data is subject to relatively strong privacy laws but marketing data is almost completely unregulated. The Fair Credit Reporting Act[4] establishes a reasonable set of fair information practices for credit records maintained by credit reporting agencies. The Act regulates collection, maintenance, retention, and disclosure of credit data. Consumers have statutory rights of access and correction. The Act is enforced both by an administrative agency and through private rights of action.

The American credit reporting experience demonstrates that privacy rules can be compatible with business success in the marketplace for personal information. The credit reporting industry appears to be flourishing and profitable today. The benefits to businesses and to consumers from credit reporting have been achieved in the presence of enforceable privacy laws. The Fair Credit Reporting Act may not be a perfect privacy law or the best model for regulating the privacy of other personal data. However, it demonstrates that privacy laws do not impose an impenetrable barrier to beneficial and profitable uses of consumer data. Indeed, it may well be that the American credit reporting industry is as successful as it is and is tolerated by consumers because it rests on a firm statutory foundation of privacy.

---

[3] John M. Barron and Michael Staten, *The Value of Comprehensive Credit Reports: Lessons from the U.S. Experience* (2000) <http://www.privacyalliance.org/resources/research.shtml>.

[4] 15 U.S.C. §1681 et seq.

B. Studies Based on Old Business Models

Industry arguments are sometimes based on old models of doing business. One study on the impact of data restrictions on consumer distance shopping illustrates this point.[5] The study was conducted by a subsidiary of the Direct Marketing Association and written by its executive director. It is difficult to take the result as objective or as reaching anything other than a pre-ordained conclusion.

The study rests largely on the assumption that the catalog business will be mostly unchanged in the future, and the methods of the past will continue to be the most effective methods in the future. Based on these assumptions, without any careful considerations of alternative ways of finding customers, without paying enough attention to the marketplace changes that the Internet is producing, and without considering that consumers may change the way they shop, the study finds that information restrictions would raise costs to catalog merchants.[6]

The tip-off comes in one of the closing paragraphs of the report, where the possibility of change is finally mentioned but remains unanalyzed:

> If companies find an alternative to catalogs as a way to successfully promote Internet apparel sites online, then it is possible that data restrictions would have less of an impact on the cost of buying apparel online than through catalogs. In this case, the interactive nature of the Internet would allow consumers to identify directly the type of products they are looking for and would make it less necessary for companies to use external information to identify interested consumers in advance.[7]

We can carry this analysis a step further because the data merchants at the Direct Marketing Association will not. The DMA's members generate large revenues by collecting and selling personal information. The DMA has little incentive to discuss methods of finding customers that would reduce those revenues. If privacy were suitably protected or were not affected by new methods of finding customers, catalog merchants might attract more business from privacy conscious consumers who would buy without having their data collected, compiled, and resold. The DMA study does not examine this side of the issue.

Because of the common practice of collecting and selling consumer data without consent, the catalog industry loses customers who are privacy sensitive. How many potential customers refuse to buy from catalog merchants because of the practice of data reuse and data resale without consent? Millions of consumers have opted-out through the Direct Marketing Association's mail preference service. Millions more would do so if knowledge of the service were more widespread and reasonable opt-out methods were provided. Many of those who do not opt-out still discard catalogs unopened.

---

[5] Michael A. Turner, *The Impact of Data Restrictions on Consumer Distance Shopping* (2001).

[6] The study also concludes that all of the increased costs would be passed on to consumers. It is far from clear that costs could be fully passed on to consumers by one class of merchants in a competitive marketplace.

[7] Id. at 43-44. The very last paragraph of the last appendix to the report also offers another brief mention of alternatives. Id. at 56.

A greater respect for consumer privacy might well entice more consumers back into a marketplace that they perceive as privacy invasive. Part of the *privacy toll* paid by consumers today comes in the form of unwanted and non-consensual uses and disclosures of their personal information. If this privacy toll were reduced, then more consumers might be willing to do business with direct marketers. The gains might well exceed any potential losses from new restrictions on personal information.

Another shortcoming is a failure to consider how privacy can be protected in a way that is compatible with the interest of businesses to deal with consumers in a personal, one-to-one, fashion but without identifiers. New methodologies also allow website operators to compile aggregate market research data without compromising privacy. The Center for Media Education documented creative solutions adopted by websites following passage of the Children's Online Privacy Protection Act.[8]

C. Just What Constitutes a Consumer Benefit?

A study conducted for the Financial Services Roundtable argues that information sharing among financial institutions produces large amount of consumer benefits. Without doubt, there are some benefits to some information sharing activities. However, the study is filled with broad conclusions that have little clear basis.

For example, the study never clearly defines what constitutes a consumer benefit. Everything that increases bank revenues or profits cannot be fairly characterized as a consumer benefit. If a bank shares customer information with a third party and profits from the products and services sold to the consumer by the third party, some would count this activity as a consumer benefit. Let's see how that works in the real world with a real example.

In 1999, U.S. Bancorp assembled information about its customers from its own databases and those of others and then sold the information under contract to a telemarketing firm. The information disclosed included credit card numbers, credit limits, checking account numbers, account balances, and Social Security Numbers. Consumers were not notified about the sale of their data nor asked for their permission. The bank received commissions equal to 22 percent of the telemarketer's net revenues.

U.S. Bancorp's information sharing with telemarketers is the type of data sharing that appears to create consumer benefits according to the analysis presented in the Financial Services Roundtable study. The study counts as consumer benefits promotions provided to consumers with proactive offers, the sharing of data that enabled the telemarketer to have a pre-filled application, a reduction in the amount of junk mail that consumers might have received, and the availability of third party services.

---

[8] *Children's Online Privacy Protection Act (COPPA) - The First Year* at 8 (2001) <http://www.cme.org/children/privacy/coppa_rept.pdf>.

Would consumers agree with the characterization of the information sharing as creating a consumer benefit? Another view of the same "consumer benefit" comes from a lawsuit that was filed by the Minnesota Attorney General alleging that the data selling was an illegal violation of privacy. A few days after the suit was filed, U.S. Bancorp settled the suit without admitting guilt. The bank agreed to contribute profits gained from sales that telemarketers made to bank customers. The bank also agreed to give Habitat for Humanity in Minnesota $1.5 million, the state $500,000, and charities and others $1 million. Whether the Financial Services Roundtable would also count the payments by the bank to the state and to charities as a "consumer benefit" is not clear. Presumably, however, the higher price paid by the consumer for the telemarketer's service to support the 22% commission to the bank could have counted as another consumer benefit.

Some telemarketing campaigns are only profitable if the callers already have the credit card numbers of the individuals being called. The U.S. Bancorp data transfer may be an example of a telemarketing activity that would not have been successful without pre-acquired billing information from the bank. When individuals must disclose a credit card number over the telephone, it dissuades them from buying the product or service being offered. How can we evaluate this factor in determining whether there was a consumer benefit from the transaction? If consumers would not buy but for the nonconsensual transfer of personal information to a telemarketer, how meaningful is the consumer benefit?

It is one thing for a bank or other institution to use customer data internally to offer goods and services to its own customers. Banks may also contract with another company to operate its network of ATM machines. These activities involve data use and sharing that customers are more likely to accept if reasonable conditions attach to the transfer. These uses and disclosures can reasonably be identified as consumer benefits most of the time. However, the broad generalities of the study lump those benefits along with much more questionable consumer benefits.

Consumers know what benefits them, and not all data sharing activities that are designed to enrich data holders qualify. It is hard to believe that many U.S. Bancorp customers would have agreed to the data sharing of credit card and Social Security numbers with a telemarketer, and the bank surely knew this. It shared the data anyway, until it was caught. If consumers actually derive benefits from sharing, then perhaps they should be given the opportunity to decide for themselves about many proposed disclosures.

The presumption in the Financial Services Roundtable study that the banks can fairly define what is good for consumers is hard to accept. Without more information about the way in which consumer benefits were calculated in the study, it is hard to evaluate the results. It is clear that data sharing benefits the banks, but the extent of customer benefits remain open to considerable debate.

D. Cost Estimate Problems

A study by Robert Hahn purports to identify the costs of proposed online privacy legislation.[9] Mr. Hahn is Director of the AEI-Brookings Joint Center for Regulatory Studies, and the study was paid for by the Association for Competitive Technology, an industry trade association.

The study might be called a *press release study*. It was designed and conducted to produce a huge number that could be quoted in industry press releases. The study produced a cost estimate of as much as $36 billion. What's wrong with the study?

First, the privacy requirements came from Hahn's interpretation of introduced privacy bills. Hundreds of privacy bills have been introduced in recent years. Why Hahn chose some bills for costing and not others is not clear. Further, bills that have not been honed by the legislative process are often filled with broad and loose ideas. Costing bills at an early stage is not a meaningful exercise. Privacy principles can be implemented in dozens of different ways. No two countries around the world have the same precise requirements. Hahn's requirements appear to have been selected to establish as high a cost as possible.[10]

Second, the estimates have little credibility. They come from contractor surveys of the "initial costs" of meeting defined requirements. Those who were surveyed were told that it was for a study, so there was no need for estimators to sharpen their pencils. They were not bidding on real jobs where there would be pressure to keep costs down. The estimates ranged from $46,000 to $670,000. The extremely wide range of estimates suggests that the requirements were not well defined or that there were other flaws. Further, the estimates covered the "initial cost" of compliance. How much would it cost to do the same work a second time? Probably considerably less. A contractor with the prospect to sell the same work to another website could charge a much smaller amount. However, one of the study's requirements was that the source code belonged to the client. A change in this single technical specification might have made an enormous difference in the actual price.

Third, Professor Peter Swire criticized the study for, among other things, not defining a baseline.[11] The cost of any privacy legislation is the difference between what industry would do in the absence of a law and what it would do if the law were enacted. Swire pointed out that many Internet companies have already taken some steps to implement a privacy policy. The incremental cost of new requirements would be less than the cost reported in the study, and the incremental cost might be small or even zero in some instances.

Fourth, the study mentions several existing privacy laws, but it includes no attempt to discover the costs of compliance with those laws. If we want to know what privacy laws cost, then the

---

[9] *An Assessment of the Costs of Proposed Online Privacy Legislation* (2001) <http://www.actonline.org/issues/privacystudy.asp>.

[10] When the Privacy Act of 1974 was being considered, the Office of Management and Budget estimated that annual costs would be $200-$300 million per year, with a one-time startup cost of $100 million. Once the law was in place, the actual startup costs were less than $30 million and that first year operating expenses were less than $37 million. Privacy Protection Study Commission, Personal Privacy in an Information Society at 500 (1977).

[11] *New Study Substantially Overstates Costs of Internet Privacy Protections* (2001) <http://www.osu.edu/units/law/swire1/hahn.doc>.

best source is to look at real laws implemented by real companies. This approach was rejected. It is quite likely that the actual cost of many existing privacy laws is relatively small, probably orders of magnitude smaller than the estimates that Hahn produced. A study of actual costs might not have produced the desired results. Another useful approach might have involved identifying the costs of voluntary compliance with company or industry codes. Reliable information might have been available for self-regulatory activities, but no attempt was made to identify any real costs.

Fifth, the study makes no attempt to quantify the costs incurred by companies that have already adopted privacy policies. One reason may be that evidence showing that companies have voluntarily chosen to have privacy policies undercuts the pre-ordained conclusion of the study that privacy is not worth the cost. It is apparent that any company that voluntarily agreed to a privacy policy concluded that the benefits outweigh the cost.

Sixth, other countries have privacy laws today that cover online activities. All fifteen members of the European Union have privacy laws, and many have had laws in place for decades. In addition, New Zealand and Hong Kong are other countries that have considerable experience with private sector privacy laws. The study does not include a single actual cost figure from any other country. Why? Perhaps the collection of real world data would not have supported the striking number that the study sponsors wanted in the press release.

Finally, does privacy save money? The study did not consider any savings that might have resulted from the application of fair information practices to websites. Cost savings might result from higher quality and more accurate data, from avoidance of retention of unnecessary or duplicative data, or from better information processing practices. Other likely benefits include increased sales to privacy sensitive customers, improved customer relations, and avoidance of litigation costs from privacy lawsuits.

E. Other Studies

The privacy cost "studies" are now multiplying in number and compounding the errors. A newer entry in the field relies upon and accepts as gospel many of the other flawed "studies" discussed here. A paper, funded by the Direct Marketing Association and the California Chamber of Commerce, purports to show the costs of opt-in privacy laws in California.[12] There can be no question that an opt-in law would have costs and consequences. However, privacy protections include other elements other than opt-in, and not all proposals for improved privacy call for opt-in requirements. It is noteworthy that many foreign data protection laws, for example, allow for marketing uses of personal information under an opt-out scheme.

Some of the problems with the paper are:

· The assumption that no one would opt-in. It may be that in a regime that protects privacy fairly, more people would agree to the use of their information in ways that might be

[12] Peter A. Johnson & Robin Varghese, *The Hidden Costs of Privacy: The Potential Economic Impact of 'Opt-In' Data Privacy Laws in California* (2002) <http://www.the-dma.org/cgi/registered/whitepapers/costofprivacy.pdf> (registration required).

objectionable without the protections. For example, privacy-sensitive individuals might make new charitable contributions if they knew that they would not be inundated with other solicitations.

· The attempt to draw a connection between the cost of mortgages and an opt-in requirement. Without a doubt, higher interest rates will make home ownership more expensive. But people seeking mortgages already opt-in when they apply. They can accept or reject the terms under which mortgages are offered. If there is any nexus between opting-in and mortgage rates – a point not demonstrated by the authors – then people can opt-in to the mortgage that offers lower rates and the supposed extra costs will disappear.

· The failure to consider other ways that business and charities can solicit individuals to replace any losses from opt-in requirements. Newspaper, Internet, radio, and television advertising may be effective substitutes for direct mail. There are other ways to approach individuals without the compilation of detailed personal dossiers. None of the alternatives is adequately considered.

II. The Costs Businesses Incur by NOT Protecting Privacy

The absence of privacy rules directly affects the interests of and costs incurred by data subjects. It also, however, can affect record keepers. Companies that do business with consumers can pay a price when those consumers react to the lack of privacy afforded by the companies or by the general environment.

A. Sales Losses Due to Lack of Privacy

The growth in Internet sales has been spectacular, but the lack of adequate controls over the use and disclosure of personal information has taken a significant toll. Internet users fill and then abandon shopping carts in huge numbers. One study suggests that four out of five consumers try to purchase online and give up. The two leading reasons are 1) too much information has to be provided; and 2) unwillingness to enter credit card details.[13]

Other studies and surveys also show the importance of privacy in the online environment. In a recent report to the Congress, the Federal Trade Commission estimated that lost online retail sales due to privacy concerns may be as much as $18 billion. The FTC also cited a study showing that 92% of respondents from online households stated that they do not trust online companies to keep their personal information confidential.[14] This lack of trust takes a heavy toll on e-business.

If industry can legitimately make a case that stricter privacy rules would increase costs and result in lost business, then the figures must be balanced against comparable evidence showing that the *lack* of privacy rules is also affecting business by dissuading customers from buying and by imposing costs on those who use the Internet for commerce. When both sides of the privacy equation are considered, the net effect will not be so clear as the one-sided studies suggest. Both privacy and its absence may affect business costs and consumer sales. Based on the current record, it is impossible to say which of the direct effects is greater or how to factor in the secondary consequences on Internet usage and values.

B. One Retailer's Loss Is Another Retailer's Opportunity

Some of the questions posed by industry-funded privacy studies have a distinctive old-fashioned quality. They rely for the most part on traditional models of marketing, using ever-increasing amounts of personal information obtained from every possible source available. Even within the marketing community, some recognize that old methods have significant problems and that new, less privacy-invasive, approaches can work. If those old methods are undermined by privacy rules, new methods may replace them with no systemic losses. One company's lost sale becomes another company's new sale. The net effect on the economy at large may be zero.

---

[13] A.T. Kearney, *Satisfying the Experienced On-Line Shopper* at 8 (2000) <http://www.atkearney.com/main.taf?site=1&a=5&b=4&c=1&d=14>.

[14] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* 2 (2000) <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.

One of the justifications for the collection and maintenance of personal information is so-called *relationship marketing*, which is supposed to be based on a better understanding of and response to the needs and preferences of customers. Personal information is primary fuel for relationship marketing. However, even within industry circles, recognition of the shortcomings of relationship marketing is growing. A recent article in the Harvard Business Review makes the point that consumers feel trapped and victimized by the manipulation:

> Unfortunately, a close look suggests that relationships between companies and consumers are troubled at best. When we talk to people about their lives as consumers, we do not hear praise for their so-called corporate partners. Instead, we hear about the confusing, stressful, insensitive, and manipulative marketplace in which they feel trapped and victimized. Companies may delight in learning more about their customers than ever before and in providing features and services to please every possible palate. But customers delight in neither.[15]

The Internet offers businesses and consumers a new forum and new capabilities to find each other. Businesses can find customers without collecting massive amounts of personal information and sending unwanted mail in an attempt to find a two- percent response rate. With search tools of the Internet, new ways of enticing customers to a shop are available using other types of targeted advertising aimed at groups rather than identifiable individuals.

Parts of the marketing industry are using new approaches effectively. Permission marketing has grown significantly in the last few years.[16] Many new marketing companies are exclusively devoted to opt-in approaches to consumers. A study of the permission marketing finds higher customer interest:

> Permission marketing offers the promise of improving targeting by helping consumers interface with marketers most likely to provide relevant promotional messages. Many permission-marketing firms (e.g. yesmail.com - now part of the business incubator, CMGI) claim customer response rates in the region of 5-20% and since most use e-mail, they are not affected by the measurement problems of banner advertising. Since the ads arrive in the mailbox of the individual, it is likely that more attention would be paid to them in comparison to banners.[17]

It is not the purpose of this report to suggest how to restructure the marketing industry. However, there are alternatives to old-fashioned, privacy-invasive, marketing methods. Even if privacy rules would undermine an existing methodology to some extent, it does not mean that sales will be lost. The notion that less consumer information means less sales and profits has not been proven. It may just mean that privacy-invasive dinosaurs have lost business to more nimble and perceptive competitors. Studies sponsored by those dinosaurs lack credibility.

---

[15] Susan Fournier, Susan Dobscha, and David Glen Mick, *Preventing the Premature Death of Relationship Marketing*, Harvard Business Review (Jan.-Feb. 1998).

[16] See, e.g., *Opt-in News, A Newsletter For Permission-Based Email* <http://www.optinnews.com/about.asp>.

[17] Sandeep Krishnamurthy, *A Comprehensive Analysis of Permission Marketing*, Journal of Computer Mediated Communication 6 (2) (Jan. 2001) <http://www.ascusc.org/jcmc/vol6/issue2/krishnamurthy.html>.

The importance of new approaches will be crucial as new technology becomes more commonplace and as older opt-in/opt-out thinking becomes increasingly obsolete. Facial recognition technology that may be installed in stores, on streets, and in other public places provides a good example. Government officials and private companies with the ability to link faces with names may be able to monitor activities of identifiable individuals in ways that were never possible before. The technology may support tracking of individuals in any public place without any notice to them or any opportunity to express a preference about the use of personal information.

Consider an individual who enters a bookstore. Under the marketer's traditional view of the world, the store can record a purchase by that person and can use or sell the information to others. At best, the consumer might be given a chance to opt-out of these other uses of information, although many companies that accumulate transactional information do not offer that opportunity. What happens to information about that same individual who is identified using facial recognition technology while examining a book that is not purchased? Can that information also be captured, used, and sold? How will people even know what information is being collected? With a transaction, a person who leaves a trail by paying with a check or credit card knows that he or she can be identified. With this facial recognition surveillance, individuals captured by the camera will not receive effective notice and will not be able to exercise meaningful choice or give permission.

Old models of opt-out or even opt-in no longer have meaning when surveillance can be conducted in secret. The practices of the past grew up incrementally in an environment where slow increases in technological capabilities combined with hidden information practices resulted in ever-increasing trafficking in personal data. The precedents of the past, if expanded to the new world of wireless and other hidden surveillance techniques, suggest a future that many American would not welcome. Some narrow-minded economists focus only on the goal of lowering business costs of customer surveillance. These economists pay no regard to the social consequences. The expansion of personal information trafficking possible with new technology could lead to a future that will make George Orwell seem like an optimist.

C. Lost International Opportunities

Many other countries around the world have comprehensive privacy laws. In some of these countries, including Member States of the European Union, the law restricts the export of personal data to other countries that have insufficient privacy protections for that data. Most United States privacy laws do not meet international standards. As a result, U.S. companies that want to import personal data from Europe face the prospect of either lost business or increased costs to meet international requirements. It is difficult to put a price tag on the potential losses, but the strong objections to international privacy standards from parts of the business community suggest that the costs are large.

The Department of Commerce negotiated with the European Union to establish a so-called Safe Harbor framework[18] that allows U.S. companies to avoid interruptions in business dealings with the EU. A company that meets the conditions set out in the Safe Harbor documents will be

[18] <http://www.export.gov/safeharbor/>.

deemed to meet the adequacy requirements in EU law. The requirements include complying with fair information practices. Companies that have certified to the Safe Harbor requirements or have announced an intention to do so include Dun & Bradstreet, Hewlett-Packard, and Microsoft.

The costs incurred by Safe Harbor participants would have been avoided had the U.S. enacted laws that meet international privacy standards. In addition, Safe Harbor companies would not face the possibility of maintaining different privacy regimes for different customers as well as the unattractive possibility of having lower privacy standards for American customers. In other words, U.S. privacy laws could have avoided some costs for American multinational companies while providing improved privacy protections for Americans.

D. Increased Legal Costs

Personal information has uses for communicating with customers. Accumulations of personal information are also attractive to others. Law enforcement agencies are increasingly interested in obtaining records about individuals maintained by businesses, especially online businesses. A story in USA Today in 2000 found that the number of search warrants aimed at America Online has increased substantially, more than 800% since 1997.[19] AOL is not the only Internet provider that receives search warrants, but statistics for other providers are not readily available.

Internet providers and others with personal data are also at the receiving end of subpoenas from private litigation. AOL reported that in 2000, it received about 475 civil subpoenas.[20] Each subpoena brings with it a cost. While there may be nothing unusual when a business has to comply with legal process, the accumulation of new and detailed information about individuals may become more attractive to more potential users. Data accumulations may eventually be used routinely in litigation to cross-examine witnesses, in divorce or child custody cases, or even to evaluate jurors.

Privacy laws are not likely to exempt these data collections from all legal process, but higher and clearer standards might help. Further, if individuals have a greater ability to control the collection of their personal information, the value of the data to third parties may be reduced. In addition, privacy laws could require individuals to take more responsibility when a third party is served with legal process for their records.

Another type of legal cost results from private and governmental litigation over privacy policies and practices. Many leading Internet companies have been the target of class action lawsuits, and federal and state agencies have opened numerous investigations. Litigation can be both expensive and embarrassing for companies. Clearer rules can make it easier for companies to comply with privacy standards and may reduce the amount and cost of litigation. For example,

---

[19] Will Rodger, *Search Warrants for Online Data Soar*, USA TODAY (7/28/00) <http://www.usatoday.com/life/cyber/tech/cti289.htm>.

[20] Brief Amicus Curiae of America Online, Inc., *Melvin v. Doe* (Pa. Superior Court, Pittsburgh District) (Nos. 2115 WDA 2000 & 2116 WDA 2000). Many of the subpoenas sought identity information about an AOL subscriber with a particular screen name.

the Video Privacy Protection Act enacted in 1988 defined the obligations of video storeowners clearly, and little if any litigation has resulted.

E. Investor Losses

It is probably somewhat unfair to include within this review the huge losses incurred by investors in Internet companies whose business models were based on exploiting personal information obtained from Internet users. However, it is interesting to note that many of these businesses have failed or are failing. The direct losses to investors are one result. Wisely or not, the investors made decisions on their own, with eyes wide open. The consumers, whose data was at the heart of many of the failed companies, were rarely aware of what was being done with their data or asked for their consent.

In May 2000 – well before the crash of the dotcoms – an article in the *New York Times* suggested that business models based on personal data were not likely to succeed:

> For all the discussion about how the Internet is stripping consumers of whatever thin veil of privacy they have left in this world of credit bureaus and supermarket scanners, analysts have failed to recognize just how ineffective most of these data-gathering systems have been. Sure, many companies are trying to peer back through the glowing screens at Internet users, but so far no one has been able to make a big business out of being Big Brother.[21]

That investors lost money pursuing the wrong business model is not of immediate consequence to the privacy debate. What is notable is that the lack of privacy protections contributed to the illusion that fortunes could be made by exploiting consumer data. Not only was that illusion costly to investors, but the massive increase in concern over privacy that resulted from attempted exploitation of Internet users also damaged the Internet as a platform for economic commerce by scaring individuals away.

It is impossible to say how the Internet might have developed if it were imbued with strong privacy protections from the start. However, it is fair to suggest that the lack of privacy was a contributing factor to investor losses incurred to date. Stronger privacy protections for individuals may well have resulted in more efficient and effective business markets.

[21] Saul Hansell, *So Far, Big Brother Isn´t Big Business*, New York Times Magazine (May 7, 2000).

III. The Costs Consumers Incur When Privacy is NOT Protected

Although privacy restrictions may impose costs on record keepers, the lack of privacy protections constitute a *privacy toll* paid by consumers in hours and dollars spent. The privacy toll is paid to grocers and telephone companies and includes efforts to stop junk mail and avoid identity theft.

A. Higher Prices

Merchants increasingly offer frequent shopper programs that offer lower prices to consumers who register, provide personal information, and allow their purchases to be tracked. One opponent of the cards calls them *registration and monitoring programs*.[22] Perhaps the most common examples are supermarket frequent shopper cards. Before the cards were in common use, supermarkets and other merchants usually offered sales and discounts to all customers. The ability of merchants to set prices and limit discounts to registrants places tremendous pressure on consumers to agree. Any customer who refuses to use a frequent shopper card – or is unaware of the requirement – is likely to pay more for groceries, books, or other products.

Individuals may object to these programs for many different reasons, including inadequate privacy policies from the merchants and the lack of statutory privacy protections. Some merchants address these concerns, at least in part, by allowing anonymous registration. Some individuals evade the programs by acquiring cards using pseudonyms or through other tactics. However, some stores require identification.

The number of people who refuse to have or use frequent shopper cards is impossible to estimate. The higher prices paid by those who reject frequent shopper cards represent a direct financial sacrifice for privacy.

B. Junk Mail

Traditional junk mail is distinguishable in one important respect from unsolicited commercial email or spam. The sender of snail mail pays a significant cost in printing, postage, and handling for each item placed in the mail stream. The marginal cost of spam is often close to zero, and that is not true for snail mail.

Recipients of junk mail can discard it, but junk mail still imposes costs. Recipients spend time sorting and discarding unwanted mail. They pay to have the trash removed, not a trivial expense on a nationwide scale. The basic numbers of junk mail make this point:

- The average person receives 10.8 pieces of junk mail each week or nearly 560 pieces per year. For a household, the amount of junk mail received annually can easily exceed 1000 pieces a year.

[22] Consumers Against Supermarket Privacy Invasion and Numbering <http://www.nocards.org/faq/index.shtml>.

- The total volume of junk mail produced each year in the United States is approximately 4.5 million tons.

- Each year, 100 million trees are used to produce junk mail.

- Estimates are that 44% of junk mail is discarded unopened and unread.[23]

- A 1995 survey by the U.S. Postal Service found that 50% of households wished that they received less "advertising" mail, up from 30% in 1987.[24]

Some companies allow data subjects to opt-out of the sharing of their personal information for marketing purposes. Those who do opt-out may receive less unwanted mail. However, the burden on consumers of opting-out is significant. Most companies require those seeking to opt-out to write letters.[25] Writing a letter is a significant burden on most individuals, and the cost for paper, postage, and time is not trivial. If the cost to a consumer of sending an opt-out letter were 50 cents, the consumer who opted out of one type of junk mail each week would spend $26.00 in the course of a year. For an average household, the annual cost could easily exceed one hundred dollars per year.

Some broader opt-outs are available, but not all are free. Individuals who want to use the Mail Preference Service run by the Direct Marketing Association to opt-out of junk mail must pay a five dollar "processing fee" and pay by credit card if they want to register for the service online.[26] The reticence of privacy-sensitive consumers to disclose their credit card numbers online is well known so the demand for a credit card places a real barrier on the use of this DMA service. The fee seems designed to discourage easy online opt-outs. The DMA's email opt-out service has no processing fee. However, it is only effective for one year and must be affirmatively renewed annually. Exercising these opt-outs imposes a cost on consumers that must also be attributed to the lack of adequate privacy protections.

C. Telemarketing

Telemarketing is not popular among consumers. Indeed, of all the invasions of privacy that people encounter in their day-to-day activities, receiving unwanted telephone calls tends to be at the top of most lists. Polls confirm that people find telemarketing calls annoying, unacceptable, invasive, and offensive.[27] The Privacy Rights Clearinghouse makes the point with the subtitle of its fact sheet on telemarketing calls: *Whatever Happened to a Quiet Evening At Home?*[28]

---

[23] <http://www.nativeforest.org/campaigns/recode/junkmail.html>.
[24] Direct Marketing Association, Statistical Fact Book 1998 at 37.
[25] In regulations issued under Gramm-Leach-Bliley governing opt-outs offered by financial institutions, the Federal Trade Commission distinguished between reasonable and unreasonable opt-out methods. The Commission said expressly that it is an unreasonable method if the only way for a consumer to opt-out is to write a letter. The Commission favored check-off boxes, reply forms, and electronic means to opt-out. 16 C.F.R. §313.7(a)(2).
[26] <http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#risk>.
[27] For a collection of polls on the subject, see <http://telejunk.norman.ok.us/surveys.html>.
[28] <http://www.privacyrights.org/fs/fs5-tmkt.htm>.

Connecticut is one of many states that operates a state do-not-call list. Recent statistics show that nearly half of Connecticut households have placed their telephone number on the list.[29]

Some consumers take action to stop unwanted calls. Several websites are devoted to helping people stop telemarketing calls, and one reports that its members have recovered more than $800,000 in damages over the calls.[30] When AOL announced in 1997 that it would begin to sell the telephone numbers of its members, the move "unleashed a storm of criticism."[31] It took only one day for AOL to hear the complaints and reverse its decision.

The Telephone Consumer Protection Act[32] gives recipients of unwanted calls a limited legal remedy. However, the courts are beyond the reach of most, and consumers use other techniques and technologies to avoid, evade, and stop telemarketing calls. Consumers spend time, effort, and money in their efforts, and these are costs that result from the lack of adequate protections for the privacy of personal information. Many consumers simply suffer the aggravation and disruption of unwanted telemarketing calls.

Telephone companies and device manufacturers rely on consumer objections to telemarketing as a selling point for enhanced telephone services. Here are some examples:

- Caller ID is often promoted as a privacy protection and a way to avoid unwanted calls. Qwest's version is called *Caller ID with Privacy+*.[33] Verizon offers a service under the name *Call Intercept*. The pitch to customers is:

> Caller ID with Call Intercept screens unidentified calls and lets you handle them the way you want. Fewer unwanted calls mean more peace and quiet for you at home.[34]

The price for Verizon Call Intercept service as described on its website is $5 per month. Caller ID with Name costs an additional $7.50 per month.

- Answering machines and voice mail have long been used to screen calls. A 1997 survey found that about 3 in 4 households had answering machines. The firm that conducted the survey took special note of the role of answering machines in avoiding telemarketing calls:

---

[29] DM News, *Connecticut DNC List Doubles in Size* at 6 (June 11, 2001). The degree of public antipathy toward telemarketing is also illustrated by the comments of a representative from the Kentucky Attorney General's office about the response to the state's do-not-call list. "There has been nothing in the 200 years-plus of Kentucky's history that the Attorney General's Office has ever seen that equaled the public response to the no-call list . . . It literally – and I mean literally – fried our telephone systems. It knocked our telephone line out . . . [Tennessee's] telephone lines have been broken down because of the overwhelming response, and their list is not even ready . . . to be implemented . . .[Georgia] had exactly the same response, that there was truly a tidal wave of people who were seeking to be on the list." Quoted in Federal Trade Commission, Telemarketing Sales Rule, Notice of Proposed Rulemaking at note 242 <http://www.ftc.gov/bcp/conline/edcams/donotcall/pubs/NDNCR_therule.pdf>.

[30] See Private Citizen, < http://www.private-citizen.com/>. See also <http://www.stopjunkcalls.com/links.htm>.

[31] Associated Press, *AOL Backs Off Plan to Give Out Phone Numbers* (July 25, 1997).

[32] 47 U.S.C. §227.

[33] <http://www.qwest.com/pcat/for_home/product/1,1354,431_1_8,00.html>.

[34] <http://www.bellatlantic.com/foryourhome/MD/Products/CIX-01/>.

> The answering machine is no longer a luxury. It has become a household utility, a necessity. It is perceived as valuable in screening out those annoying telemarketing calls that we all like to avoid, as well as capturing those calls and messages that we don't want to miss.[35]

Answering machines can also serve another purpose in protecting consumers. State securities regulators consider answering machines to be the consumers' best weapon in the fight against telemarketers selling fraudulent investment schemes.[36] The advice is a reminder that not all telemarketers offer legal products and services. The same lack of consumer control over the use of personal information, including telephone numbers, fuels telemarketing of all stripes.

- A promotion for call waiting uses avoiding telemarketing calls as a major selling point:

> Mike is in the middle of an important phone call when he hears his Call Waiting beep. But there is no number displayed on his Caller ID Box. Mike assumes correctly that the call is from a telemarketer so he continues his important conversation.[37]

- A service from Bell South – *Privacy Director* – is pitched at protecting customers from unwanted telemarketing calls:

> If you are receiving silent or hang up calls between 8:00 a.m. and 9:00 p.m., it is possible these calls are from telemarketers. Many of these calls will display on Caller ID as UNKNOWN or OUT OF AREA. * * * It is possible for you to receive numerous calls from many different telemarketing sources. For the calls that display on Caller ID as UNKNOWN or OUT OF AREA BellSouth now offers Privacy Director which will assist you with these calls.[38]

- Another product expressly and exclusively aimed at telemarketers is *EZ Hangup* by Zenith. This telephone accessory allows a the user to hang up on an unwanted sales call and press a button to play a recording rejecting the call and asking to be removed from a calling list. The product lists for around $25.00.[39]

- Verizon, like other telephone companies, offers its customers several ways to keep their telephone numbers private. These services are not free. Customers can pay for non-listed numbers (not in the telephone directory but listed for directory assistance) or non-published numbers (not in the directory or directory assistance). Each service has a monthly charge.[40]

---

[35] Decision Analyst, Inc., *More Households Using Answering Machines* (Press Release, October 15, 1997) <http://www.decisionanalyst.com/publ_data/1997/ansmachi.htm>.
[36] ABP News, *Regulators: Answering Machines Can Foil Telemarketing Fraud*, (Oct. 17, 1999) <http://www.apbnews.com/safetycenter/business/1999/10/17/securitiesfraud1017_01.html>.
[37] CC Communications, *Caller I.D. w/Call Waiting* <http://www.cccomm.net/AtHome/Calling_Features/calleridwait.htm>.
[38] BELLSouth, *Annoyance Call Center* <http://contact.bellsouth.com/acc/AnnoyanceTelemarketing.asp>.
[39] Full Life Products, *EZ Hangup* <http://www.superproducts.com/anti-telemarketing/ez/index.htm>.
[40] <http://www.bellatlantic.com/foryourhome/DC/Products/NPT-01/index.html>.

A 1995 study found that 31.5% of households had unlisted or unpublished numbers. In some communities, the percentage exceeds 60%.[41] Another estimate is that a quarter of households pay an average of $1.50 a month to be unlisted. The total cost to telephone subscribers for these privacy-protecting services is more than $400 million a year.[42]

Techniques to avoid telemarketing are not practices only for those who are especially privacy sensitive. The widespread use of answering machines and unlisted numbers shows the breadth of public concern. Anti-telemarketing techniques are a recognized activity recommended by governments and other mainstream organizations as a way of protecting privacy and avoiding unwanted calls. Evidence for this also comes from a consumer guide published by the Commonwealth of Massachusetts. Consumers are advised to put their names on company and national do-not-call lists, to consider having an unlisted number, to avoid disclosures through contests, surveys, and sweepstakes, to use blocking technology to avoid disclosing a telephone number when making a call, and to screen calls with an answering machine.[43]

Consumers who want to avoid telemarketing calls can spend their own time and money to avoid them. Even an individual with a casual objection to telemarketing could spend a considerable sum on equipment or monthly charges. These represent costs that consumers pay because they are unable to control how their personal information is used and disclosed. Obviously, some telephone capabilities, such as answering machines, voice mail, and unlisted numbers serve other goals beyond the protection of privacy and avoidance of telemarketing. A fair cost accounting would allocate only some of the expense to privacy protection and some to other objectives. Nevertheless, the telephone costs consumers incur for privacy reasons are significant.

Society faces other consequences when consumers are forced to act in their personal interest to keep their telephone numbers secret. Telephone directories help to make the telephone network inclusive, efficient, and useful. Because most households have telephones, a complete telephone directory would enhance the ability of individuals and businesses to find and contact other people. When large percentages of the population pay to have their numbers unlisted because of concern about misuse, every telephone directory user suffers from the lack of an effective, interconnected universal telephone system.

D. Identity Theft

Identity theft occurs when an individual appropriates another's name, address, Social Security number, or other identifying information to commit fraud. Identity thieves may use consumers' identifying information to open new credit card accounts, take out loans, or steal funds from existing checking, savings, or investment accounts.[44]

---

[41] Brad Edmonson, *Unlisted America*, American Demographics (June 1995) <http://www.demographics.com/publications/ad/95_ad/9506_ad/AD767.htm>.
[42] Jay Chris Robbins, *Phone Book "Non-Service" Dials up Huge Profit* (Jan. 14, 2000) <http://tampabay.bcentral.com/tampabay/stories/2000/01/17/editorial3.html>.
[43] *A Massachusetts Consumer Guide: Stopping Junk Mail, Phone Calls, And Email* <http://www.state.ma.us/consumer/pubs/stopjunk.htm>.
[44] Testimony of David Medine, Associate Director for Credit Practices, Bureau of Consumer Protection, Federal Trade Commission, before the Subcommittee on Technology, Terrorism and Government Information, Senate Committee On The Judiciary (May 20, 1998) <http://www.ftc.gov/os/1998/9805/identhef.htm>.

The harm to victims of identity theft is significant and long lasting,[45] both emotionally and financially. It can take years of hard work and hundreds or thousands of dollars in out-of-pocket expense before all vestiges of identify theft are removed from a victim's record.[46] In the interim, a victim of identity theft may be unable to obtain a job, purchase a car, or qualify for a mortgage.[47] Hundreds of thousands of individuals are victimized by identity theft each year.[48]

The costs to financial institutions are also significant. Definitional problems and lack of data make it difficult to estimate costs with precision, but the losses appear to be measured in the hundreds of millions of dollars.[49] Consumers ultimately pay for many of these losses through higher prices and higher interest rates. In addition to out of pocket losses, identity theft undermines consumer confidence in the credit system and especially the Internet, deterring the growth of electronic commerce.[50]

Identity theft mushroomed in the 1990s. It may not be a coincidence that the growth of identity theft roughly parallels the growth of the Internet. Personal information is available from multiple sources on the Internet both commercial and public. The widespread availability of the information makes it easier for criminals to engage in identity theft. Identity theft occurs for many reasons, and the routine trafficking in personal information is a significant contributing cause.

The relationship between personal information availability and identity theft is supported by several independent studies. In a 1998 report on identity theft, the General Accounting Office said that "[m]any of the officials we contacted said that Internet growth, which enhances the availability and accessibility of personal identifying information, obviously creates greater risks or opportunities for criminal activity, including identity fraud."[51]

The National Fraud Center, a private organization operated by a major information company, offered a similar opinion about how the availability of personal information from the Internet contributes to identity theft:

> The computer and, more recently, the Internet have brought identity theft to a much more insidious level. They have allowed the identity thief to obtain personal identifiers of multiple persons quicker; to access higher quality fake identification tools (drivers licenses, birth certificates, social security cards, etc.)

---

[45] Id.
[46] The Identity Theft Resource Center reports that, on average, victims spend 175 hours and $808 in out-of-pocket expenses to clear their names <http://www.idtheftcenter.org/html/facts_and_statistics.htm>.
[47] General Accounting Office, *Identity Fraud: Information on Prevalence, Cost, and Internet Impact Is Limited* at 4 (GAO-GGD-98-100BR) (1998) [hereinafter cited as *GAO Identity Fraud*].
[48] See id at 24-41 (discussing information sources and lack of comprehensive national statistics). The Identity Theft Resource Center estimates that there were 700,000 victims in 2000. <http://www.idtheftcenter.org/html/facts_and_statistics.htm>.
[49] *GAO Identity Fraud* at 4.
[50] See, e.g., National Fraud Center, *National Fraud Center White Paper Says Internet Driving Dramatic Increase in Identity Theft - Balanced Approach Required to Address Issue* (Press Release, March 16, 2000) <http://www.nationalfraud.com/pressrelease/IDTheft.htm>.
[51] *GAO Identity Fraud* at 4.

> and, through e-commerce, to render the credit transaction completely impersonal. Indeed, this "faceless" aspect of e-commerce renders the purpose of credit-cards, driver's licenses and other identification tools, meaningless.[52]

Industry argues that the availability of personal information helps to avoid identity theft by reducing fraud.[53] This is undoubtedly true to some extent. Yet the vast amount of consumer information available today to credit grantors has not stopped the enormous growth of identity theft in the last decade. The value of information as a protection against identity theft is limited. At the same time, it is also true that extensive and largely unregulated trafficking in personal information – typically without consumer knowledge or consent – makes it easier for identity thieves to operate.

Privacy laws that would give individuals more control over the use and disclosure of their personal information have potential to limit identity theft.[54] The lack of privacy protections thus contributes to the cost of identity theft. Further, activities that individuals take on their own initiative to protect against identity theft impose costs that can be attributed in significant part to the absence of privacy protections.

Some companies profit by selling personal information to detect or avoid fraud. At the same time, they also sell personal information that is used directly or indirectly, legally or illegally, to support identity theft. These companies profit from both sides. Now these same information companies seek to profit in a third way as well. The companies want consumers to pay for services to protect themselves against identity theft. An example comes from a recent Equifax press release about a Credit Watch service that costs $39.95 a year. The service promises:

> [T]o quickly detect possible identity theft and minimize its potentially devastating consequences. Providing consumers of notice about activity on their credit file with unmatched speed, the product also empowers consumers to manage their personal credit more effectively. A rash of recent identity theft cases point to the importance of consumer vigilance; Equifax Credit Watch makes it easier for consumers with a front line of defense.[55]

---

[52] National Fraud Center, Inc., *Identity Theft: Authentication As A Solution* (2000) <http://www.nationalfraud.com/identity%20theft%203.13.htm>.

[53] Ernst & Young, *Customer Benefits of Information Integration by Financial Services Companies* 5 (2000) <http://www.privacyalliance.org/resources/research.shtml>. This Ernst and Young survey of members of the Financial Services Roundtable found that 63% of respondents thought that restrictions on information sharing included in the Gramm-Leach-Bliley (GLB) law would restrict their ability to detect fraud. A second question found that 79% thought that potential new restrictions on information sharing would restrict their ability to detect fraud. The questions contained no details about the GLB restrictions, and it is unknown whether the respondents were familiar with the law. The second question left the nature of any information restrictions to the imagination of the respondent. Even so, 21% did not see a connection between information restrictions and ability to detect fraud. In a survey designed to elicit positive responses to these questions, the presence of a sizeable minority view may be more telling than the opinion of the majority. These questions show how surveys are manipulated to support impressive results that actually have no significance.

[54] The same point could be made that privacy laws would limit telemarketing fraud and other forms of consumer fraud that benefit from the ready availability of personal information.

[55] Equifax, Inc., *Equifax Credit Watch Provides Early Warning Of Identity Theft To Consumers* (Press Release 4/10/01) <http://www.equifax.com/press_room/press_releases2001/2001_04_10.html>.

These costs incurred by individuals who are afraid of being victims of identity theft represent costs that result from the lack of adequate privacy protections. A family concerned about identity theft might have to pay for two or more credit watch subscriptions annually.

These are not the only costs incurred by individuals who suffer from the lack of protection for their personal information. Consumers can find no shortage of advice about what to do to protect themselves against identity theft. The New York State Attorney General is one of many authorities suggesting that consumers buy a copy of their credit report each year.[56] For a family with two adults, the cost is $51 a year to buy reports from three credit bureaus. Better privacy protections for personal data would lessen the risks and the need for checking on credit reports annually.

The Federal Trade Commission suggests that consumers undertake other activities to protect themselves and their information.[57] These activities include opting out of having personal information held by third parties shared. An example would be opting out of pre-screening for credit offers. This strategy can only have limited benefits. Many companies that traffic in personal information do not notify data subjects that their records are being sold, do not allow consumers to opt-out, or allow limited opt-out choices. The number of telephone calls and letters required for a family that elects all available opt-outs is unknown, but it could easily be measured in the dozens. The time, trouble, and expense of opting out are other costs that consumers incur.

E. Internet Effects

The lack of privacy protections for personal information has taken its toll on the Internet in a variety of ways.

1. Financial Costs of Spam

Unsolicited commercial electronic mail, often called *spam*, imposes costs on Internet users. Spam is a privacy issue because it results, in significant part, from the inability of Internet users to control the way in which their email addresses are collected, used, disseminated, and sold. Uncontrolled trafficking in email addresses contributes directly to spam.

Spam imposes costs mostly on the recipient and on intermediaries. While the sender must compose the message and pay for an Internet connection, the cost of bulk Internet mail can be insignificant. One estimate is that bulk email may cost the sender only 1/100th of a cent per address.[58] The more mail sent, the lower the cost per message for the sender, and the more costs imposed on recipients and others.

---

[56] <http://www.oag.state.ny.us/consumer/tips/identity_theft.html>.
[57] <http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#risk>.
[58] S. Hambridge & A. Lunde, *Don't Spew: A Set of Guidelines for Mass Unsolicited Mailings and Postings* (1999) <http://www.imc.org/rfc2635>.

A recent study of unsolicited commercial email and privacy commissioned by the European Union provides some estimates of the costs to consumers. Based on the study's assumptions about the cost of Internet connections, it concluded that the cost of downloading 15 spam messages a day could be as high as 30 Euros (a Euro is worth approximately 90 cents) per user each year. The study was projected for 400 million worldwide online users so the total global costs *borne by consumers* were estimated conservatively at 10 billion Euros (or 8 to 10 billion US dollars) annually.[59] Varying the assumptions would produce a different cost estimate, but the costs to consumers will still be measured in the billions.[60]

Spam also imposes costs on Internet service providers, network administrators, employers, and others who use or support the Internet. By congesting the Internet, other types of indirect costs attributable to spam are imposed, even on users who do not receive the spam. For example, the Los Angeles Times reported that in 2000, 144,000 subscribers of Pacific Bell's Internet service repeatedly lost access to e-mail for hours because servers were clogged with spam.[61]

2. Other Effects of Spam

Some Internet users are so outraged by spam that they operate websites dedicated to stopping spam or advising users what to do. Dozens and perhaps hundreds of individuals, acting on their own or through nonprofit groups, dedicate significant time and effort to blocking spam using various Internet tools and techniques.[62]

The broader effects of spam are more troublesome because they affect the vitality of the Internet as a means of open communications. Nolan Bowie, Senior Fellow at Harvard University, described the social and economic consequences of the lack of Internet privacy in these words:

> This discourages citizens and consumers from using [the Internet] because they fear, justifiably, that their personal information may be monitored, captured, processed, manipulated, and sold as commodities to vendors or used by government agencies to spy on their buying habits, viewing habits, e-mail messages, online chats, or political interests.[63]

Many users have learned that posting on mailing lists or Usenet groups will place their email addresses in public sight where email list compilers can easily collect them. The fear of spam is

---

[59] Commission of the European Communities, *Unsolicited Commercial Communications and Data Protection* at 66-67 (2001) <http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/spam.htm>.

[60] Cost estimates for Internet usage can be complex, especially in the US environment where users often pay a flat fee for unlimited Internet service and for telephone service. Not all Internet is flat rate, and telephone service – especially wireless – is increasingly based on usage. Regardless of the immediate relationship between fees and usage, spam raises system costs for every institution that provides facilities that support the Internet. All Internet users will ultimately pay more for Internet service because of the receipt of increased and unwanted commercial solicitations. Internet users also spend time reading and deleting messages. The EU study quotes one estimate that a user who receives six spam messages a day will waste two hours each year just deleting spam.

[61] Michael Hiltzik, *Lone Guns Set Sites on Spam*, Los Angeles Times <http://www.latimes.com/business/cutting/lat_spam010416.htm>.

[62] Id.

[63] Nolan A. Bowie, *An E-Public Sphere for the Digital Age: What Needs to be Done to Enhance Democratic Values and Engage Greater Civic Participation in the United States* at 3 (2000).

so great for some that they deliberately avoid using open methods of communications.[64] Others post messages using a deliberately false or changed address, and this too undermines the openness and utility of the Internet.

Some users maintain multiple mailboxes as a way to avoid spam.[65] Some use filters, even though the filters do not work perfectly. Others may not use email at all or to its full potential because of unhappiness over spam.

Vint Cerf, Senior Vice President of MCI and one of the principal designers of the Internet, summarized the broad and deleterious effects of spam on the resources of Internet users in these words:

> Spamming is the scourge of electronic-mail and newsgroups on the Internet. It can seriously interfere with the operation of public services, to say nothing of the effect it may have on any individual's e-mail mail system. * * * Spammers are, in effect, taking resources away from users and service suppliers without compensation and without authorization.[66]

3. Anonymity

Internet users have many reasons for wanting to be able to surf without leaving an identifiable trail. Dislike of spam is just one reason. Other reasons include the avoidance of surveillance and the ability to speak freely. Not all of the reasons for anonymity relate to privacy, but it is a significant factor for many individuals.

The demand for privacy and anonymity is being met with Internet software products and services like the Anonymizer,[67] which prevents anyone "from marketers to ID thieves to your coworkers" from seeing where an Internet user surfs. It costs $49.96 annually. Other types of privacy protection software, including programs to give users control over cookies and Internet advertising, are available from many other sources. Consumers who purchase these products and services are buying privacy protections that they cannot obtain otherwise. In these and other instances, the privacy protections that can be acquired individually by consumers are not as good as those that might be provided in other, more systemic ways.

Other software and surfing tools designed to protect user privacy include WebWasher, which offers services that stop Web bugs and cookies from tracking users. WebWasher also has other functions that filter content and provide security. The software costs $29.00.[68] According to a Reuters news story, WebWasher claims four million users, including 1000 corporate users.[69]

---

[64] Paul Hoffman, *Unsolicited Bulk Email: Definitions and Problems* (1997) (Internet Mail Consortium Report UBE-DEV IMCR-004) <http://www.imc.org/ube-def.html>.
[65] The Pew Internet & American Life Project, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules* at 10 (2000) <http://www.pewinternet.org/>.
[66] Quoted at <http://www.cauce.org/about/problem.shtml>.
[67] <www.anonymizer.com>.
[68] <www.webwasher.com>.
[69] Andy Sullivan, *Plugged In: Ad-Blocking Software Gains Traction* (May 1, 2001) (Reuters) <http://www.quote.com/quotecom/news/print_story.asp?story=21776768>.

Many other privacy protection programs and services can be found on the Internet and elsewhere.

The use of privacy software by corporations as well as individuals is a reminder that protections from Internet surveillance benefit businesses. The protection of trade secrets and other confidential corporate information is another benefit realized by protective software and practices.

Another response by those who do not want to be identified is lying. Polls show that 20 to 30 percent of web users provide false information online.[70] Most do it because they care concerned about how a website will use the information, to avoid junk email, or to be anonymous.[71] One consequence of lying and other "guerilla tactics"[72] is that information collected and relied upon by websites is wrong, and this increases the cost and decreases the value of the data.

F. The Dossier Society

Arguments that focus solely on monetary costs and benefits miss a major part of the privacy debate. The lack of privacy is changing American society in non-monetary ways that many find undesirable.

The extensive literature on privacy often addresses the importance of privacy for self-development, the need for privacy in the establishment of human relationships, or as a collective value for society as much as for the individual.[73] The lack of clear agreement among lawyers, philosophers, sociologists, political scientists, and others about the meaning and purpose of privacy should not mask the fact that the debates are rarely conducted based on economic costs and benefits. We value privacy in ways that are not measurable by dollars and cents.

Do we want a society where every scrap of personal information about each individual can be collected, sorted, and compiled for unrestricted use by business and government without consent or knowledge of the data subjects? We know the answer when it comes to government. The Bill of Rights created a series of limitations on the ability of government to collect and use information about individuals and to enter private homes. Legislation also limits the ability of government to collect personal information.

Other approaches might produce more effective or less expensive law enforcement or public safety operations. However, Americans have always rejected strict economy or efficiency arguments in favor of the protection of fundamental rights. We proceed with rules and

---

[70] See Forrester Research, *The Privacy Best Practice* at 5 (32% of online consumers have misrepresented themselves online); The Pew Internet & American Life Project, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules* at 10 (2000) (24% of Internet users have provided a fake name or personal information in order to avoid giving a Web site real information.) <http://www.pewinternet.org/>.

[71] Forrester Research, *The Privacy Best Practice* at 5 (figure 2-2) (1999).

[72] The Pew Internet & American Life Project, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules* at 10 (2000) <http://www.pewinternet.org/>.

[73] For a useful summary of privacy as a philosophical and legal concept, see Priscilla M. Regan, Legislating Privacy: Technology, Social Values, and Public Policy (1995).

procedures that strike a fair, reasonable, and appropriate balance between the rights of individuals and the needs of government.

The same balance is appropriate when it comes to commercial uses of information. Americans will not tolerate every possible data collection, use, or disclosure just because some economist can argue that it has a potential to support better-targeted marketing or might encourage the sale of a product or service. Several observations make this point more clearly.

1. Economic Effects

Both business and consumers incur costs from *not* having adequate privacy protections. People will not purchase items on the Internet and otherwise when they fear that their personal information will be misused. Individuals spend time and money solely to evade the consequences of too much data sharing.[74] Privacy has its costs. Not having privacy has its costs too.

2. Private Ownership and Government Intrusion

In the US, we have traditionally applied different rules to the public and private sectors. Constitutional protections only limit government activities, not private ones. However, as the line between the public and private sectors regarding personal data grows ever less clear, the protections against government weaken. A recent Wall Street Journal article on this subject emphasizes the increasing flow of consumer data from private sector databanks to law enforcement agencies:

> Big Brother isn't gone. He's just been outsourced. After surveillance scandals in the 1960s and 1970s, the Federal Bureau of Investigation and other federal law-enforcement authorities curbed their file-keeping on U.S. citizens. But in the past several years, the FBI, the Internal Revenue Service and other agencies have started buying troves of personal data from the private sector.[75]

The article describes how private sector companies specialize in collecting and compiling on individuals from multiple scores, including credit bureaus, marketers, and public records. The records are sold to dozens of government agencies. Do Americans want the records of their purchases, activities, and interests available online for casual use by the FBI and other law enforcement agencies without any requirement for a court order or search warrant?

---

[74] A 2001 poll by the American Society of Newspaper Editors and the First Amendment Center found that 70% of the public have refused to give information to companies because they thought it was too personal; 62% asked for their name to be removed from a marketing list; and 23% avoided using a grocery store frequent shopper card. *Freedom of Information in the Digital Age* at 19 <http://www.freedomforum.org/publications/first/foi/foiinthedigitalage.pdf>.

[75] Glenn R. Simpson, *FBI's Reliance on the Private Sector Has Raised Some Privacy Concern*s, Wall Street Journal (April 13, 2001).

3. Informed Consumer Choice

Economic arguments mask the fundamental unfairness of many current business practices for personal information. Much current personal information collection and dissemination for marketing uses goes on today in a manner hidden from the average person. The arguments about consumer benefits conceal the reality that many people would object if given a fair choice. If there are consumer benefits from information sharing, then consumers should have the chance to agree to receive the benefits. Consumers routinely engage in behavior that economists would find to be economically irrational. This does not mean that consumers are wrong but that they are acting out of non-economic motives. The arguments that business makes to policy makers in support of unrestricted markets in consumer information should be made directly to consumers. Consumers who believe that they benefit from increased marketing and information sharing will agree to receive solicitations.

Arguments in favor of greater use of personal information for the enhancement of private sector marketing activities have a significant slippery slope problem. Where do we draw the line? Targeted marketing might be greatly enhanced if personal income tax records or medical records were available freely to marketers. Yet it is clear that most Americans would not tolerate this type of activity. Proposals for expanded access to these records would be rejected universally.

Existing data collection practices may also be objectionable to many consumers, but few have any idea of the extent of the collection. Companies that share or compile data rarely offer complete descriptions of their data practices to data subjects. A description about the activities of data aggregators from a recent Federal Trade Commission workshop illustrates the scope of personal data activities:

> Aggregators have data on a broader population. Some aggregators have most of the U.S. population. The data comes from many, many sources. As we discussed, some of them are public record sources. Some of them are surveys. Some of them are purchase data, but the data comes from many sources, not a single source. Typically the data that is held by an aggregator is not experiential data. It tends to be demographic or psychographic data, and, last, typically the aggregator does not have regular contact with the customer, the consumer, but rather relies on the party that collected the data to have had that contact with the consumer, and most aggregators build systems to make sure they only get data from reliable sources.[76]

4. Weakening Public Policy Objectives

The unrestricted use of personal information for private purposes can weaken well-established public policy objectives. A good example involves criminal history records. Records about criminal convictions can be expunged under carefully defined circumstances. The policy is that an individual who made a mistake should not be saddled forever with a criminal record.

---

[76] Martin Abrams, Executive Director of the Center for Information Policy and Leadership, Hunton & Williams, Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data* (March 13, 2001) <http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm>.

However, the maintenance of private databases may make it impossible for a conviction to be fully erased. A vast array of private information databases and computer networks collect and disseminate criminal history information. It can be impossible for an individual to find the multiple record keepers and to erase the records. The objectives of expungement have been undermined by databases that operate without any privacy rules.[77]

5. Non-Economic Privacy Interests

Finally, privacy serves objectives that go beyond the narrow economic interests of data subjects or of data users. The Fair Credit Reporting Act is a privacy law with a strong economic flavor because it protects against unfair financial discrimination based on outdated or incorrect information. Other privacy legislation protects non-economic interests along with privacy interests. The Telephone Consumer Protection Act allows individuals to avoid annoying and disruptive telephone solicitations. The increasing number of State mandated do-not-call lists accomplish the same purpose. Both the Video Privacy Protection Act and the Cable Communications Policy Act protect the First Amendment interests of those who rent movies and watch television. State library laws offer similar First Amendment protections to book readers. The Children's Online Privacy Protection Act prevents the collection of data from children without parental involvement. These privacy laws demonstrate the breadth of interests covered by privacy.

[77] See, e.g., Dan Horn, *Offenders Find Records Hard to Erase*, Cincinnati Enquirer (Dec. 18, 2000) <http://enquirer.com/editions/2000/12/18/loc_offenders_find.html>; *Smith v. Daily Mail Publishing Co*, 443 US 97 (1979) (Rehnquist, J. dissenting) ("Such publicity also renders nugatory States' expungement laws, for a potential employer or any other person can retrieve the information the States seek to "bury" simply by visiting the morgue of the local newspaper."). Newspaper morgues may have been the only independent source of criminal history information when the decision was written in 1979, but there are many more sources today. See, e.g., *United Reporting Publishing Corp. v. California Highway Patrol*, 146 F. 3d 1133 (CA9 1998), reversed on other grounds, 528 U. S. 32 (1999).

Sidebar: The Annual Privacy Toll for a Privacy Sensitive Family

Elements of the Privacy Toll

Identity Theft

Credit Watch	$39.95 a year for two adults	$79.90
Credit Reports	$8.50 a year for two adults at two credit bureaus	$34.00

(There are three major credit bureaus. These services will cover all three.)

Telemarketing Avoidance

Caller ID with Name	$7.50 per month	$90.00
Unlisted Number	$1.50 per month	$18.00

Internet Privacy

Anonymization Service	$50 per year	$50.00

Junk Mail

Opting out	12/year @ .50 per opt-out	$6.00
Total Annual Costs		**$277.90**

Time Losses

· Spam download time 5 hours/year
· Spam deletion time 2 hours/year

Intangible and Unmeasured Costs

· Higher credit costs due to ID theft
· Costs incurred directly by ID theft victims (hundreds or thousands of dollars per victim)
· Disruptions and aggravation from unwanted telemarketing calls
· Consumer losses due to telemarketing fraud that rely on targeted marketing data
· Internet service outages and delays due to spam (losses to consumers and to businesses)
· Internet costs due to capacity necessary to support spam (costs to ISPs, users, and others)

Note: Some products and services may have other purposes in addition to protecting privacy interests. A fair accounting may attribute some costs to these other interests.

IV. Conclusion

The protection of privacy, like other good things in life, has benefits, costs, and consequences. The public is clearly concerned about the loss of privacy is demanding better privacy protections.

In responding to the demand for privacy, the costs for businesses and other record keepers are relevant. However, the costs of privacy must be fairly assessed. Studies based on one-sided, biased, and unrealistic estimates have little value. Studies funded by industry with questionable methodologies or conducted by partisan researchers have little value. Studies conducted without any participation from consumer or privacy organizations or without an objective methodology have little value. Studies that ignore the real costs incurred by real businesses that have implemented privacy policies have little value.

The benefits of privacy must also be fairly assessed. Privacy saves money. If privacy rules force record keepers to keep fewer records or to maintain records for a shorter period, the costs of record maintenance will be reduced. If accurate records result in fairer decision making about individuals, savings and benefits will result. If privacy protections encourage more individuals to use the Internet to make purchases and to engage in other activities, the cost of doing business will drop, and many will benefit.

The consequences of not having privacy protections must also be assessed. If we have few systemic protections and leave individuals to protect their own privacy, we must consider the costs that individuals incur as part of the costs of not having privacy. If someone will pay for privacy, then the right question may be: Is there someone else who can bear the costs more efficiently and more fairly?

Policymakers also have to remember that privacy is not measured solely with a financial yardstick. Privacy is relevant to many aspects of our daily lives. If a lack of privacy saps the vitality of the Internet, we pay a price that cannot be measured entirely in dollars. If a lack of privacy discourages telephone subscribers to include their names in telephone directories, we pay a price that cannot be measured in dollars. If a lack of privacy fills our landfills with junk mail, we pay a price for that, too. If a dossier society makes an individual think twice before using a frequent shopper card to buy a tube of Preparation H in a supermarket, we pay a price.

We are on the verge of widely implementing new technologies that can increase the surveillance of routine activities. We need to make decisions about the privacy consequences of those technologies. Existing patterns of usage for personal information developed at a time when privacy was not as highly valued or as widely debated. Much of the current trafficking in personal information developed without any public notice, awareness, or debate. It is questionable whether the patterns of the past and present will be acceptable in the future.

This report brings the debate about privacy costs back into the middle of the road by identifying some of the negative results for consumers from an unregulated, privacy-invasive market in personal data. It also points out some of the costs that businesses and consumers incur when privacy is not adequately addressed and the consequences for a democratic society as well. This report is not a complete or academic study of the issue of privacy costs. Rather, it identifies the

types of costs that are ignored in business sponsored studies. It also discusses societal goals, values, and methods that are not part of cost-benefit analysis.

This report includes no recommendations. Privacy remedies are a different subject. Formal remedies may or may not alleviate a problem or avoid a cost. Further, solutions are not limited to "all privacy" or "free trade in consumer data." Privacy and commerce can and must be compatible. The standard privacy toolkit offers a wealth of measures that allow consumers and business to coexist profitably in a commercial marketplace of goods, services, and privacy.

Privacy is an important value in making decisions about how we permit the processing of personal information. The benefits, costs, and consequences of privacy and of lack of privacy must be fairly assessed.