#2006-06
February 2006

Defending Your Financial Privacy: The Benefits and Limits of Self-Help

by

Robert N. Mayer, Ph.D.
University of Utah

The AARP Public Policy Institute, formed in 1985, is part of the Policy and Strategy group at AARP. One of the missions of the Institute is to foster research and analysis on public policy issues of importance to mid-life and older Americans. This publication represents part of that effort.

The views expressed herein are for information, debate, and discussion, and do not necessarily represent official policies of AARP.

AARP, 601 E Street, N.W., Washington, D.C. 20049
http://www.aarp.org/ppi

FOREWORD

Today's consumers face a significant challenge in navigating an increasingly complex marketplace and obtaining financial security. An important aspect of this financial management challenge is safeguarding their personal financial information from unauthorized access and theft. Threats to financial privacy have multiplied in recent years both in terms of their frequency and seriousness. In 2005, over 100 incidents of security breaches involving sensitive personal information exposed some 56 million consumers to potential identity theft. Given this situation and the continuing shift of responsibility for financial management and decision-making from employers and other institutions to individual consumers, the AARP Public Policy Institute commissioned Professor Robert N. Mayer of the University of Utah to investigate how consumers are coping with threats to their financial privacy.

The findings of *Defending Your Financial Privacy: The Benefits and Limits of Self-Help* indicate that consumers, on the whole, have been very responsible in heeding the advice offered by an array of government and private sources and adopting new behaviors to guard their financial privacy. These include everything from shredding financial documents and using secure mailing locations to using anti-spyware software and "always" or "most of the time" checking Web site security policies before paying online. Indeed, 60 percent of respondents to the survey conducted for this report indicate that they spend "a lot" or "moderate" amounts of time protecting their financial privacy. However, the survey also found clear evidence that a substantial minority of consumers avoids various offline and online transactions due to concerns about privacy. Not only does this signify fewer opportunities for business but also potentially diminished choices and benefits for consumers.

As Professor Mayer notes, the burden of protecting privacy should not fall solely on consumers. "Businesses and governments have a strong stake in creating a climate in which consumers are not only knowledgeable about how to defend their financial privacy but also are motivated to engage in privacy self-protection. This climate is best achieved when businesses and governments offer consumers efficient ways of guarding their privacy". The findings of this report are particularly relevant as Congress and the states consider proposals to: (1) require notification of consumers in the event of a data breach involving sensitive personal information and (2) allow consumers to initiate a "freeze" on their credit report. AARP believes that this report will contribute to a constructive discussion regarding privacy protection policies.

George J. Gaberlavage
Associate Director/Financial Services & Utilities Team
Sharon Hermanson
Senior Policy Advisor
AARP Public Policy Institute

EXECUTIVE SUMMARY

Background

Consumers, after a long period of enjoying the benefits of having their personal financial information easily transmitted and stored by sellers of goods and services, now confront significant new threats to their financial privacy. Identity theft no longer happens to *other* people, and breaches of sensitive data no longer only plague small, poorly operated companies. Millions of people have been victims of identity theft, and the security of account information of major companies has been compromised. How are consumers coping in this environment of fear and insecurity?

Purpose

This report investigates the state of consumer self-protection with respect to financial privacy. After assessing the advice being directed at consumers by government agencies, privacy activists, journalists, and businesses, the report summarizes and adds to survey research findings on the actions people are taking – and not taking – to defend their financial privacy. These actions by consumers establish the context for government policy and business initiatives in the area of financial privacy because the successes of all three are interdependent.

Methodology

Three new empirical studies are incorporated in this report. First, there is a content analysis of advice being offered to consumers on how to guard their financial privacy. The advice comes from thirty-two sources representing government agencies, nonprofit organizations, financial journalists, and for-profit companies. They include the Federal Trade Commission, the Privacy Rights Clearinghouse, *PC World* magazine, and American Express. While these sources do not exhaust all the advice being directed at consumers, they are among the most prominent and credible and hence represent the type of information people are likely to encounter during their self-protection efforts. The data were collected during November 2004.

The second empirical study is a small-scale effort to gauge the ease or difficulty of obtaining free access to one's credit report. The ability to obtain these reports was guaranteed by the Fair and Accurate Credit Transactions Act of 2003. This new right was made available beginning in December 2004 to people living in the western United States and then gradually extended to people in the remainder of the country. The study reported here is based on the experience of 77 people in a western state who tried to access their reports during the spring of 2005.

The third new empirical study conducted for this report is a telephone survey of a nationally representative sample of 1,010 people age eighteen and older. The survey asks respondents whether they have engaged in a range of privacy self-protection activities. Some of these activities, such as updating computer software, represent cautious engagement with companies and new technologies; other activities, such as refraining from shopping online or declining discount cards from grocery stores, involve avoiding potentially beneficial products and services. The data were collected November 3-7, 2004.

Findings

1. There is no shortage of advice for consumers on actions they can be taking to protect their financial privacy. The thirty-two advice sources analyzed for this report offered 105 unique suggestions. The average source dispensed fourteen pieces of advice, meaning that any single source of advice represents only a small portion of the overall range of self-protection ideas. Nevertheless, certain suggestions surfaced repeatedly, so it was possible to construct "top ten" lists of frequently tendered advice regarding both offline and online privacy.

The offline list of recommended behaviors is headed by:
• shredding documents that contain sensitive financial information,
• annually verifying the accuracy of credit report content, and
• sending outgoing mail from a secure location.

The most frequently offered advice for the online word is:
• refrain from giving out personal information unless a Web site's identity is verified or the site visit was initiated by the consumer,
• use firewalls to prevent unauthorized access to computers , and
• read Web site privacy policies for collecting, using, and sharing information .

2. While the time, money, and mental costs of following any single piece of advice can be minimal, the cumulative costs of privacy self-protection can be substantial. Some methods of defending personal financial privacy involve financial outlays, such as buying a new high-security mailbox, purchasing a cross-cut shredding machine, or subscribing to an identity theft monitoring service. Most self-protection actions, however, involve low-level but repeated expenditures of time. These actions include taking outgoing mail to a secure location, shredding documents containing sensitive financial information, and promptly checking the accuracy of all financial statements and bills. Even if the time, money, and mental costs of engaging in any single action are low, the cumulative costs of protecting financial privacy both offline and online can be high.

Given all the actions consumers could possibly be taking, the key is choosing those that are most efficient in the sense that they yield relatively high privacy dividends at relatively low cost. Having one's social security number removed, where possible, from identification cards, registering on the federal do-not-call list, opting out of prescreened credit card solicitations, and installing a computer firewall are examples of actions that are likely to be efficient in protecting privacy. However, not all such do-it-once-and-you're-done actions are as easy as they seem. A case in point is obtaining free copies of credit reports. According to a small-scale study of seventy-seven people, only thirty-nine percent (39%) were able to access online all three of their credit reports. While technical improvements have been made since this study was conducted in the spring of 2005, the results underscore the importance of designing mechanisms of privacy protection that avoid unnecessary mental costs associated with frustration and aggravation.

3. People vary in their desire for financial privacy, but large percentages of consumers have adopted new behaviors to guard their financial privacy. The national survey commissioned for this report found:
• 51% of respondents claim to "always" shred their financial documents,
• 49% "always" send mail from a secure location like a post office or locked mail box,
• 33% had paid to see their credit reports prior to the passage of the FACT Act,
• 59% have added or updated anti-spyware software
• 42% check Web site privacy policies "always" or "most of the time" before providing personal information, and
• 61% check Web site security policies "always" or "most of the time" before paying online.

These findings are highly consistent with the results of other surveys and strongly suggest that people have adopted a variety of new behaviors to protect their offline and online privacy. There are still plenty of chinks in the privacy armor of consumers, especially the practice of carrying social security numbers in wallets and purses, but consumers have clearly learned new behaviors or, at least, new norms of what they *should* be doing.

4. Most people perceive that they are currently working hard to protect their financial privacy. When asked to describe the amount of time and effort they devote to protecting their financial privacy, sixty percent of respondents describe the amount as "a lot" or "moderate." Moreover, consumers have responded aggressively to offers of government assistance in guarding privacy, like signing up for the Federal Trade Commission's do-not-call list and trying to obtain free copies of their credit reports. It would not be surprising if most consumers feel that they are "doing their part" in defending their financial privacy.

5. Most people have chosen to take new sensible precautions rather than give up transacting with firms offline and online, but a significant minority of consumers are choosing to avoid these transactions rather than expose themselves to invasions of their financial privacy. The survey commissioned for this report found clear evidence of offline and online avoidance behavior, some of which can be traced to concerns about privacy:
• 24% of respondents "always" pay restaurant bills with cash because they are worried about credit and debit card information being misused,
• 64% "never" accept offers to sign up for frequent-buyer discount cards, such as thoses offered by grocery stores and gas stations,
• 64% of respondents report having asked a company to take their name off mailing or phone lists, and
• of the two-thirds of the sample who had a computer with Internet access at home, 32% had never purchased anything online.
These forms of avoidance and withdrawal are hardly confined to elderly consumers who are unfamiliar with new technologies. Without a sense of confidence about the ability to control one's financial information, people of all ages and characteristics may decide that avoidance is the best protection strategy.

Conclusion

Consumers are "doing their part" by heeding the advice offered by various experts on how to defend personal financial privacy. Sixty percent of respondents in the 2004 AARP survey reported spending "a lot" or "a moderate amount" of time and effort protecting their financial privacy. People could show more restraint in carrying around their Social Security numbers, change their passwords and PINs more often, and show more persistence in reading the lengthy privacy disclosures provided by financial institutions under the terms of the Gramm-Leach-Bliley Act. On the whole, however, consumer actions are going beyond costless verbal expressions of concern for their financial privacy. In a few short years, people have learned new habits related to the way they receive, send, and discard mail; the way they access their financial accounts; and the way they operate their computers. They are now in the process of learning another new habit—how to read their credit reports and correct any misinformation they contain.

Privacy is not costless. More privacy can mean higher prices, less convenience, and greater threats to personal health and safety. The consumer is therefore in the best position to decide how much privacy he or she wants. It does not follow, however, that the task of achieving this desired level of privacy falls solely on the shoulders of consumers. Nor is privacy a matter of consumer vs. business vs. government responsibility. Businesses and governments have a strong stake in creating a climate in which consumers are not only knowledgeable about how to defend their financial privacy but also are motivated to engage in privacy self-protection. This climate is best achieved when businesses and governments offer consumers efficient methods of guarding their privacy. In the absence of high benefit-low cost methods, consumers may succumb to "privacy protection fatigue" and choose instead to avoid new and potentially beneficial financial services.

TABLE OF CONTENTS

INTRODUCTION

In the not-very-distant past, consumers might have been able to dismiss identity theft, "phishing," "pharming," and other threats to financial privacy as problems that only happened to *other* people. Today, people know better. Consumer complacency has been shattered by a steady stream of news about sensitive data being lost by or stolen from major companies. Consumers have been surprised as well to discover the existence of largely unregulated entities—like ChoicePoint and Acxiom—that collect, aggregate, and sell their personal information. Keeping up with threats to privacy can feel like a full-time job for the consumer, because as quickly as authorities unmask and defuse one new threat, a new and more insidious one seems to arise.

How do consumers cope with complex and rapidly changing threats to their personal privacy? Some people do nothing because they blindly trust that someone else—businesses, government, privacy advocates—will protect their privacy. Others succumb to paranoia and close themselves off from new technologies. Most people fall somewhere between blind trust and paranoia. They want to enjoy the benefits and conveniences of modern life while minimizing the threats to their personal privacy. But striking this balance requires a lot of work. What privacy-protection actions are individuals being advised to take, what actions do they already take, and how much more can people reasonably be expected to do? How can government and industry action create an environment that supports individuals as they seek the level of privacy that is right for them? This report, which focuses on financial privacy and draws on both new and existing data, answers these questions.

THE NATURE AND IMPORTANCE OF FINANCIAL PRIVACY

Financial privacy is an important component of overall personal privacy. Other domains of personal privacy include health (e.g., genetic makeup), education (e.g., grades in college), communication (e.g., parties to whom we address phone calls and mail), and politics (e.g., candidates for whom votes are cast). Financial privacy is especially important because it pertains to the daily actions of virtually every adult and overlaps with other domains of personal privacy (e.g., medical expenditures and campaign contributions).

What Is Financial Privacy?

Like the broader concept of personal privacy, financial privacy is neither simple nor one-dimensional. Financial privacy can be defined as the ability of an individual to control his or her personal financial information. Within this definition, however, lie two related but distinct concerns: data protection and freedom from intrusion. Data protection speaks to the potential misuse of personal financial information that is contained in databases held by financial services companies and units of government. The fair information practice principles of notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress were developed in response to concerns about data protection.[1]

With all the attention to data breaches and identity theft, it is easy to lose sight of a second important aspect of financial privacy—the loss of privacy that results from intrusive offers to borrow, buy, invest, or contribute funds. An ill-timed phone call, an overly aggressive door-to-door salesperson, or an annoying pop-up ad on a computer screen are examples of intrusions on financial privacy. These intrusions were presaged in 1890 in a *Harvard Law Review* article by Samuel Warren and future Supreme Court Justice Louis Brandeis. The authors defined privacy as "the right to be let alone."[2] Whereas data protection involves forestalling unwanted communication *to* others, freedom from intrusion consists of preventing unwanted communication *from* others. Both aspects of financial privacy, *data protection* and *freedom from intrusion*, are important to consumers and are included in the popular meaning of the phrase "financial privacy;" therefore, both aspects are covered in this report.

Why Is Financial Privacy Important?

The importance of financial privacy is easy to underestimate...until it is lost. Some people may say, "I have nothing to hide, so why should I care about privacy?" These individuals may not recognize that invasions of privacy can have serious financial and nonfinancial consequences. Consider identity theft. According to a 2003 study commissioned by the U.S. Federal Trade Commission, 27.3 million people in the United States had been victimized by identity theft during the previous five years, at a cost of $48 billion to businesses and financial institutions, plus an additional $5 billion to consumers for out-of-pocket expenses.[3] Another study found that victims of identity theft lose time as well as money—an average of 600 hours spent over several months trying to resolve the problems created by identity theft.[4]

Phishing—the use of deceptive emails to trick recipients into divulging financial data such as credit card numbers, Social Security numbers, and account names and passwords—is one of the newest tricks in the identity thief's book.[5] MessageLabs, a provider of email security services for businesses, measured an increase in phishing email from 279 instances in September 2003 to more than two million by a year later.[6] The April 2005 report of the Anti-Phishing Working Group, a coalition of banks, Internet service providers, and other businesses, documented a 15 percent average monthly increase in phishing Web sites between July 2004 and April 2005.[7] While most people like to think they are too smart to be hooked by phishing, seven of 10 respondents in a study of Internet users acknowledged they had unintentionally visited a spoofed Web site, and more than 15 percent admitted to providing it with sensitive financial information, including credit card numbers, checking account information, and Social Security numbers.[8] The study also estimated that the annual monetary loss to U.S. victims of phishing was about $500 million.

When personal financial data fall into the hands of the wrong parties, major financial loss can occur. Even in the "right" hands, a lack of financial privacy can result in losses through financial discrimination. Many have raised the possibility that employers and insurers will discriminate against people based on their genetic makeup,[9] but discrimination based on a person's income or past purchases is also possible. In a world where more and more transactions occur over the Internet, how long will it be before, say, an airline offers different prices to different travelers based on the airline's calculation of each customer's ability and willingness to pay?[10]

Even people who believe they have "nothing to hide" and no data to protect may object to intrusions into their financial privacy. For example, a person whose parents died recently may not appreciate telephone calls from financial services companies offering advice on how to invest an inheritance. Similarly, a woman who goes online to buy a book about breast cancer may become upset when her computer is suddenly filled with pop-up ads for breast enhancement procedures.

So, if financial privacy is so important, why aren't people clamoring for more of it? One reason is that a loss of financial privacy may be viewed as the inevitable price of economic progress. Recall, for instance, computer company executive Scott McNealy's famous 1999 remark, "You have zero privacy anyway. Get over it."[11] Similarly, people may be willing to sacrifice some degree of financial privacy in exchange for other goals, such as personal safety, convenience, or financial gain.[12] For example, most people are glad to give up some of their financial privacy for tangible gains in the fight against terrorism. On a more mundane level, people let grocery stores track their purchase patterns through preferred shopper programs in exchange for occasional discounts on grocery items. In addition to involving trade-offs with other values such as safety and convenience, actions in defense of financial privacy can be costly in terms of time and money. For these reasons, consumers may take only some of the many actions that could enhance their financial privacy. Yet, as we see later in this report, most consumers respond enthusiastically when government and corporate action reduces the costs of guarding financial privacy.

Organization of this Report

This report has four sections. The first synthesizes the vast amount of advice government agencies, journalists, privacy advocates, and businesses offer to consumers concerning ways to protect their financial privacy. This section not only discusses the most commonly offered pieces of advice, but given the time, money, and psychological costs involved in protecting financial privacy, identifies the most efficient steps people can take. The second section describes the financial and nonfinancial costs of protecting financial privacy. It contains the results of a study of the nonmonetary costs involved in exercising the new consumer right of free access to credit reports. The system for doing so, at least as initially constructed, is far from free when one considers time and energy costs. The report's third section relies on survey research, including a national survey conducted specifically for this report, to assess how consumers respond to this advice. In particular, which pieces of advice are consumers heeding and which are they ignoring? The final section contains recommendations for government, business, and nonprofit groups regarding ways to increase the effectiveness and efficiency of consumer efforts to protect their financial privacy.

PART 1: CONSUMER ADVICE AND EDUCATION

Financial Privacy in Daily Life

The number of times a day that a consumer faces choices about financial privacy is potentially overwhelming. Imagine a day in the life of a person named Elizabeth. Awakening from a particularly good night's sleep, Elizabeth decides to go jogging in the park before heading to work. She pops one of her credit cards into the pocket of her jogging shorts just in case she wants to buy a drink or something special for breakfast on the way back from the park. Just as Elizabeth is about to walk out the door, the phone rings. She notices on her caller ID that the call is coming from a credit card company offering her yet another card with benefits too good to refuse. Elizabeth chooses not to answer the call but mutters to herself, "I really must figure out how to place my phone number on that government do-not-call list."

On the way out of the apartment building, Elizabeth stops to check that her mailbox is locked. Sometimes, when inspecting a particularly interesting-looking piece of incoming mail, she forgets to lock it properly. Outside, Elizabeth rounds the first street corner and passes her bank. It is only 7:30 a.m., too early to pick up that box of checks that she asked not be mailed to her for fear they might be stolen. A few blocks further on, Elizabeth passes the post office and remembers the stack of bills that were on her dresser in need of mailing. She is annoyed at herself; she could have easily taken the letters with her and placed them in a secure post office box rather than leaving them for all the world to see in the box for outgoing mail at her office.

The morning is beautiful and Elizabeth runs with special vigor. Almost back home, she decides to stop at the local coffee shop and order something tasty. She notices that the cute guy working the counter is new. She hands him her credit card, and he notices the words "Check my ID" on the back of the card. When he asks Elizabeth for a form of identification, she is annoyed that she doesn't have one. How embarrassing! Fortunately, the clerk isn't a stickler for detail and runs her credit card through.

Upon arriving back at her apartment, Elizabeth notices that her copy of the morning newspaper has not arrived yet. "No problem," she says, "I'll just go online and submit a request for another copy." In attempting to log onto the newspaper's Web site, however, Elizabeth realizes that she has forgotten her login name and password. She tries a couple of likely possibilities, but none of them work. "Oh well," she sighs, "I'll just pick up a copy of the newspaper on my way to work."

After showering and dressing, Elizabeth notices that she has just enough time to catch her bus to work. But today is Wednesday, the day her garbage is picked up each week, and she has forgotten to shred the big stack of financial documents she has let accumulate in the corner of her small living room. She had promised herself that she would finally read all of those privacy notices that come from her bank, insurance company, phone service, and stock broker. Normally, she would let the untidy stack of paper continue to grow for another week, but her parents are coming for dinner in two days. Her choice is either to throw out the documents without running them through the shredder or to be late to work. Elizabeth is so conflicted she could scream.

At home after work, Elizabeth goes online to purchase a birthday present for her brother. She knows she should read Web site privacy policies, make sure each site's methods of payment are secure, update her antivirus software, and clear her browser's memory when she is finished. After a hard day of work, though, it seems like such a hassle to be a vigilant consumer. She would so much rather be thinking about the cute server in the coffee shop.

It is easy to sympathize with Elizabeth and the fact that guarding her financial privacy has become such an important part of her daily routine, but at least Elizabeth knows some of the ways to protect herself. She has been exposed to at least some of the information directed to consumers regarding how to protect their financial privacy. Some of this information has been facilitated by the federal government, as in the case of the privacy inserts that accompany statements from banks, mortgage firms, insurance companies, investment houses, and tax preparers. But the vast majority has been provided voluntarily by a variety of government and private entities. What exactly does this information advise consumers to do?

Survey of Consumer Advice

Sources of advice on how to safeguard financial privacy are numerous, and new ones appear frequently. To study these efforts at informing and educating consumers, we drew a sample in November, 2004 of 32 of these sources of advice, emphasizing those that consumers would be most likely to consult due to the source's familiarity, credibility, and/or accessibility. Some of the advice appeared originally or simultaneously in print form, but all of the 32 sources can be found online. The Websites containing privacy advice appear readily if a person searches on Google or Yahoo using the phrase, "protect financial privacy" or "avoid identity theft." Because advice on guarding financial privacy comes from many quarters, our sample gives roughly equal coverage to four general types of sources: government agencies, nonprofit organizations, financial journalists, and for-profit companies. Within the sample of 32 sites, we also tried to give equivalent prominence to advice on protecting privacy offline (e.g., sending regular mail, receiving phone calls, shopping at stores) and online (e.g., reading financial news, purchasing from online vendors). We could have included more sites, but we found that adding more did not alter the substantive findings. The list of 32 advice sources, which appears in Appendix 1, contains well-known entities from the government (e.g., U.S. Federal Trade Commission), nonprofit (e.g. Privacy Rights Clearinghouse and Consumers Union), journalistic (e.g., *PC World* and *Motley Fool*), and business (e.g., Equifax and American Express) arenas.

The advice offered to consumers on protecting financial privacy comes most often in the form of lists, such as "Protect Your Privacy: Ten Simple Steps"[13] or "15 Must-Know Tips for Protecting Your Identity."[14] The Electronic Privacy Information Center, a leading privacy advocacy organization, offers 10 consumer privacy resolutions for the new year 2005.[15] Frank Abagnale, a reformed con man and the source for Leonardo DiCaprio's character in the movie, *Catch Me If You Can*, presents "14 Tips To Avoid Identity Theft."[16] There is no apparent rationale for the exact number of recommendations on these lists or the order of the advice. There are, of course, entire books devoted to the subject of personal privacy, such as Eric Gertler's *Prying Eyes*,[17] or to the prevention of and recovery from identity theft.[18] By virtue of their length, these books are more comprehensive and more systematic in their privacy recommendations than lists and other brief documents, but few consumers have purchased them compared to the number of people

who have read a pamphlet or brief article on guarding their financial privacy. For the sake of representativeness, however, our sample includes one such book, Gertler's.

The 32 advice sources analyzed for this report comprised 105 unique suggestions on how to guard one's financial privacy, with that number reflecting our best effort to combine similar pieces of advice into a single category. For example, essentially the same piece of advice can be framed in terms of risk-increasing behavior to avoid (e.g., "never leave mail in your mail box overnight") or risk-reducing behavior to undertake (e.g, "remove your mail promptly after it arrives"). Each source had an average of 14.4 items of advice per source, with a range from three to 47. Any single information source (other than a book) contains a sliver of the total pie of advice. Tables 1 and 2 show the most frequently offered pieces of advice for protecting financial privacy offline and online. To the extent that there is a consensus among the advice givers, these lists are it.

Table 1: Most Frequently Offered Advice on Guarding Privacy Offline

Rank	Advice
1	Shred or otherwise destroy documents containing sensitive financial information.
2	Obtain and verify credit report at least annually.
3	Send outgoing mail from a secure location.
4	Don't give out personal information without verifying a party's identity or unless you initiate the transaction.
5	Minimize personal information, especially Social Security number, on checks or forms of identification (e.g., driver's license).
6	Promptly monitor accuracy of monthly or quarterly financial statements.
7	Don't carry your Social Security number in your wallet or purse.
8	Minimize the personal information you carry with you.
9	Don't give out your Social Security number unless absolutely necessary.
10	Keep financial information at home secure from other people.

Table 2: Most Frequently Offered Advice on Guarding Privacy Online

Rank	Advice
1	Don't give out personal information without verifying identity or initiating contact.
2	Use firewalls to prevent unauthorized access to computers.
3	Read Web site privacy policies for collecting, using, and sharing information.
4	Regularly update virus protections.
5	Read Web site security policies for information transmission.
6	Use difficult-to-guess passwords.
7	Properly wipe or otherwise destroy hard drive before computer disposal.
8	Give minimal personal information to Web sites.
9	Get updated security patches.
10	Screen, reject, or otherwise control cookies on your computer hard drive.

Some of the recommendations on these two "best of" lists will strike many people as matters of common sense. Should a person really have to be told not to give out his or her Social Security number to an unknown party or to read the privacy and security policies of unfamiliar Web sites? Other recommendations will seem quite useful even to savvy consumers. The main problem with these lists is that they lack an underlying structure, so they seem ad hoc. To give structure to the more than 100 recommendations to consumers, we developed a five-category organizational scheme. The five categories are privacy-enhancing actions related to:

- receiving information;
- sending information;
- storing information that is primarily under the consumer's control;
- monitoring information that is stored by other parties; and
- disposing of information.

Table 3 shows how some of the most frequently offered pieces of advice fit into these five categories.

Table 3: Categories of Advice on Financial Privacy

Information	**Offline**	**Online**
Receiving	Opt out of prescreened credit card offers	Screen unnecessary cookies
Sending	Send mail from a secure location	Encrypt communications
Storing	Don't carry Social Security number	Use firewalls
Monitoring	Check credit report annually	Read Web site privacy policies
Disposing	Shred documents	Wipe hard drive when disposing

The five-category scheme is useful in gauging the comprehensiveness of any source of information on financial privacy. The more categories covered, the more complete the advice. Awareness of the five categories can also help consumers act in a balanced and *efficient* fashion. It makes little sense, for example, to devote substantial resources to preventing the receipt of unwanted information (e.g., buying a new lockable mailbox), while ignoring privacy vulnerabilities in disposing of that same information (e.g., failing to shred documents containing sensitive financial information).

Efficiency in guarding one's financial privacy requires more, however, than making sure not to ignore one or more of the five categories. Consumers vary widely in their desire for financial privacy and, more important, in the costs they are willing to incur to protect their financial privacy. These costs include the expenditure of time, money, and physical and mental energy. Efficiency, therefore, involves achieving the greatest level of privacy from a given expenditure of time, money, and effort (or reaching a desired level of privacy at the least possible cost). To be efficient in the pursuit of financial privacy, consumers need to begin by taking actions that are both inexpensive and effective.

Unfortunately, there is virtually no research on the relative effectiveness or relative costs of various privacy-protection strategies. Some strategies do have the *potential* to be efficient inasmuch as either (1) a one-time action pays long-term dividends (e.g., opting out of prescreened credit card solicitations) or (2) intermittent, low-cost actions yield unique protections (e.g., using a credit card when shopping online). For example, signing up for the national do-not-call list requires only a single phone call or Web site visit, but the list's protection from unwanted calls lasts five years. Table 4 lists 10 actions that appear to be potentially efficient.[19] Only the last item in Table 4, installing a firewall, involves more than a minimal financial outlay; it is included because of the many problems firewalls can forestall.

Table 4: 10 Efficient Actions for Guarding Financial Privacy

Sign up on the national do-not-call registry at 1-888-382-1222 or www.donotcall.gov.
Opt out of pre-screened credit card offers by dialing 1-888-5-OPTOUT.
Exercise the financial privacy rights afforded by Gramm-Leach-Bliley Act.
Exercise the right to get free annual copy of your credit report at www.annualcreditreport.com.
Remove unnecessary or infrequently used personal information from your wallet or purse.
Put minimal information on your personal checks.
Get a credit card that has your photograph on it.
Look for reputable icons and seals of approval to verify Web site privacy and security practices.
Use a credit card instead of a debit card when buying online.
Install a firewall and configure it to start automatically.

Some consumers, especially those who have already been victims of identity theft and incurred the substantial cost of recovering from it,[20] will care more about their overall level of protection than the efficiency of their actions. These consumers will be willing to spend time and money beyond the most efficient actions exemplified in Table 4. The next section of this report considers in more detail some of the monetary and nonmonetary costs of protecting one's financial privacy.

PART 2: COSTS OF DEFENDING FINANCIAL PRIVACY

If a person is willing to spend money to protect his or her financial privacy, it is not difficult to draw up a shopping list. To protect financial data as they enter and leave the home, one might follow the commonly dispensed advice to purchase a cross-cut shredder (price for a home model: $50–$130)[21] and a new, secure mailbox (price range, uninstalled: $50–$350).[22] To safeguard one's credit report against fraudulent activity, new inquiries, and new accounts, another common recommendation is to sign up for a credit-monitoring service (typical price: $100 per year).[23] Most experts on online privacy strongly recommend an additional purchase: a suite of software containing updated antivirus, antispyware, and anonymizing program (typical price: $75).[24] To screen out unwanted phone solicitations at home, one can purchase caller ID service (typical price: $85 per year, plus installation and possible equipment upgrade).

In short, financial privacy can be purchased, but it doesn't come cheap. It is easy to accumulate annual expenditures of $300–$500—about as much as many people pay for cell phone service or homeowner's insurance. Dollar expenditures only capture part of the cost of defending financial privacy. There are additional non-monetary costs, especially time costs. Buying a shredder is of little value unless a person uses it, and using it takes time. Antivirus software not only takes

time to install; it can slow down the logging in process every time a person gets on his or her home computer. At least the consumer anticipates the time costs of these activities . The time costs of other activities can be more than expected...and more than necessary. A good example is the new system for allowing consumers free, annual access to their credit reports.

"Free" Access to Credit Reports: A Case Study

The Fair and Accurate Credit Transactions (FACT) Act of 2003 granted consumers for the first time free and annual access to the credit reports compiled by the three major U.S. credit reporting agencies—Equifax, Experian, and TransUnion. Free access began December 1, 2004, in the western United States and was gradually extended eastward until U.S. consumers in all states became eligible to see free copies of their credit reports on September 1, 2005.

As we discussed in Part 1, checking the contents of one's credit reports regularly is second only to shredding documents containing sensitive financial information in terms of how often consumers should undertake this privacy-protection strategy. In Part 2 of this report, we said that, even before implementation of the FACT Act, about a third of a national sample of consumers had *paid* a credit reporting agency to see the contents of their credit report; and, according to a study conducted for the U.S. Government Accountability Office, 58 percent of consumers had *seen* their credit reports before, perhaps after having been denied credit, insurance, or employment.[25] Hence, given the importance of examining the contents of one's credit reports, and the willingness of some consumers in the past to pay for access to them, one would think that free annual access would be a major advance for consumers. But how easy is it to exercise the new right of access provided by the FACT Act? Accessing the reports may be free in terms of money but not in terms of time, effort, and, aggravation.

Early Reports of Problems. The first complaint to arise about the system of granting consumers free annual access to their credit reports surfaced less than a week after the system was opened to consumers in the western United States. On December 7, 2004, representatives of six major consumer organizations wrote to the Federal Trade Commission to protest the fact that links to the single site for obtaining the results were blocked.[26] For example, links on the Web sites of reputable consumer organizations and mainstream news services were blocked initially. This practice of blocking links was discontinued in March 2005.

More critical of the new system were two reports by the World Privacy Forum, a nonprofit organization devoted to the study of privacy and technology. The first report, issued in February 2005, pointed out a host of "imposter sites," often with URLs similar to www.annualcreditreport.com, whose purpose is to charge people for the credit reports they are entitled to receive for free and/or to sell credit scores (which are not offered free).[27] The report found that some of the imposter sites were owned by one of the three major credit reporting agencies. The report contained several other criticisms: the confusion of free and paid services on the menu bars of individual company sites, the need to read four different privacy policies, and the practice (since discontinued) of one credit reporting company, TransUnion, of requiring consumers to opt out of marketing and information sharing. A follow-up report issued in July 2005 found that the number of imposter sites had more than doubled.[28] The overall conclusion of both reports was that consumers were often better off calling or writing for their credit reports

than they were getting them online. (Of course, calling and writing require consumers to wait for their reports and may entail their own privacy risks.)

In addition to the existence of imposter sites, major search engines could not be relied on to help consumers find the legislatively required, industry-operated, legitimate site for obtaining free credit reports. Journalist Stephanie Zimmermann demonstrated the problem.[29] She typed "free credit report" into Google. According to Zimmerman, the legitimate site was not listed until the fifth page of results, where it was the 30th entry overall. Most of the preceding 29 search results referred to companies that might provide free credit reports but only in conjunction with other paid products, such as credit-monitoring services, identity theft insurance, or credit scores.

Study of Additional Problems. Given the documentation of problems that potentially beset consumers *before* they arrive at the annualcreditreport.com Web site, we conducted a new study for this report of the problems consumers may experience *after* they have managed to locate the government-mandated, industry-operated site. The study approximated the process by which consumers, acting naturally in the privacy of their own home, tried to access and reaccess their free credit reports, as the FACT Act mandated. Study participants were directed to the annualcreditreport.com site and asked to access all three of their credit reports. Then they were directed to reaccess any reports they initially obtained successfully. (While the FACT Act does not specify a right to reaccess a free report within a reasonable time period, consumers might want to recheck the contents of one credit report after seeing something odd in the content of another.) Using a one-page questionnaire, subjects were asked to (1) time the various phases of the exercise, (2) rate the ease of use of the three company Web sites, and (3) describe any difficulties experienced in accessing or reaccessing their credit reports. Subjects were asked *not* to examine the contents of the credit reports, including the accuracy of their information, or to comment on the ease of navigating through the report. Subjects were also asked *not* to spend time thinking about purchasing credit scores.

The majority of study participants were recruited from two undergraduate classes at a western, public university. To make the sample more closely resemble the adult population, students were invited to recruit one additional study participant, with preference given to someone older than a typical college student. To ensure that participants would have credit reports, they had to have at least one credit or debit card in their name. All told, 77 people chose to participate in the study: 28 males and 49 females. The average age of participants was 30, with a range of 18 to 78. The data were collected between late April and the middle of June 2005. (Several problems identified in this study were ameliorated or eliminated after the study's completion.)

Problems with the Master Site. The study uncovered four main problems in using the master site, annualcreditreport.com, the necessary gateway for obtaining free credit reports. First, the study investigators noted that the privacy policy is sufficiently long (almost 2,000 words) that few consumers are likely to spend the time to read it, certainly not in its entirety. Second, the investigators also found that, despite the sensitive nature of the information visitors are asked to provide (e.g., Social Security number), the site does not use privacy or security certifications, such as TRUSTe or VeriSign. By allowing consumers to click through to trusted sites, these certifications help consumers differentiate the single legitimate site from "pharming"(redirecting Web traffic from the intended site to another one) and other methods of Internet fraud.

Annualcreditreport.com does allow people to click on the logos of the credit reporting agencies, but this is of limited help, because some imposter sites also direct people to credit reporting agencies. A third problem highlighted by study participants is the site's failure to explain that a consumer who wants to access all three credit reports as part of a single visit should simultaneously check the boxes next to all three companies. With no way to know this procedure, many study participants reported being annoyed by having to reenter all of their information for each credit report. A fourth problem mentioned frequently by study participants is the failure to explain whether and how a consumer can reaccess a given credit report within a reasonable period of time. The lack of information about the reaccess process on annualcreditreport.com and the individual company sites resulted in the majority of study participants being unable to reaccess their credit reports.

Problems with the Company Sites. The study revealed that participants had more problems using the sites of the individual credit reporting agencies than using the master site, annualcreditreport.com. These problems surfaced virtually every step of the way: registering at the company's site, authenticating the consumer's identity, and finding information about how to reaccess one's credit report within the statutory 30 days. For example, TransUnion requires consumers to create a username and password, but does not explain why. Equifax requires consumers to give their email address in addition to creating a username and password, but only if they want to reaccess their reports. Some subjects wondered if, by creating a username or giving their email address, they were signing up for something they might not understand or want.

A variety of problems arose in trying to access the three credit reports. As a result of these problems, only 30 of 77 people (39 percent) were able to access all three of their credit reports. Sixty-one were able to access their Equifax report, 58 their Experian report, and only 38 their TransUnion report. The most common reason cited for being unable to access the TransUnion report was the site's failure to accept an address, account number, Social Security number, or other information that the study subject insisted was correct. TransUnion's stringent authentication process may prevent unauthorized access to its credit reports, but in doing so, it might go too far. The most common reasons for being unable to access Equifax or Experian reports were similar to each other: either technical malfunctions (e.g., "site temporarily unavailable") or unexplained requests for consumers to request their reports by mail (e.g., "Internet Delivery Unavailable—Mail in Request"). Sending for and receiving a credit report by regular mail raises its own privacy problems, since both the request and the report are likely to contain highly sensitive financial information.

Ratings of the three sites correlated highly with the ease or difficulty of accessing their respective credit reports. In general, study participants found the Equifax and Experian sites fairly easy to use, and they considered the amount of information required for identification to be reasonable. Ratings dropped for Equifax and Experian, however, for the clarity and prominence of their instructions for reaccessing the site within the 30 days allowed by law. The same general pattern held for TransUnion, but with lower ratings in each category of Web site performance than those for Equifax and Experian.

Subjects were asked to record the time spent on each task. The average amount of time spent registering on the annualcreditreport.com site and accessing (or trying to access) the three credit reports was 40 minutes. People who successfully accessed all three reports spent slightly longer—44 minutes—than the overall average. Recall that subjects had to begin at the annualcreditreport.com site, so these time estimates do not include any time spent finding the master site. Subjects were asked to leave each of the credit agency sites as soon as they were sure they could reach their reports...or when they gave up trying. Hence, subjects did not spend any time looking at the contents of their credit reports, something that the typical consumer certainly would do. Finally, subjects were not explicitly directed to read the privacy policies on all four sites, although some may have spent time doing so. Reading these policies would add to the time vigilant consumers spend on these sites. In light of these considerations, it seems conservative to conclude that a typical consumer, acting under everyday conditions, would take at least an hour to find and register at the master site, access all three reports, and conduct a cursory examination of them.

Part of the study was intended to determine whether people could reaccess their credit reports. Although the FACT Act does not explicitly direct credit reporting agencies to provide reaccess, servies that charge for access generally allow reaccess within a reasonable period of time, and all three major credit reporting agencies have chosen to provide some free reaccess privileges. Study participants were asked to close their browsers after accessing (or trying to access) all three credit reports. They were then asked to reaccess any report they had already accessed successfully. Instructions for the initial access task were printed in bold letters and were as follows: **Before you leave each of the three credit reporting company sites, pay attention to whatever is needed to be able to reaccess your report within 30 days**. Consumers acting under real-world conditions might not want or need to reaccess their reports. Most consumers who decided later to reaccess a report would have likely paid far less attention than our study subjects regarding how to do it. Hence, the level of difficulty our subjects experienced probably understates the level of difficulty encountered under natural conditions, if a consumer tried to reaccess a report.

People were successful in reaccessing reports only 70 percent of the time, and the percentage did not vary greatly by credit reporting agency. Slightly less than half of the people who were able to access all three reports initially (14 of 30) were able to reaccess all three of them. The major reason for this low percentage appears to be the absence of clear and conspicuous instructions for reaccess on both annualcreditreport.com and the sites of the individual credit agencies. Some instructions do not seem designed to encourage reaccess. For example, the Equifax site asks visitors, “Would you like to view this credit report online free for 30 days?” The consumer must then *change* a button from “no” to “yes” to avoid losing the privilege of reaccessing a report. Moreover, this question appears before the consumer gains initial access to his or her credit report, that is, when reaccess is not particularly salient to the consumer. Another problem is that notifications of the abililty to reaccess a report are inconspicuous. Experian’s notice, for instance, appeared in a small, hard-to-read font.

Independent of the different methods used by the three companies, one problem plagues all of their sites. Consumers are confused about whether to gain reaccess by going back to annualcreditreport.com or by going to the sites of the individual companies. If consumers chose

the first option, annualcreditreport.com denied their request. This confusion appears to account for the majority of failed attempts at reaccessing reports. (Again, improvements have been made with respect to reaccess since the study's completion.) Even if a consumer realized the need to gain reaccess through a company's Web site, it was difficult to know where on the site to go or what to do once one arrived there. This is true of all three company sites. Equifax is the only site with the explicit link, "View your credit again," but that link was not conspicuous.

Finally, throughout the registration, authentication, and reaccess process, consumers are offered opportunities to purchase products and services from the credit reporting agencies. Equifax attributed its selling effort to the government with the statement: "Under the FACT Act, we are required to offer you the opportunity to purchase your Credit Score." This statement is technically . Section 609(a)(6) of the Fair Credit Reporting Act, amended in 2003, requires credit reporting agencies to "clearly and accurately disclose" that consumers may request and obtain a credit score. This requirement appears to have been interpreted as an opportunity to aggressively market credit scores but without clearly and conspicuously disclosing whether consumers will receive the well known FICO score or a different one.

Overall, this small-scale study of consumers trying to access and reaccess their credit reports reveals a system with multiple glitches that likely added to the time and money consumers originally expected to spend in exercising their new rights and options under the FACT Act. As one consumer confided to a journalist, "It seems like they [the credit report agencies] are doing everything they can to make this as hard as possible."[30]

Of course, many actions consumers can take to protect their financial privacy are far easier than accessing and reviewing credit reports, although few are recommended as strongly. For example, shoppers can be on guard for "shoulder surfers" who attempt to watch or listen while personal financial information, such as debit card PINs, is used. Online, computer users can periodically purge their Web browsing history and change their passwords frequently. There is a limit, however, to what reasonably cautious but busy consumers can and will do to guard their financial privacy. In the next section of this report, we compare the most common advice to consumers (see Part 1) with the actions consumers actually take to limit unwanted intrusions into their financial affairs and unwanted use of their financial data.

PART 3: FINANCIAL PRIVACY MANAGEMENT BEHAVIOR: ADVICE VS. ACTION

There are many actions that privacy professionals believe consumers *should* take to guard their financial privacy. In three instances, this advice has been organized in the form of a privacy "quiz" or "IQ test" by means of which consumers can test their own behavior against the recommendations of experts.[31] (These quizzes are in Appendix 2.) These quizzes were designed as teaching devices rather than evaluation tools, but what if such a quiz was actually given to a representative sample of U.S. adults? What score would they earn?

In this section, we essentially administer a privacy test that compares what the experts say consumers *ought* to do to protect their financial privacy with what consumers *actually* do. We administer this privacy test in two steps. First, we review the results of a number of large-scale surveys each of which includes a few questions about privacy behavior, both online and offline.

This review gives a general picture of the actions people claim to take in defense of their financial privacy. Second, we use data from a survey commissioned for this report to generate offline and online test scores of the American public's privacy-protection behavior. Although the number of items in each test is limited, the results may nevertheless provide direction in furthering self-protection on the part of consumers and may suggest the limits of self-help as a consumer protection strategy.

Survey Research

It is important to note that financial privacy quizzes don't have right and wrong answers as in traditional tests. Privacy quizzes ask people whether they take various privacy-protection actions. While these actions are desirable if a person values financial privacy, one must keep in mind that financial privacy carries a cost, and, for some people, that cost may outweigh the benefit. For example, several lists of recommendations urge consumes to use cash rather than a credit or debit card. While using cash may enhance financial privacy, using a credit or debit card may be more convenient and may earn the consumer benefits such as cash rebates and frequent-flier miles. So it is far from self-evident that an individual should always use cash. As another illustration, consumers who register on the national do-not-call list enjoy the benefits of fewer telephone interruptions, but they also forgo the opportunity to hear about new and potentially beneficial telemarketing offers. Hence, one cannot assume that consumers who do more to protect their privacy are more responsible or more rational than those who do not. Some people may simply be, in Alan Westin's words, "privacy pragmatists,"[32] while others may be largely unconcerned about their financial privacy. Given the high degree of concern expressed in public opinion surveys about privacy and identity theft, however, we proceed on the basis that, for many consumers, "more privacy is better."[33]

A second caveat concerns the validity of the survey responses.[34] The skeptic can be excused for asking whether survey responses measure what consumers think they *should* be doing or what they *actually* do. Researcher George Milne asked the same question.[35] He found that, at least among university students, respondents answer privacy questions quite honestly. Among his survey respondents, there was little relationship between a measure of "social desirability" (the tendency of people to answer questions to gain social approval) and their claims of taking, or not taking, a variety of offline measures to prevent identity theft. Another reason to feel confident about survey results is their relative consistency across surveys. For example, three surveys conducted in the same year using differently worded questions yielded very similar estimates of the percentage of consumers who had recently seen their credit reports.[36] Similarly, four surveys conducted within a two-year period found similar percentages of people who say they regularly shred documents containing sensitive financial information.[37]

Consumers cannot be counted on, however, to give completely accurate descriptions of their behavior. In a study conducted by AOL and the National Cyber Security Alliance, consumers tended to overestimate the software programs that protect their computers from viruses, spyware, and hackers.[38] Whereas more than three-quarters of the study participants thought their home computer was very or somewhat safe from online privacy threats, physical examinations of their computers revealed that 67 percent of them did not have current antivirus software, 80 percent had unwanted spyware or adware programs, and 67 percent had no firewall protection. Of

course, antivirus programs, anti-spyware software, and firewalls are somewhat complicated technologies, and consumers may not realize their responsibility for installing and upgrading these features. Still, the results suggest that the self-reported privacy behavior of consumers may not be perfectly accurate, especially with regard to their computers. Assessments of simple behaviors, like opting out of prescreened credit card offers or regularly shredding documents containing sensitive financial information, may be more accurate.

Specific Offline Behaviors

Perhaps offline behavior is less headline-grabbing than online behavior, but several national surveys have addressed consumers' offline privacy management strategies. Leaving aside the survey conducted for this report, there have been nine national surveys since 2000 that measure at least one offline privacy-protection behavior. These surveys, shown in Table 5, are ordered chronologically by the period during which their data were collected. They are coded with a single letter, a–i, in Table 6.

Table 5: National Surveys of Offline Privacy-Protection Behavior

Code	Sponsor	Data Collection	# of Subjects
a	American Society of Newspaper Editors[39]	11/2000	1,005
b	Privacy & American Business[40]	11/2001	1,529
c	AARP[41]	12/02–1/2003	1,500
d	Harris Interactive[42]	1/2004	3,378
e	Privacy & American Business[43]	6/2004	2,136
f	American Express[44]	10–11/2004	1,024
g	Experian[45]	2/2005	,2000+
h	Javelin/Better Business Bureau[46]	9–10/2004	1000+
i	Office Depot[47]	3/2005	1962

Table 6 summarizes the major findings of the nine surveys described in Table 5. The left-hand column on Table 6 shows the five major categories of privacy-protection behavior. The middle column provides examples of commonly offered advice that falls into each of the five categories. The right-hand column presents survey evidence of the extent to which each item of advice is being followed by consumers.

Table 6: Consumer Advice vs. Behavior in Protecting Offline Privacy

Offline Behavior	Common Advice	Behavior: Survey Results
Receiving Information	(1) Pick up incoming mail promptly (2) Sign up for the national do-not-call list	(1) 71% regularly retrieve mail promptly (h) (2) 57% signed up for the do-not-call list (d)
Sending Information	(1) Send mail from secure location (2) Don't give personal information without verification or initiation	(1) 37% always send mail from secure location (i), and 74% do so regularly (h) (2) 70%–87% don't give personal information (a, b, c, e)
Storing Information	(1) Don't carry Social Security number and limit ID cards in wallet or purse (2) Keep financial information at home secure from other people	(1) 51% do not carry Social Security number (f), and 72% limit ID cards (c) (2) 23% keep valuable information locked in file cabinet (i)
Monitoring Information	(1) Annually obtain and verify credit report contents (2) Promptly monitor accuracy of monthly financial statements	(1) 32%–42% have obtained credit report in last year (f, g) (2) 68% regularly review financial statements (c), and 75% reconcile checking accounts monthly (f)
Disposing of Information	(1) Shred or destroy financial documents	(1) 66%–79% destroy credit card receipts, forms, checks, etc. (c, f, h, i)

Based on the survey results shown in Table 6, how do U.S. consumers rate in terms of their likelihood to protect their financial privacy? Two-thirds or more of survey respondents get passing grades when it comes to retrieving their mail promptly, being circumspect about giving out sensitive personal information, regularly reviewing financial statements and reconciling checking accounts, and shredding documents containing sensitive financial information. Perhaps the most disconcerting admission revealed by the survey data is that roughly half of consumers carry their Social Security number in their wallet or on their person. Also, less than half of the respondents examined their credit report in the last year, but this proportion will likely increase as consumers gain free annual access to their reports under the terms of the FACT Act.

*Specific Online Behavior*s

People score very well on some aspects of protecting their offline financial privacy; how do they do in the online environment? The survey data are somewhat richer in this regard. Leaving aside for the moment the 2004 AARP survey commissioned for this report, 10 recent studies provide useful data on the behavior of large and, typically, nationally representative samples of computer users (see Table 7). Whereas studies of offline behavior are usually conducted via telephone surveys, online behavior is sometimes gauged through online surveys[48] and in-home research.[49]

Table 7: National Surveys of Online Privacy-Protection Behavior

Code	Sponsor	Data Collection	# of Subjects
a	Pew Internet & American Life Project[50]	5–6/2000	2,117
b	Privacy Leadership Initiative[51]	11/2001	2,053
c	Privacy & American Business[52]	11/2001	1,529
d	Annenberg Public Policy Center [53]	1–3/2003	1,200
e	PC World Magazine[54]	~7/2003	1,500
f	AOL/National Cyber Security Alliance[55]	9–10/2004	329
g	American Express[56]	10–11/2004	1,024
h	Javelin/Better Business Bureau[57]	9–10/2004	1,000+
i	Office Depot[58]	3/2005	1,962
j	Privacy & American Business[59]	5/2005	2,322

Table 8, which parallels Table 6, compares the most commonly offered pieces of consumer advice on how to protect financial privacy online with available survey data on the extent to which consumers follow this advice.

Table 8: Consumer Advice vs. Behavior in Protecting Online Privacy

Online Behavior	Common Advice	Behavior: Survey Results
Receiving Information	(1) Use a secondary or fake email address to avoid spam (2) Avoid unnecessary cookies	(1) 20% use a secondary email address (a) (2) 15%–25% set computer to reject cookies (b, c, e), and 65% have erased unwanted cookies (d)
Sending Information	(1) Encrypt communications (2) Give minimum personal information (3) Check Web site security policies	(1) 9% send encrypted email (a) (2) 82% refused to give sensitive info to a Web site (b); 67% decided not to register because of complicated or unclear privacy policy (j); and 24%–34% supplied false personal information (a, b) (3) 50%–61% check for Web site security features (c, e, g)
Storing Information	(1) Use a firewall (2) Update antivirus protection (3) Update antispyware protection	(1) 60%–63% claim to have updated firewall (h, i), but computer inspection shows only 33% of all computers and 51% of broadband users had a firewall (f) (2) 33% have up-to-date antivirus software (f) (3) 80% of machines are infected with spyware (f)
Monitoring Information	(1) Read Web site privacy policies (2) Use "strong" passwords and change them regularly	(1) 18%–42% always or frequently read Web site privacy policies (b, e) (2) more than half use passwords with both letters and numbers, but 34% never change their passwords (e); 27% change passwords frequently (i)
Disposing of Information	(1) Properly delete information before disposing of computer	No evidence

In the online context, rarely do a majority of consumers take a given action to guard their online financial privacy. A clear majority of survey respondents report actions designed to stem the flow of their personal information to Web site operators, but people do far less to control the

receipt of information, store it securely, and monitor its use by others. Moreover, some reported behaviors are overstated. Whereas a majority of survey participants claim to have updated firewalls and adequate antivirus and anti-spyware software installed on their home computers, an inspection of their machines revealed that a minority of computers actually had these protections. A study conducted by AOL and the National Cyber Security Alliance in which experts inspected people's home computers, found: (1) 67 percent of all computers had no firewall protection, including half of those with broadband connections; (2) 67 percent of computers did not have current antivirus software (where current is defined as having been updated within the last week), and 15 percent had no antivirus software at all; and (3) 80 percent of computers were infected with spyware or adware, with the average infected computer having 93 spyware/adware components.[60]

The failure to protect online privacy extends beyond high-tech computer software. A slim majority of consumers regularly read Web site security features, and less than half of survey respondents examine Web site privacy policies. People apparently find it difficult to create difficult-to-guess passwords and change these passwords regularly. For most people, just remembering all their passwords is a feat, let alone changing them.[61]

One of the primary ways people protect their online financial privacy (although not a method recommended by experts) is to refrain from making maximum use of the Internet. The biggest casualty is online shopping. Some people have never shopped online because of privacy fears, and others are cutting back on their online purchases. Depending on the survey, between 20 percent and 40 percent of respondents claim they have reduced their online purchases due to fears of their financial privacy being compromised.[62] People also report reducing their use of email, especially choosing not to open attachments or respond to special offers.[63] Withdrawing from the Internet and all that it has to offer may be one strategy for protecting financial privacy, but it is a costly one in terms of forgone benefits

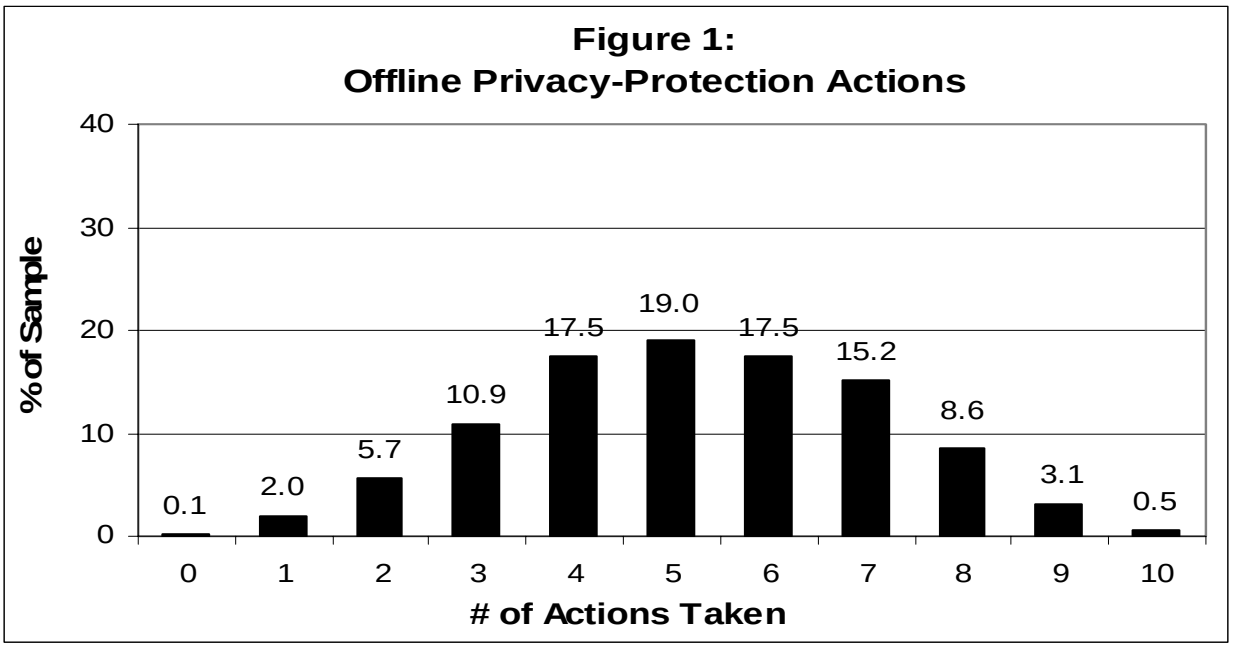
General Patterns of Action

So far we have reviewed national surveys containing one or a few questions about the many offline and online behaviors individuals can take to defend their financial privacy. What "grade" would consumers earn if a single national survey looked simultaneously at a wide variety of privacy behaviors? To answer this question, AARP commissioned a telephone survey in November 2004. The survey work was performed by ICR/International Communications Research of Media, Pennsylvania. The sample of 1,010 people was nationally representative of individuals ages 18 and older. Appendix 3 shows the complete survey questions, including top-line results.

Summary Measure. The 2004 AARP survey contained a single-item question that referred to a person's overall level of these behaviors. The question was: "How would you describe the amount of time and effort, if any, that you devote to protecting your financial privacy?" The responses across all 1,010 respondents were as follows: 14 percent chose the "a lot" answer category; 46 percent chose "a moderate amount"; 31 percent chose "a little"; 8 percent chose "none." These percentages, while plausible, taken on greater meaning when one examines individual actions and clusters of behavior.

Composite Measures. The 2004 AARP survey contains 10 items that can be combined into a simple scale of privacy-protection behaviors *offline*. These items cover all five categories of privacy advice: receiving, sending, storing, monitoring, and disposing of information. The 10 specific privacy protection behaviors are: (1) registering on the national do-not-call list; (2) asking to be removed from a company's marketing list; (3) paying cash to avoid privacy risks of using credit cards; (4) sending mail from a secure location; (5) rejecting store frequent-buyer cards; (6) not carrying a Social Security number in a wallet or purse; (7) regularly changing PINs and passwords on financial accounts; (8) paying to see a copy of a credit report; (9) reading the privacy notices that come from banks and other financial institutions; and (10) shredding documents.

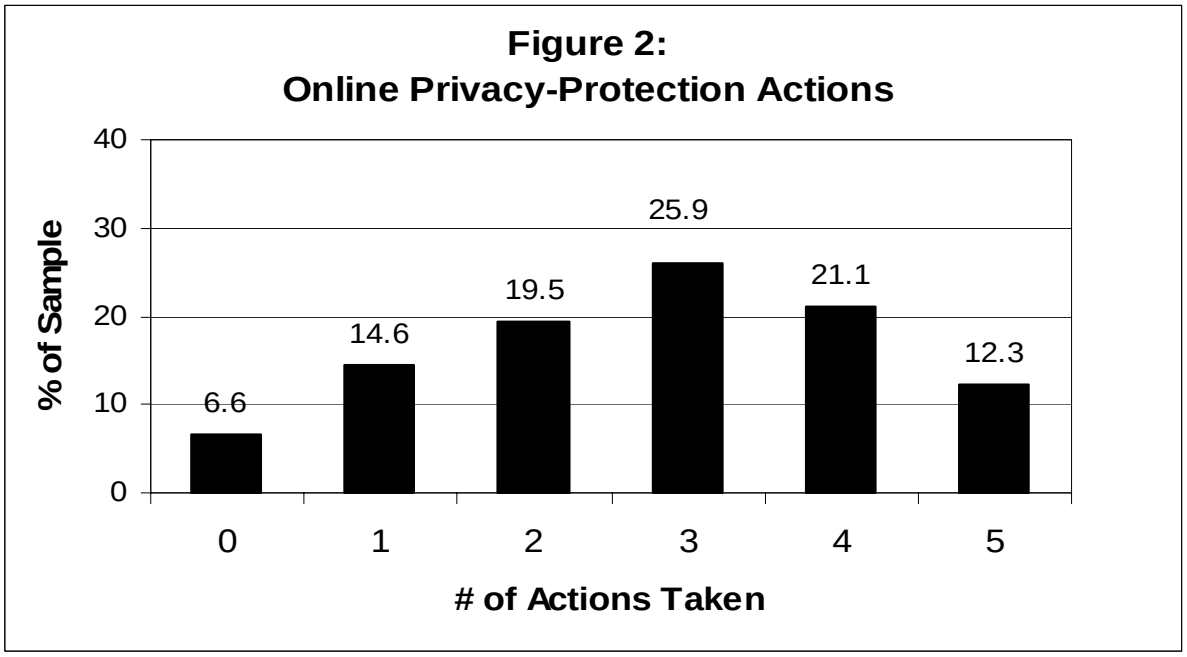
Each of the 10 behaviors was coded into two categories. This was straightforward in the case of yes-or-no questions. For "how often" questions, the four answer categories (never, once in a while, most of the time, always) were collapsed to create two categories as equal in size as possible. Using this approach, each respondent received a score between zero and 10: the higher the score, the greater number of privacy-protection behaviors the person reported doing. If a person couldn't or wouldn't answer any of the 10 questions, he or she was dropped from the analysis, leaving 910 of the original 1,010 participants. The average score across the 910 people for whom complete information was available was 5.24 behaviors, that is, slightly more than half of the 10 possible offline actions. At the extremes, 19 people engaged in zero or one privacy protection behaviors, and 33 people engaged in nine or 10 of these behaviors.



The scale for *online* behavior was created from questions about five behaviors: (1) using a fake or rarely used email address to reduce unwanted communications; (2) using a third party, like PayPal, to secure online payments; (3) checking Web site security policies; (4) checking Web site privacy policies; and (5) regularly updating spyware. The same procedure was used for

constructing a scale of online behaviors designed to guard consumer privacy. One complication, however, stemmed from the fact that some survey respondents did not use the Internet, and of those who did, only some made online purchases. As a result, scores for online privacy protection activities are limited to 450 people for whom complete data existed for all five questions. The average score across these people was 2.77 behaviors, again slightly more than half of the five possible online actions (see figures 1 and 2).

The scores on the two scales correlate well with the general measure of privacy-protection behavior described above. Specifically, the greater the amount of time and effort people said they devoted to protecting their financial privacy, the higher they scored on offline and online scales. For example, people who said they devoted a lot of time and effort to privacy protection scored 6.10 (out of 10) and 3.26 (out of five) on the offline and online scales, on the other hand, , people who reported spending no time and effort on privacy protection scored 3.83 and 1.59, respectively, on the two scales. This correlation between general and specific survey questions adds confidence that the survey questions elicited truthful responses.



Offline vs. Online Behavior. How closely are scores for offline behavior related to scores for online behavior? The only study to investigate this question found no such relationship in a sample of 289 students but did find a connection in a small sample of 26 nonstudents.[64] The AARP data are more consistent with the latter finding: people who score higher on the index of offline privacy tend to score higher on the index of online behaviors. When people are classified into low, medium, or high groups based on their offline or online behavior, one finds that 56 percent of people who are low offline are also low online, and 48 percent of those who are high offline are high online (see Table 9).[65] There are, however, some people whose behavior varies substantially depending on whether the context is offline or online. Twenty-one percent of people who rate low in terms of their offline privacy-protection behavior rate high in their online

behavior; conversely, 29 percent who rate high offline rate low online. Hence, there is considerable consistency across offline and online domains, but there are enough exceptions to suggest that behavior in each domain can be treated separately.

Table 9: Comparison of Offline and Online Protection Behaviors

	Low Offline	**Medium Offline**	**High Offline**	**Totals**
Low Online	56%	45%	29%	(185)
Medium Online	23%	27%	24%	(114)
High Online	21%	28%	48%	(151)
Totals	100% (68)	100% (235)	10% (147)	450

Note: Column percentages may not add up to 100 percent due to rounding error.

Differences Among People. As with any test, some types of people will score higher than others on our quiz of privacy-protection behaviors, but which types? Relatively little is known about the personal characteristics that predispose people to act more or less aggressively in guarding their financial privacy. Perhaps people with high incomes score high because they have greater financial resources to protect than do people with lower incomes. One might also surmise that people with higher levels of education are more knowledgeable about threats to financial privacy and methods of protecting it than are people with lower levels of education. Finally, one might conjecture that older consumers are less comfortable than younger consumers with computers and the Internet and, therefore, feel more compelled to protect themselves from the privacy threats associated with these technologies. Are these speculations corroborated by survey results?

The evidence in previous studies about personal correlates of privacy-protection actions is thin. The most consistent results pertain to differences among income groups. According to a 2004 American Express study, wealthier people are less likely to carry their Social Security number in their wallet or purse, and they are more likely to check a Web site's security features before buying online than are people with lower levels of wealth.[66] When compared to less affluent individuals, wealthier ones are also more likely to reconcile their billing statements each month and less likely to use their Social Security number as an employee or student identifier or to print their Social Security number on their checks or driver's license. Along the same lines, a study conducted by Harris Interactive for Office Depot found that people in the study's highest income bracket ($75,000 or higher) were the most likely of any income group to take a variety of offline and online actions to safeguard their financial privacy.[67] Offline behaviors included shredding credit card offers and/or convenience checks, taking outgoing mail to a secure location, and checking credit reports frequently. Higher-income respondents' most prevalent online behaviors included updating firewall software and changing passwords frequently.

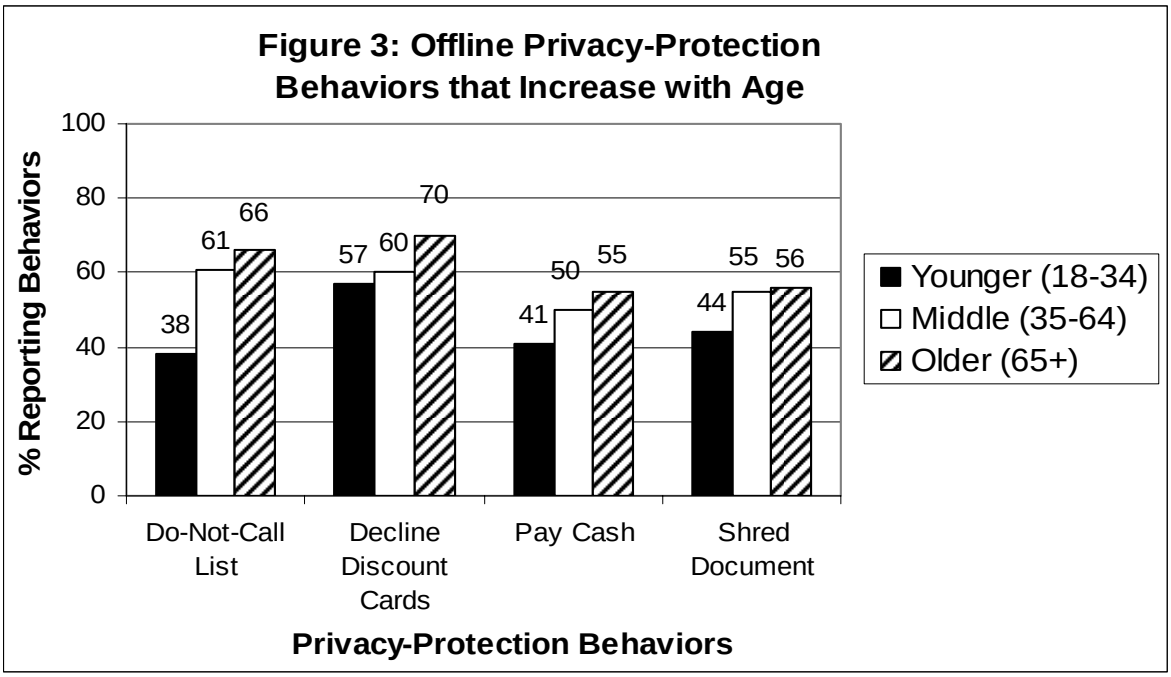
Besides income, the personal characteristic that has drawn the most attention in reporting survey results has been respondent age, and the results have not been clear-cut. The Office Depot study found that people between the ages of 18 and 34 differ from their elders, but their elders do not differ much among themselves. Younger survey participants were less likely to shred credit card

offers and/or convenience checks, more likely to leave outgoing mail unattended, less likely to check credit reports, and less likely to keep copies of important documents. Only with respect to frequently changing passwords did younger respondents report more action to protect financial privacy than older respondents. Based on other surveys, older respondents express more worry about identity theft, and they are more likely to refrain from using the Internet for banking and shopping out of fear for their financial privacy.[68] Here's the strange fact, though. Although older consumers are less likely to shop online, those who do are *less* likely than younger consumers to check to see if Web sites are secure.[69] Adding to the mystery about the relationship between age and privacy protection, a 2002 study conducted for Privacy & American Business reported that middle-aged respondents were more likely than either younger or older ones to check Web site privacy and security policies, and George Milne and his colleagues found that older people engaged in *fewer* online privacy-protection behaviors than did younger people.[70] Perhaps the lower levels of online privacy-oriented behaviors among older people reflect their relative unfamiliarity with how to protect themselves in the online environment.

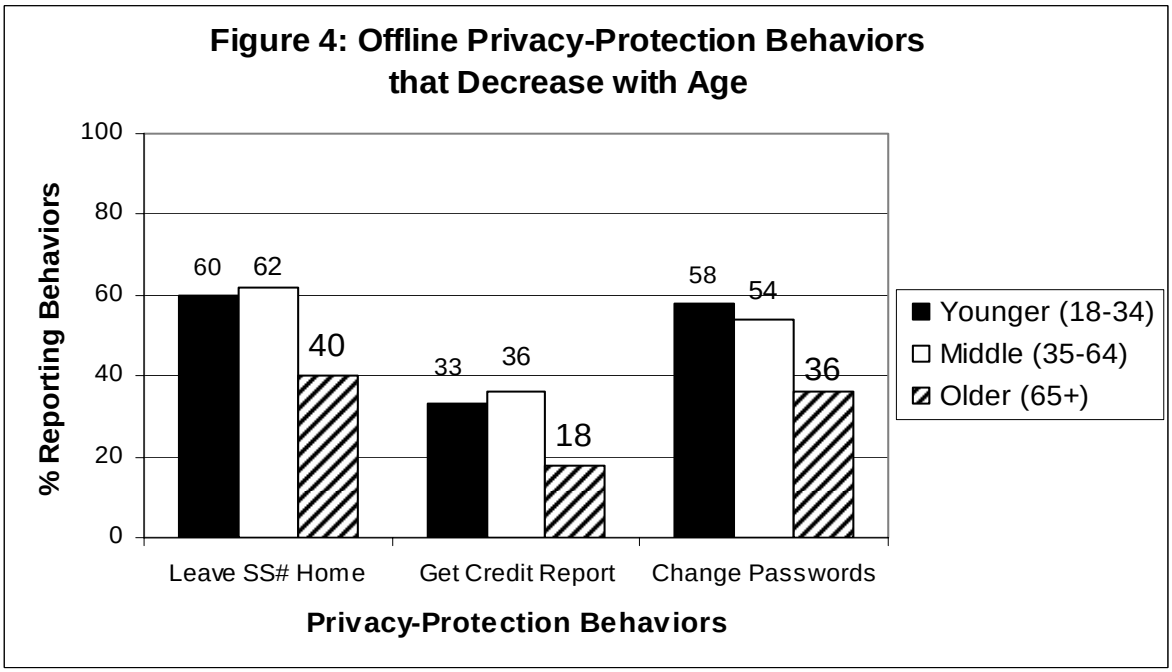
To provide greater insight into the role of socio-economic and demographic characteristics, such as education, income, and age, we probed the data from the 2004 AARP survey. Recall that these data allow us to construct a 10-item measure of offline privacy-protection behavior and a five-item measure of online behavior. With the exception of Milne's 2004 study, all of the demographic results reported above are based on the analysis of single-item behavior measures. Moreover, previous studies have reported simple bivariate relationships, for example, between education and a behavior, but without controlling for the influence of income on both education and behavior. With the 2004 AARP data, we can report multivariate results that allow one to separate the influence of such closely connected characteristics as education and income.

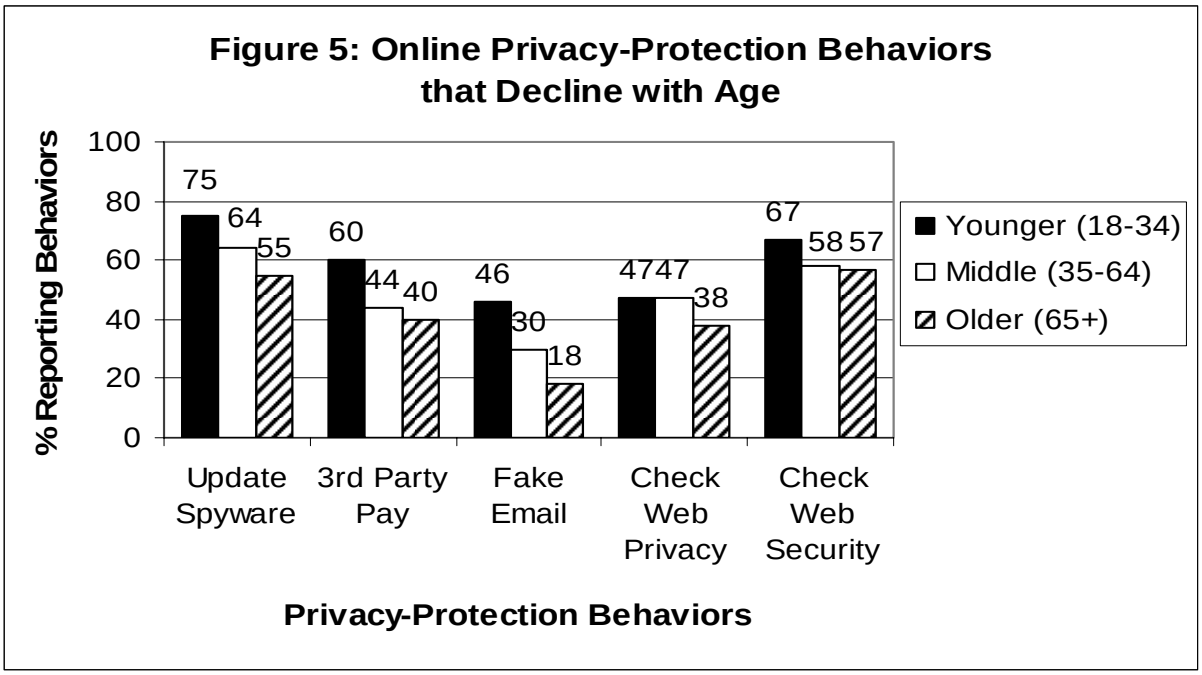
The 2004 AARP data reveal that people with more education or higher household incomes take more actions to guard their financial privacy *offline* than do their counterparts with less education or lower levels of education. Since education and income tend to be correlated, it is important to note that each has an independent, statistically significant effect on behavior, as determined by a regression analysis that predicts behavior while holding constant the effects of multiple personal characteristics.

Whereas a person's age has no apparent connection to the *total* number of actions he or she takes to protect financial privacy offline, a person's age does matter when examining the likelihood of taking some specific offline actions. Figure 3 shows four privacy-protection behaviors in which older consumers are more likely to engage than are younger ones: registering for the do-not-call list, declining frequent-buyer discount cards, paying with cash rather than credit or debit card, and shredding financial documents. Figure 4 shows the opposite tendency, that is, three privacy-protection behaviors that are more appealing to younger people than to older ones: keeping Social Security numbers out of purses and wallets, obtaining a copy of one's credit report, and changing passwords or PINs on financial accounts. (No doubt, older consumers are more likely to carry their Social Security numbers with them because of the controversial use of this number as a Medicare identifier.[71]) For the three remaining offline actions, age differences are not noteworthy.



The pattern for online behavior is quite different. Whereas education and household income have no connection to the number of privacy protection behaviors in which a person engages, a person's age does matter. Specifically, younger people report doing more to guard their online privacy than do older people.[72] Figure 5 shows that, for each of the five online behaviors, the youngest respondents were more likely to protect their privacy than were the older respondents.





At first blush, this pattern seems to contradict surveys in which older respondents express greater concern about privacy in general and online privacy in particular than do younger respondents. The apparent inconsistency may have an explanation, though. Results regarding online privacy-protection behaviors are based on the responses of people who have Internet access and have shopped online at least once. Internet access is nearly universal (95%) among respondents ages 18-34 compared to an access rate of 50% among those 65 years old and older. Similarly, over half (54%) of the respondents in the 18-34 age category had purchased something online from a home computer, whereas only 16% of people in the 65+ age category had done so. As a result, older consumers who have Internet access and make online purchases are not necessarily representative of their age cohort as a whole. Indeed, the survey results suggest that older consumers who use the Internet and engage in ecommerce constitute a special subgroup. Members of this subgroup are not only more risk-tolerant when it comes to financial privacy than their age peers who refrain from online activity; they are also more risk-tolerant than younger people taken as a whole.

Test Summary. We cannot emphasize too strongly that the references to tests, quizzes, scores, and grades have their limits. Most important, one cannot assume that all individuals should take all of the actions that experts recommend for protecting financial privacy. For some individuals, financial privacy is a low priority and the costs of protecting it may outweigh the expected benefits. On the other hand, one can argue that people have a *responsibility*—to their family members, other consumers, and the businesses with which they deal—to take actions that defend their financial privacy. For example, it does little good for a business to invest in a fancy double-password system if consumers fail to take simple steps like safeguarding their passwords, protecting their Social Security numbers, and providing a secure receptacle for incoming mail from the U.S. Postal Service. Thus, it is not too farfetched to think of answers to a privacy test as right or wrong. At the very least, these answers provide a benchmark against which efforts to encourage consumers' self-defense behaviors can be evaluated.

With the limitations and uses of a privacy test in mind, what grade did our national sample of consumers earn? With respect to both offline and online actions, our average respondent scored only slightly above 50 percent. Using 80 percent as a cutoff for a "good grade," we conclude:

- Only 12.2 percent earned such a grade for offline privacy-protection behaviors and 12.3 percent for online behaviors.
- Only about half of those people earning a good grade for offline behavior also earned a good grade for online behavior (see Table 9).
- People with higher levels of income or education were more likely to earn a good grade than were people with lower levels of income or education for offline behavior, but younger people were more likely to earn a good grade than were older people for online behavior.

PART 4: RECOMMENDATIONS AND CONCLUSIONS

As we have noted several times, financial privacy is not such an unmitigated benefit that all consumers should take every conceivable self-protective action. Rather, each individual must decide how much privacy he or she wants based on its perceived benefits and costs. The results of our privacy test suggest that consumers vary to a large degree in their preference for financial privacy. Judging by their actions, many consumers want a high level of financial privacy and are willing to spend time and money to achieve it. Large percentages of consumers are, for example, taking their outgoing mail to secure locations, shredding mail that contains sensitive financial data, updating antispyware software on their computers, and using third-party payment services like PayPal when making online purchases. Conversely, many consumers choose or feel compelled to carry their Social Security number in their wallet or purse and use the same passwords over and over again.

It is tempting to assume, then, that differences in privacy actions perfectly reflect differences in privacy preferences, but such an assumption is likely faulty. People cannot obtain their desired level of financial privacy as easily as they can buy pants that fit properly or order a hamburger that is cooked just right. People may not be knowledgeable about either the threats to their financial privacy or the means of protecting it. We call this the *education challenge*. In addition, there are limits to the effectiveness of individual consumers' self-help action. For example, no amount of shredding of financial documents can prevent a dishonest bank or store employee from stealing a person's financial information. Hence, consumers must have confidence that their personal actions are complemented by those of the other entities involved, especially businesses and government. We call maintaining this confidence the *motivational challenge*.

The Educational Challenge

Properly balancing the benefits and costs of privacy presumes that consumers are knowledgeable about both factors, but it seems unlikely that people are able to estimate in any meaningful way their likelihood of being victimized by identity theft or the benefits of any actions that may reduce that likelihood. General estimates of the number of victims of identity theft are becoming more reliable, but estimating the risk to a particular individual consumer remains elusive. It is also unlikely that people who have experienced identity theft view the crime as the unavoidable cost of all the benefits they receive from having their personal financial information available to other parties. It is more plausible these people view themselves as victims of forces over which they had little control, such as a dishonest employee of a distant company who stole their financial information.

There are also substantial knowledge barriers to consumers protecting their financial privacy online. Computer technology changes so fast that only the most technologically savvy remain unintimidated by all the recommendations directed at consumers about buying, installing, and updating various types of antivirus, antispyware, and antihijacking software. Survey evidence suggests that consumers recognize their lack of knowledge. In a recent national study, only a minority of Internet users described themselves as either "extremely knowledgeable" or "reasonably knowledgeable" about viruses (39 percent), spyware (24 percent), hacking (19 percent), and phishing (16 percent).[73] In a separate survey, 71 percent of respondents said they didn't know or were uncertain of how to tell if a Web site is secure.[74] Whatever level of knowledge people think they possess is probably overstated, as shown by the lack of correlation between the privacy protection features consumer think they have installed and updated on their computers and the protection features they actually have.[75] Software improvements that make it easier for consumers to install and update privacy-protection technologies for their computers would likely narrow this gap.

Multiple constituencies can meet the educational challenge. As the survey conducted for this report showed, consumer advice on financial privacy comes from four major quarters: nonprofit organizations, journalists, business, and government. The first two sources likely enjoy a credibility advantage in communicating information about financial privacy; the second two typically enjoy an advantage in terms of resources. Combining these assets through creative partnerships may be necessary to meet the challenge of educating consumers about the ever-evolving threats to their financial privacy.

The Motivational Challenge

Education is one thing; motivation to use that education is another. All the consumer knowledge in the world about the threats to financial privacy and the actions individuals can take to reduce these threats is of little value without the motivation to use this knowledge. There is a real danger that consumers will lose the motivation to engage in self-protective behavior if they believe that controlling identity theft and other threats to their financial privacy are beyond their control.

Several recent events have given consumers some reason to be feel helpless and fatalistic about their financial privacy. Foremost among these events have been reports of potential information compromises at leading financial institutions. Also undermining consumer motivation to safeguard their financial privacy aggressively are a variety of high-tech and/or stealthy methods of invading financial privacy. These methods feed the perception that it is difficult or even impossible to maintain financial privacy. Online, privacy is threatened by spyware, browser hijacking (in which a user is taken to a different site from the one he or she requested), phishing, and pharming (creation of fictitious Web sites to entice people into providing their personal information). The privacy of a person's telephone calls is increasingly under attack as well. A variety of commercial services sell a list of a person's outgoing phone calls, whether made by cell phone or conventional phone. Sellers of phone records use several techniques to obtain their data, including paying telephone company employees, pretending to be the account holder ("pretexting"), or accessing customer accounts online.[76] Regardless of the method used, a person's phone records can contain a wealth of financial information, including the stores a person patronizes, the travel companies a person uses, and the investment company a person consults. Given these developments, it is perhaps not surprising that a recent survey by the privacy survey conducted by Privacy & American Business in conjunction with Deloitte & Touche found that 78 percent of a national sample agreed with the statement, "consumers have lost all control over how personal information is collected and used by companies."[77]

The keys to maintaining consumer motivation to engage in privacy self-protection activities are making such activities less costly and giving consumers confidence that their actions are complemented by those of business, government, and other handlers of their financial information. Consumers have demonstrated their willingness to take action when the costs to do so are low and the benefits are potentially high. Perhaps the most dramatic example is the speed with which people signed up for the national do-not-call registry, which limits certain types of telephone solicitations. President Bush signed the law in March 2003. In June 2003, the Federal Trade Commission began accepting registrations on the list from consumers; 10 million people registered in the first four days! Before the rule even went into effect in October 2003, consumers had registered more than 50 million phone numbers.[78]

Another example of consumer responsiveness to privacy-enhancing opportunities involves the new right to obtain free copies of one's credit reports. The Federal Trade Commission has not yet released data on the number of people who have exercised their new right. (The right wasn't extended to all U.S. consumers until September 2005.) Despite the problems documented in this report, the number of consumers availing themselves of this new opportunity will reach into the millions.

In contrast, consumer response to the opportunity provided by the Gramm-Leach-Bliley Act of 1999 to opt out of personal information sharing by their financial institutions seems to have been lukewarm. Perhaps consumers are not worried about information sharing by their banks, insurance companies, and investment firms. Equally plausible is that the opt-out right was not implemented well. Consumer advocates argued in a petition addressed to agencies responsible for implementing the new consumer right that the notices used dense, misleading statements and confusing, cumbersome procedures. As a result, consumers were discouraged from opting out.[79] Since 2003 and 2004, federal regulators sought comments on how to improve the privacy notices, and regulators are still conducting research to determine how consumers would respond to restructured notices and more convenient mechanisms for opting out of information sharing by financial institutions. The Fair and Accurate Credit Transactions Act of 2003 enhanced disclosure of the means available to consumers for opting out of receiving prescreened offers for credit and insurance, effective August 1, 2005. Learning from the implementation of the Gramm-Leach-Bliley Act, the Federal Trade Commission has determined that new notices regarding prescreened offers will be "layered," that is, there will be a short and conspicuous notice on the first page of a solicitation with a longer notice elsewhere.

As the above examples show, many consumers respond to opportunities to protect their financial privacy when these opportunities do not cost a lot in time and money. Conversely, opportunities that are unclear or cumbersome are left unfulfilled. Currently, there is a consensus among leading consumer organizations that the next such opportunity should be the right for individuals to freeze their credit reports so the information they contain cannot be given out without the consumer's explicit permission.[80] Several states have already passed laws to this effect, but resistance to national legislation is strong from credit reporting companies, which argue that freezes are inconvenient for consumers and are ineffective.[81]

Giving people the right to freeze their credit reports is one privacy priority of consumer advocates. Another is subjecting data brokers/aggregators to the provisions of the FACT Act, especially with respect to granting consumers access to data on them that have been collected and are intended for sale.[82] Until recent privacy breaches involving data brokers, these financial entities were invisible to most consumers. Given the sensitivity of financial information handled by data brokers, consumers need mechanisms by which to hold them more accountable.

While federal action has a number of advantages in a national marketplace for financial information, it should be noted that the states have often been incubators for privacy legislation. For example, California was the first state to require financial institutions to notify consumers when their personal financial information has been potentially compromised. This requirement has been credited with bringing to light several major breaches of financial information. Other states have passed similar requirements, and the U.S. Congress is considering a national standard for notifying consumers about security lapses.[83] California was also the first state to give consumers the right to decide whether their cell phone number is listed in a wireless 411 directory, and it was one of the first states to pass antispyware legislation. Hence, it is important that state efforts to protect financial privacy not be preempted except in the case of strong federal legislation.

Making it easier for consumers to act in defense of their financial privacy is not the exclusive prerogative of the government. Banks, insurance companies, credit reporting agencies, and other financial institutions can act proactively through self-regulation. For example, a recent study of how companies notify consumers about privacy breaches concluded that consumers are dubious about the honesty and completeness of these notifications.[84] Consumers also believed that financial organizations should provide more customer assistance when breaches occur. The study's author felt it was a mistake when a company informs customers in states where it is required to do so but fails to in states that do not mandate such notification. The study's bottom-line argument for self-regulation was: if you notify customers the right way, they will stay with you.

Maintaining consumer confidence in self-protection requires going beyond making it easier for consumers to take action on their own behalf. Consumer self-help is supported by the knowledge that businesses, government, and other handlers of sensitive financial information are doing their part in protecting financial privacy. Many of these actions involve new methods of authenticating the identity of users when engaged in online banking or electronic commerce; other actions entail bolstering internal security procedures. Their common denominator is often the use of highly complex, secret, and expensive technologies. While it is not generally possible for organizations to truly explain their procedures to customers, these organizations can set up panels of consumer representatives who monitor financial privacy efforts for consumers in general.

The following list summarizes the major recommendations in this section:

- Nonprofit organizations, journalists, business, and government must find ways to reinforce each others' efforts and work in partnership to meet the challenge of educating consumers about the ever-evolving threats to their financial privacy.
- Legislation—whether federal or state—should establish the right of consumers to freeze their credit reports so these cannot be given out without the consumer's explicit permission.
- Data brokers/aggregators should be subject to the provisions of the FACT Act, especially with respect to granting consumers access to data on them that have been collected and are intended for sale.
- Legislation—whether federal or state—should establish the right of consumers to be notified when a potentially serious breach of personal financial data occurs.
- Federal law should not preempt state privacy legislation except in the case of strong federal legislation.
- Instances in which financial service organizations act in advance of legislation or go beyond its requirements should be well publicized.
- Large organizations that handle sensitive financial information should establish consumer panels to represent consumers in the process of upgrading authentication procedures and internal security practices.

In conclusion, consumers have gone a long way in heeding the advice offered by various experts on how to defend personal financial privacy. Of course, consumers could show more restraint in carrying around their Social Security numbers and more persistence in reading the lengthy

privacy disclosures provided by financial institutions under the terms of the Gramm-Leach-Bliley Act, but, on the whole, consumer actions are going beyond vague and costless expressions of concern for their financial privacy. In a few short years, people have learned new habits related to the way they receive, send, and discard mail; the way they access their financial accounts; and the way they operate their computers. They are now in the process of learning another new habit—how to read their credit reports and correct any misinformation they contain. Sixty percent of respondents in the 2004 AARP survey reported spending "a lot" or a "moderate amount" of time and effort protecting their financial privacy, so it appears that consumers are doing their part. Businesses and government bodies must be sure they are doing theirs in educating consumers, developing new privacy protection technologies, and offering credible and well-publicized programs to the public that lower the cost of defending their privacy.

APPENDIX 1: SAMPLE OF FINANCIAL ADVICE SOURCES

GOVERNMENT

1. Consumer.gov (Federal Trade Commission 1)
http://www.consumer.gov/idtheft/protect_againstidt.html#5

2. Federal Trade Commission 2
http://www.consumer.gov/idtheft/5 (online section only)

3. Federal Deposit Insurance Corporation
http://www.fdic.gov/consumers/consumer/news/cnfall04/cvrstry.html

4. Federal Citizen Information Center
http://www.consumeraction.gov/caw_privacy_general_tips.shtml

5. Federal Reserve Board
http://www.bos.frb.org/consumer/identity/idtheft.htm#resources

6. U.S. Postal Service
http://www.usps.com/postalinspectors/idthft_ncpw.htm

7. State of California Privacy Protection Office
http://www.privacy.ca.gov/sheets/cis1english.pdf

8. State of Wisconsin Extension Service
http://www.uwex.edu/news/story.cfm/475

9. National Association of Insurance Commissioners
http://www.naic.org/privacy/privacy_and_the_consumer.htm

PRIVACY ADVOCATES AND OTHER NONPROFIT ORGANIZATIONS

10. Privacy Rights Clearinghouse
http://www.privacyrights.org/fs/fs17-it.htm#reduce

11. Consumers Union
http://www.consumerreports.org/main/content/display_report.jsp?FOLDER%3C%3Efolder_id=348215&ASSORTMENT%3C%3East_id=333153&bmUID=1103488734473#

12. National Consumers League
http://nclnet.org/privacy/idtheft/getsecure.htm

13. Consumer Action
http://www.consumer-action.org/English/library/privacy_rights/2002_BACEF_leaveMeAlone/index.php

14. Identity Theft Resource Center

http://www.idtheftcenter.org/preventiontips.shtml#test

15. ConsumerPrivacyGuide.org
http://www.consumerprivacyguide.org/topthings/

16. Better Business Bureau
http://www.bbb.org/alerts/article.asp?ID=196

FINANCIAL JOURNALISTS/BOOK AUTHORS
17. *PC World*
http://www.pcworld.com/howto/article/0,aid,112468,00.asp

18. Motley Fool
http://www.fool.com/ccc/check/check06.htm

19. MSN Money
http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P33715.asp

20. CBS News
http://www.cbsnews.com/stories/2001/03/23/earlyshow/saturday/main281280.shtml

21. Yahoo Finance
http://loan.yahoo.com/c/privacy4.html

22. CNN Money
http://money.cnn.com/2002/11/26/pf/saving/q_identity/

23. Gertler Book
http://www.argospress.com/Resources/information-security/book-0375720936.htm

FINANCIAL SERVICES AND OTHER FOR-PROFITS
24. Equifax
https://www.econsumer.equifax.com/consumer/sitepage.ehtml?forward=elearning_idtheft2

25. American Express
http://home3.americanexpress.com/corp/cr/fraud/protect_identity.asp

26. American Bankers Association
http://www.aba.com/Consumer+Connection/CNC_contips_idtheft.htm

27. Travelers Insurance
https://apps.travelers.com/iwcm/Travelers_PL/Documents/trav_idtheft4.pdf

28. Quicken
http://www.quicken.com/cms/viewers/article/banking/39420

29. Bankrate.com
http://www.bankrate.com/brm/news/advice/20030124b.asp

30. Microsoft
http://www.microsoft.com/athome/security/protect/default.aspx

31. Qwest
http://www.qwest.com/about/protection/pdfs/TeenIdentityTheftTipSheet.pdf

32. Getnetwise.org
http://security.getnetwise.org/tips/

APPENDIX 2: PRIVACY QUIZZES

1. ***PC World*** [85]
WHAT'S YOUR PRIVACY QUOTIENT?

You may be aware of online privacy pitfalls, but how well are you guarding yourself against them? Take this abbreviated version of our survey to find out.

1. (a) How many of your Internal accounts (for e-mail, chat rooms, banking sites, and so on) require passwords? (b) How many unique passwords do you have in total?

2. How often do you change your most commonly used password(s)? (Choose one answer.)
- A. More often than once a month
- B. About once a month
- C. About four times a year
- D. About twice a year
- E. Once a year or longer
- F. Never

3 Which of the following choices describe the passwords you use? (Choose all that apply.)
- A. Important date or birthday
- B. Name of person or pet you know
- C. Mother's maiden name
- D. Personal interest (hobby, TV, or movie title; favorite food or drink)
- E. Random word that can be found in the dictionary
- F. Combination of letters and numbers
- G. Other

4 How do you track your passwords? (Choose all that apply.)
- A. Write them down on paper—for example, in a datebook or journal
- B. Write them on sticky notes
- C. Store them in password manager software on a PC
- D. Store them in password manager software on a PDA
- E. Store them in a spreadsheet or a text file
- F. Store them on removable media or USB drive
- G. Memorize them
- H. Tape them to keyboard, drawer, or desk
- I. I don't keep track of passwords
- J. Allow browser Or Windows to save them

5 Which computer-related activities have you done in the past year? (Choose all that apply.)
- A. Posted messages to Usenet groups
- B. Used chat rooms
- C. Sent and received e-mall
- D. Shopped or made travel plans online
- E. Banked online

F. Conducted Web research
G. Used instant messaging
H. Applied for credit card or loan online
I. Paid bills online
J. Responded to spammers to complain or unsubscribe
K. Purchased goods or services advertised through spare
L. Filed your income tax online
M. Posted your résumé on a job site
N. Played online games
O. Swapped flies using a file sharing service
P. Other

6 Typically, how often do you read most or all of the privacy policy of a Web site or online service when you sign up? (Choose one.)

A. Always
B. Frequently
C. Sometimes
D. Rarely
E. Never

7. How do you usually respond if you dislike a site's privacy policy? (Choose one.)

A. Provide the site with valid information
B. Provide the site with valid information. but complain to the company
C. Provide the site with false information
D. Provide the site with false information, and complain to the company
E. Decline to use the site
F. Decline to use the site and complain to the company

8 Which of the following activities do you regularly perform on your PC(s) at work or home? (Choose all that apply.)

A. Install patches for applications
B. Install security patches for OS
C. Delete stored cookies
D. Clear Web browser history
E. Delete Web browser cache/temp files
F. Update virus definition files
G. Run an adware removal program like Ad-aware or Spybot Search & Destroy
H. Run antivirus software
I. Use a firewall
J. Encrypt files stored on hard drive
K. Encrypt e-mail
L. Report security problems to ISP

Your key to the quiz: Question 1: Divide the number of passwords (a) by the number of accounts (b), and multiply by 20. Choices over 100 for either answer count as 100 for scoring.

Award points for each answer as follows: Q2: a: 10; b: 8; c: 5; d: 3; e: 1; f: -5. Q3: a, b: -1; C: -3; d, e: -2; f: 10; g; 1. Q4: a: -5; b, h: -10; c, d, g: 8; e: -2; f: 2; I: 0; J: -1. Q5: a, h: -5; b, d, j: -2; c, i, I, p: 0; e: -3; f, g, n: -1; k, m, o: -10. Q6: a: 10; b: 7; c: 5; d: 4; e: 0. Q7: a: -5; b: -1; c: 0; d, e: 2; f: 5. Q8: a, b, f. l: 5; c, d, e: 2; g: 7; h, i, J, k: 10.

Total your points, add 75, and then divide by 2 to get your Privacy Quotient.

1. 25: YOU'RE AT RISK: Your personal information could be open to marketers, hackers, and other snoops. Consider tightening up your handling of passwords and improving your PC's security system.
2. 50: YOU'VE COVERED THE BASICS: You've taken some steps to guard yourself, but there are still holes in your defenses.
3. 75: YOU'RE CAUTIOUS: You're practicing many of the most important strategies for protecting your information, hut there's still room for improvement.
4. 100: YOU'RE A CLOSED BOOK: You're very cautious about what you reveal online, and today that's a good thing.

2. **Privacy Rights Clearinghouse (2004)[86]**

Identity Theft IQ Test
Are You at Risk for Identity Theft? Test Your "Identity Quotient"

1. I receive several offers of pre-approved credit every week. (5 points)

2. Add 5 points if you do not shred them before putting them in the trash.

3. I carry my Social Security card in my wallet. (10 points)

4. My state driver's license has my SSN printed on it, and I have not contacted the Department of Motor Vehicles to request a different number. (10 points)

5. I do not have a PO Box or a locked, secured mailbox. (5 points)

6. I use an unlocked, open box at work or at my home to drop off my outgoing mail. (10 points)

7. I carry my military ID in my wallet at all times. (10 points)

8. I do not shred or tear banking and credit information when I throw it in the trash. (10 points)

9. I provide my Social Security number (SSN) whenever asked, without asking questions as to how that information will be safeguarded. (10 points)

10. Add 5 points if you provide it orally without checking to see who might be listening.

11. I am required to use my SSN at work as an employee ID or at college as a student ID number. (5 points)

12. My SSN is printed on my employee badge that I wear at work or in public. Or it is posted on my time card in full view of others, or is on other documents frequently seen by many others in my workplace. (10 points)

13. I have my SSN and/or driver's license number printed on my personal checks. (10 points)

14. I am listed in a "Who's Who" guide. (5 points)

15. I carry my insurance card in my wallet and either my SSN or that of my spouse is the ID number. (10 points)

16. I have not ordered a copy of my credit reports for at least 2 years. (20 points)

17. I do not believe that people would root around in my trash looking for credit or financial information or looking for documents containing my SSN. (10 points)

Each one of these questions represents a possible avenue for an identity thief.

Understanding Your Score:

100+ points—Recent surveys indicate that 7–10 million people were victims of ID theft last year. You are at high risk. We recommend you purchase a paper shredder, become more security-aware in document handling, and start to question why people need your personal data.

50–100 points—Your odds of being victimized are about average. Higher if you have good credit.

0–50 points—Congratulations. You have a high "IQ." Keep up the good work and don't let your guard down now.

3. **Wachovia Identity Theft Quiz**[87]

Personal Information

1. Do you carry with you your Social Security car, a Military ID, or any other form of ID that bears your Social Security number?

2. Do you carry anyone else's Social Security number with you?

3. Is your Social Security number used for identity purposes by your employer, school, medical practice, health club, or any other organization?

4. Is your Social Security number printed on your employee/student ID badge?

5. If your Social Security number is printed on your employee/student ID, do you wear it in public?

6. Is your Social Security number or your driver's license number printed on your personal checks or displayed on any professional, vocational, or hobby license?

7. When asked to provide your Social Security number, do you ask how the information will be used and how it will be protected?

8. Have you provided your Social Security number verbally without checking to see who might be listening?

9. Are you now or have you ever been listed in a professional directory (including a "Who's Who" guide)?

10. Does your employer perform pre-employment background checks and limit access to areas containing sensitive information?

11. Have you ever given out personal (non-public) information to someone conducting a phone survey?

12. Have you ordered your credit report in the past year?

13. Do you currently subscribe to a credit reporting service that will notify you or any changes on your credit report?

Physical Environment

1. Do you use an unlocked mailbox at work or at home to receive or send out personal mail?

2. Have you ever donated or disposed of a personal computer, Personal Digital Assistant (PDA) or cell phone without destroying your hard drive/memory chip?

3. Do you receive mail offers of pre-approved credit on a frequent basis?

4. Do you shred unwanted offers before placing them in the trash?

5. Do you shred your financial information before disposing of it?

6. Do you keep important financial information (account numbers, Personal Identification Numbers, expiration dates, customer service phone numbers) near your phone, computer, checks or credit cards in an unsecured location?

7. Do you live in one of the following high-risk states: Arizona, California, Florida, New York, Texas, or Washington, DC?

8. Do you believe that credit or financial information is or has been accessible from your trash?

9. Has your home ever been burglarized?

10. Do you keep your checkbook and bank documents in a secure place where they are not accessible to guests, contractors, service representatives and the like?

11. When you receive a credit card, Check Card, or ATM receipt, do you securely store it for your records, if appropriate, or promptly destroy it, if not?

12. Do you review bank statements promptly and report any discrepancies or suspicious transactions immediately?

13. Do you immediately inform the appropriate financial institution when you discover a lost or stolen check or a missing Check Card, ATM card or credit card?

Online Environment

1. Do you install and frequently update anti-virus protection software on your computer?

2. Do you have firewall protection on your computer?

3. Do you know how to identify a secure Web site?

4. Do you ever share your Username and Password with anyone?

5. Do you open email attachments or links regardless of whom it is from?

6. Do you use public computers to access confidential information?

7. Do you always remember to logout of online sessions that require a password or login process?

8. Do you use online banking and online bill payment?

9. Do you subscribe to any type of balance alert service from your financial institution?

10. Do you have adware/spyware detection software on your computer, either as a standalone program or within an anti-virus program?

11. Do you regularly patch your computer's operating system, browser, and other programs (Microsoft Office, Yahoo, MSN, etc.)? A patch is an update that fixes bugs, adds news features, or closes security holes in software programs.

12. Do you use any service or program that blocks unsolicited email (spam)?

13. Do you change your password on a regular basis (every 30 to 60 days) and use passwords that are difficult for someone else to guess?

EXCEL Job #D8844

53 West Baltimore Pike
Media, Pennsylvania 19063-5698

INTERNATIONAL COMMUNICATIONS RESEARCH

AARP CREDIT EXCEL
November 3–7, 2004

The AARP Credit Excel was conducted by telephone from November 3 to 7, 2004, among a nationally representative sample of 1,010 respondents age 18 and older. All fieldwork by ICR/International Communications Research of Media, PA.

CR-1. Please state whether you strongly agree, somewhat agree, somewhat disagree, or strongly disagree with the following statements (INSERT ITEM)?

a. I know how to prevent telemarketers from calling my home.

	AGREE			DISAGREE			Don't know	Refused
	NET	Strongly	Somewhat	NET	Somewhat	Strongly		
11/7/04	59	38	21	38	13	25	2	*

b. I know what identity theft is and how it occurs.

	AGREE			DISAGREE			Don't know	Refused
	NET	Strongly	Somewhat	NET	Somewhat	Strongly		
11/7/04	88	64	24	10	4	6	2	--

c. I understand how to pay for something online safely and securely.

	AGREE			DISAGREE			Don't know	Refused
	NET	Strongly	Somewhat	NET	Somewhat	Strongly		
11/7/04	66	44	22	28	7	20	5	1

d. I often worry about what will happen to my credit card number when I use it at restaurants, over the phone, or on the Internet.

	AGREE			DISAGREE			Don't know	Refused
	NET	Strongly	Somewhat	NET	Somewhat	Strongly		
11/7/04	63	35	28	31	14	16	5	1

e. I am not annoyed when a company uses personal information they have collected about me one time to sell me products or services another time.

	AGREE			DISAGREE			Don't know	Refused
	NET	Strongly	Somewhat	NET	Somewhat	Strongly		
11/7/04	27	15	12	72	13	59	1	*

f. I am quite concerned about identity theft happening to me.

	AGREE			DISAGREE			Don't know	Refused
	NET	Strongly	Somewhat	NET	Somewhat	Strongly		
11/7/04	71	43	27	28	16	12	1	*

CR-2. Are you currently signed up for the national do-not-call list, the government registry of phone numbers that telemarketers are not supposed to call under most circumstances?

	Yes	No	Don't know	Refused
11/7/04	45	49	6	*

CR-3. Do you currently have a computer at home with Internet access?

	Yes	No	Don't know	Refused
11/7/04	67	33	--	*

(Asked of those who do not have a computer at home with Internet access; n = 305)

CR-4. Do you currently have access to a computer with Internet access somewhere other than home?

	Yes	No	Don't know	Refused
11/7/04	51	49	1	--

CR-3/CR-4 Combination Table #1
Base = Total Respondents

	Have Internet access at home	DO NOT HAVE INTERNET ACCESS AT HOME			Don't know	Refused
		NET	Have elsewhere	Do not have elsewhere		
11/7/04	67	33	16	16	--	*

CR-3/CR-4 Combination Table #2
Base = Total Respondents

	HAVE INTERNET ACCESS			Do not have Internet access	Don't know/ Refused
	NET	Home	Elsewhere		
11/7/04	84	67	16	16	*

CR-5. Do you currently own a machine at home that shreds documents?

	Yes	No	Don't know	Refused
11/7/04	43	57	--	*

CR-6. Do you currently subscribe to an identity theft protection service or carry identity theft insurance?

	Yes	No	Don't know	Refused
11/7/04	12	86	2	*

CR-7. Do you currently have any cards in your wallet or purse that show your Social Security number?

	Yes	No	Don't know	Refused
11/7/04	43	56	*	*

CR-8. Have you ever paid a credit bureau to see a report of your credit history?

	Yes	No	Don't know	Refused
11/7/04	33	66	*	*

CR-9. Have you ever asked a company to take your name off its mailing or phone list?

	Yes	No	Don't know	Refused
11/7/04	64	35	1	--

(Asked of those who have Internet access at home; n = 703)

CR-10. Have you ever visited a music file-sharing Web site like Napster, Gnutella, Kazaa, or Morpheus from your home computer?

	Yes	No	Don't know	Refused
11/7/04	23	77	*	--

Total Respondents

	Yes	No	Do not have Internet access at home	Don't know	Refused
11/7/04	15	52	33	*	--

(Asked of those who have Internet access at home; n = 703)

CR-11. Have you ever added or updated any software that detects or eliminates "spyware" on your home computer

IF NECESSARY: Spyware is software that tracks your computer use and reports it to others.

	Yes	No	Don't know	Refused
11/7/04	59	37	4	--

Total Respondents

	Yes	No	Do not have Internet access at home	Don't know	Refused
11/7/04	40	25	33	3	--

(Asked of those who have Internet access at home; n = 703)

CR-12. Have you ever purchased something from an Internet Web site?

	Yes	No	Don't know	Refused
11/7/04	68	32	--	*

Total Respondents

	Yes	No	Do not have Internet access at home	Don't know	Refused
11/7/04	46	22	33	--	*

(Asked of those who have Internet access at home and have purchased something from an Internet Web site; n = 514)

CR-13. Have you ever used a third-party payment service like PayPal that makes your online payment anonymous?

	Yes	No	Don't know	Refused
11/7/04	46	53	1	--

CR-3/CR-12/CR-13 Combination Table
Base = Total Respondents

	11/7/04
Have Internet access at home (net)	67
Have purchased something online (sub net)	46
Have used third-party payment	21
Have not used third-party payment	24
Have not purchased something online	22
Do not have Internet access at home	33
Don't know	--
Refused	*

CR-14. During the last five years, has anyone misused your EXISTING credit card or checking account to place charges or obtain funds without your permission?

	Yes	No	Don't know	Refused
11/7/04	14	86	*	*

CR-15. During the last five years, has someone used your personal information without your permission to obtain NEW credit cards or loans in your name or open other new accounts in your name?

	Yes	No	Don't know	Refused
11/7/04	5	94	*	*

(Item G& H asked of those with Internet access; n = 862)
(Item I asked of those who have purchased something online; n = 514)

CR-16. The following list contains activities that some people do to guard their financial privacy. Please tell me if you never do these, do these once in a while, do these most of the time, or always do these. How often do you (INSERT ITEM)? (READ LIST)

a. Read the privacy notices that come in the mail from banks, insurance companies, credit card companies, and other financial institutions?

		EVER				Don't know	
	Never	NET	Once in a while	Most of the time	Always		Refused
11/7/04	24	75	30	19	26	1	--

b. Send your important outgoing mail from a safe location like a post office or locked mail box?

		EVER				Don't know	
	Never	NET	Once in a while	Most of the time	Always		Refused
11/7/04	23	77	14	13	49	*	*

c. Accept offers to sign up for frequent-buyer discount cards, such as those offered by grocery stores and gas stations?

		EVER				Don't know	
	Never	NET	Once in a while	Most of the time	Always		Refused
11/7/04	64	36	29	4	3	*	--

d. Change the passwords or PINs on your financial accounts, such as credit cards or bank accounts?

		EVER				Don't know	
	Never	NET	Once in a while	Most of the time	Always		Refused
11/7/04	49	49	32	8	9	1	1

e. Choose to pay a restaurant bill with cash rather than a debit or credit card because you are worried that your card information may be misused?

		EVER				Don't know	
	Never	NET	Once in a while	Most of the time	Always		Refused
11/7/04	48	50	20	6	24	1	1

f. Shred financial documents before you throw them in the trash?

		EVER				Don't know	
	Never	NET	Once in a while	Most of the time	Always		Refused
11/7/04	26	73	9	13	51	1	*

g. Check the privacy policy of a Web site before providing personal information like your email address or phone number?

		EVER				Don't know	
	Never	NET	Once in a while	Most of the time	Always		Refused
11/7/04	32	66	24	13	29	1	1

h. Give a fake or rarely used email address to Internet sites you don't want recontacting you?

		EVER				Don't know	
	Never	NET	Once in a while	Most of the time	Always		Refused
11/7/04	68	31	13	5	12	1	*

i. Check the security features of a Web site before making an online payment

		EVER				Don't know	
	Never	NET	Once in a while	Most of the time	Always		Refused

11/7/04	22	77	16	20	41	1	*

CR-17. How would you describe the amount of time and effort, if any, that you devote to protecting your financial privacy?

	ANY TIME/EFFORT				No time/effort	Don't know	Refused
	NET	A lot	Moderate	A little			
11/7/04	91	14	46	31	8	1	--

ENDNOTES

[1] Landesberg, Martha K., Toby Milgrom Levin, Caroline G. Curtin, and Ori Lev. 1998. *Privacy Online: A Report to Congress*. Washington, DC: Federal Trade Commission, June.

[2] Warren, Samuel and Louis Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4(5):193–220.

[3] Synovate. 2003. *Identity Theft Survey Report*. Washington, DC: Federal Trade Commission, September.

[4] Foley, Linda, and Jay Foley. 2003. *Identity Theft: The Aftermath 2003*. San Diego, CA: Identity Theft Resource Center

[5] Walters, Neal. 2005. "Gone Phishing: The Internet and Identity Theft." AARP Public Policy Institute Research Report, June. Available at http://www.aarp.org/research/frauds-scams/fraud/fs118_phish.html

[6] Keizer, Gregg. 2004, "Phishing: You Ain't Seen Nothing Yet." *TechWeb News*, December 7.

[7] Anti-Phishing Working Group. 2005. "Phishing Activity Trends Report for April 2004." Available at http://antiphishing.org/APWG_Phishing_Activity_Report_April_2005.pdf

[8] TRUSTe. 2004. "U.S. Consumer Loss of Phishing Fraud to Reach $500 Million." Press release, September 29.

[9] Hall, Mark A., Jean McEwen, James Barton, Ann P. Walker, Edmund G. Howe, Jacob A. Reiss, Tara E. Power, Shellie D. Ellis, Diane C. Tucker, Barbara W. Harrison, Gorden D. McLaren, Andrea Ruggiero, and Elizabeth J. Thomson. 2005. "Concerns in a Primary Care Population about Genetic Discrimination by Insurers, *Genetics in Medicine* 7(5):311–316.

[10] Odlyzko, Andrew. 2003. "Privacy, Economics and Price Discrimination on the Internet." Minneapolis, MN: University of Minnesota Digital Technology Center, July 27; Odlyzko, Andrew. 2004. "The Evolution of Price Discrimination in Transportation and Its Implications for the Internet." *Review of Network Economics* 3(3); Turow, Joseph, Lauren Feldman, and Kimberly Meltzer. 2005. *Open to Exploitation: American Shoppers Online and Offline*. Philadelphia, PA: Annenberg Public Policy Center of the University of Pennsylvania.

[11] Sprenger, Polly. 1999. "Sun on Privacy: 'Get Over It,'" *Wired News*, January 26. Available at http://www.wired.com/news/politics/0,1283,17538,00.html

[12] Hann, Il-Horn, Kai-Lung Hui, Tom S. Lee, and Ivan P. L. Png. 2003. "The Value of Online Information Privacy: An Empirical Investigation." Washington, DC: AEI-Brookings Joint Center for Regulatory Studies.

[13] Wuorio, Jeff., Undated. "Protect Your Privacy: 10 Simple Steps." *MSN Money*. Available at http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P33715.asp

[14] Arthur, Dani. 2002. "5 must-know tips for protecting your identity." bankrate.com. Available at http://www.bankrate.com/brm/news/cc/20020612a.asp, last updated August 5, 2004.

[15] Electronic Privacy Information Center. 2004. "EPIC New Year Resolutions." Available at http://www.epic.org/privacy/2004tips.html

[16] Abagnale, Frank W. 2003. "14 Tips to Avoid Identity Theft." bankrate.com. Available at http://www.bankrate.com/brm/news/advice/20030124b.asp

[17] Gertler, Eric J. 2004. *Prying Eyes*. New York: Random House.

[18] Arata, Michael J. 2004. *Preventing Identity Theft For Dummies*. Hoboken, NJ: John Wiley & Sons; Hammond, Robert. 2003. *Identity Theft: How to Protect Your Most Valuable Asset*. Franklin Lakes, NJ: Career Press.

[19] The emphasis is on the word potentially. Research by Mary J. Culnan and George R. Milne has shown how difficult it can be for consumers to exercise their rights under laws such as the Gramm-Leach-Bliley Act. See, for example, "The Culnan-Milne Survey on Consumers & Online Privacy Notices: Summary of Responses." Washington DC: FTC, December 2001, and Milne, George R. and Mary J. Culnan. 2004. "Strategies for Reducing Online Privacy Risks: Why Consumers Read (Or don't read)Online Privacy Notices." *Journal of Interactive Marketing* 18(3), 15–29.

[20] Conference Board. 2005. "Identity Theft and Online Security Worries Are Causing Changes in How People Use the Internet." Consumer Internet Barometer press release. New York, NY, June 23; First Data. 2005. "New Identity Theft Survey Reveals Latest Count of Victims, Need for Greater Protection; First Data and Regions Team to Fight Back." Press release, May 17. Available at http://news.firstdata.com/media/ReleaseDetail.cfm?ReleaseID=163659; Foley and Jay Foley, 2003, op. cit.; Phan, Don. 2005. *2005 Identity Fraud Survey Report*. Pleasanton, CA: Javelin Strategy & Research; U.S. Government Accountability Office. 2002. *Identity Theft: Prevalence and Cost Appear to Be Growing*. Washington, DC: GAO.

[21] "Shredders Can Foil ID Thieves." 2003. *Consumer Reports* 68(10):15.

[22] Identity Theft 911 Secure Locking Mailboxes. 2005. Available at http://www.identitytheft911.biz/securemailbox.html

[23] Cullen, Terri. 2005. "A Cottage Industry Blooms to Help Victims of ID Theft," *Wall Street Journal*, April 21, p. D1; Mohl, Bruce. 2005. "Providers Push Insurance Covering Theft of Identity." *Boston Globe*, February 6, p. C1; Simons, David. 2003. "ID Theft Insurance Isn't Insurance." *Forbes*, May 29, 2003.

[24] Lincoln Spector. 2003. "Extra-Suite Virus and Spam Protection." *PC World*, November; Rubenking, Neil J. 2004. "ZoneAlarm Security Suite 5.5" *PC Magazine*, December 8.

[25] U.S. Government Accountability Office. 2005. *Credit Reporting Literacy: Consumers Understood the Basics but Could Benefit from Targeted Educational Efforts*. Report 05-223. Washington, DC: GAO.

[26] Hoofnagle, Chris Jay, Norma Garcia, Edmund Mierzwinski, Beth Givens, Evan Hendricks, and Brad Scriber. 2004. *Free Annual Credit Report Site Is Block Web Links*. Letter to Federal Trade Commission, December 7.

[27] Dixon, Pam. 2005. *Call Don't Click: Why It's Smarter to Order Federally Mandated Credit Reports via the Telephone, Not the Internet*. World Privacy Forum, February 24. Available at http://www.worldprivacyforum.org/pdf/wpf_calldontclick_study_2005.pdf

[28]Dixon, Pam. 2005. *Call Don't Click Update*. World Privacy Forum. July 14. Available at http://www.worldprivacyforum.org/pdf/wpfcalldontclickpt2_7142005.pdf

[29] Zimmermann, Stephanie. 2005. "Credit Reports Can Be a Hassle to Acquire." *Chicago Sun-Times*, March 7, p. 4.

[30] Mitchell, Lesley. 2005. "It's Free to Get Credit Report, Not Always Easy." *Salt Lake Tribune*, May 14, p. B1

[31] Kandra, Anne, and Andrew Brandt. 2003. "The Great American Privacy Makeover," *PC World* 21(11):144–161; Privacy Rights Clearinghouse. 2004. "Identity Theft IQ Test." Available at http://www.privacyrights.org/itrc-quiz1.htm; Wachovia. 2005. "Identity Theft Quiz." Available at http://www.wachovia.com/misc/0,,799,00.html

[32] Westin, Alan F. 2004. "Consumer Activism on Privacy." *Privacy & American Business Newsletter* 11(5):1–6.

[33] Dingboom, Teresa. 2004. Results of Dittus Communications Spyware Survey Conducted by Ipsos-Public Affairs, September 22; Kandra and Brandt, 2003, op. cit.; Phoenix Marketing International. 2005. "Identity Theft Is a Major Concern for Affluent Households." Press release, July 26; Privacy & American Business. 2005. "New Survey Reports an Increase in ID Theft and Decrease in Consumer Confidence." Press release, June 29; R R. Donnelley. 2003. "Survey Confirms that 70% of Consumers Are Privacy Seekers." News release, August 20; Roberts, Paul. 2004. "Gartner: Consumers Dissatisfied with Online Security' *PC World*, December 6; TRUSTe. 2004. "Study Reveals Over Half of Consumers Chilling to Online Holiday Shopping Due to Identity and Credit Card Theft." Press release, San Francisco, November 23.

[34] Goldman, Eric. 2002. "The Privacy Hoax," *Forbes*, October 14, p. 42; Information Policy Institute. 2003. "Privacy Survey Report Card," October 15; Sheehan, Kim Bartel. 2004. "How Public Opinion Polls Define and Circumscribe Online Privacy." *First Monday* 9(7).

[35] Milne, George R. 2003. "How Well Do Consumers Protect Themselves from Identity Theft?" *Journal of Consumer Affairs* 37(2):388–402.

[36] AARP. 2004. "Credit Survey Conducted by International Communications Research, November 3–7"; American Express. 2004. "Consumers Report Strong Support of Increased ID Theft Precautions When Making Purchases, Reveals New American Express Survey." Press release, November 18; Experian. 2005. "Americans Feel More Confident about Their Future Financial Health Compared to their Current Situation." *Monthly Report of the Experian-Gallup Personal Credit Index*, March. Available at http://www.nationalscoreindex.com/Gallup_Archive_Content.aspx?id=1

[37] AARP, 2004, op. cit.; American Express, 2004, op. cit.; Office Depot. 2005. "New Information Protection Survey from Office Depot Reveals Many Working Adults Are Taking Extreme Caution to Protect their Identity and Information." Press release, May 5; Phan, 2005, op. cit.

[38] America Online and National Cyber Security Alliance (AOL/NCSA). 2004. *AOL/NCSA Online Safety Study*. Dulles, VA: AOL/NCSA.

[39] American Society of Newspapers Editors (ASNE). 2001. *Freedom of Information in the Digital Age*. Reston, VA: ASNE.

[40] Krane, David, Laura Light, and Diana Gravitch. 2002. *Privacy On and Off the Internet: What Consumers Want*. Conducted for Privacy & American Business. New York: Harris Interactive.

[41] AARP. 2003. *Consumer Experience Survey: Insights on Consumer Credit Behavior, Fraud, and Financial Planning*. Washington, D.C.: AARP State and National Initiatives.

[42] Taylor, Humphrey. 2004. "Do Not Call Registry Is Working Well," Harris Interactive Poll #10, February 13.

[43] Westin, Alan F., 2004, op. cit.

[44] American Express, 2004, op. cit.

[45] Experian, 2005, op. cit.

[46] Phan, 2005, op. cit.

[47] Office Depot, 2005, op. cit.

[48] Kandra and Brandt, 2003, op. cit.; Krane, Light, and Gravitch, 2002, op. cit.

[49] America Online and National Cyber Security Alliance, 2004, op. cit.

[50] Fox, Susannah. 2000. *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*. Washington, DC: Pew Internet & America Life Project.

[51]Culnan and Milne, 2001, op. cit.

[52] Krane, Light, and Gravitch, 2002, op. cit.

[53] Turow, 2003, op. cit.

[54] Kandra and Brandt, 2003, op. cit.

[55] America Online and National Cyber Security Alliance, 2004, op. cit.

[56] American Express, 2004, op. cit.

[57] Phan, 2005, op. cit.

[58] Office Depot, 2005, op. cit.

[59] Westin, Alan F. 2005. "While Number of ID Theft Victims Rise, Consumers Continue to Jump on 'Self-Help" Bandwagon. *Privacy & American Business Newsletter* 12(6):1–3.

[60] America Online and National Cyber Security Alliance, 2004, op. cit.it.

[61] Kandra and Brandt, 2003, op. cit.

[62] Chu, Kathy. 2005. "*Banks and Online Retailers Lose Customers to the Fear of ID Theft*.", March 24, p.D2; Conference Board, 2005, op. cit.; Office Depot, 2005, op. cit.; TRUSTe. 2004. "Study Reveals Over Half of Consumers Chilling to Online Holiday Shopping Due to Identity and Credit Card Theft." Press release, November 23.

[63] Conference Board, 2005, op. cit.; Fox, Susannah. 2005. *The Threat of Unwanted Software Programs Is Changing the Way People Use the Internet*. Washington, DC: Pew Internet & American Life Project.

[64] Milne, George R., Andrew J. Rohm, and Shalini Bahl. 2004. "Consumers' Protection of Online Privacy and Identity." *Journal of Consumer Affairs* 38(2):217–232.

[65] The low, medium, and high categories were defined as follows: for offline behavior, low meant engaging in zero to three activities; medium, four to six activities; and high, seven to 10 activities. For online behavior, low was defined as none or one of the five activities, medium as two or three activities, and high as four or five activities.

[66] American Express, 2004, op. cit.

[67] Office Depot, 2005, op. cit.

[68] Intervoice. 2005. "Identity Theft Study Finds Most Americas Feel No More Secure than One Year Ago." Press release, May 23; Louvel, Sophine. 2005. "ID Theft Concerns Change U.S. Consumer Banking Behaviors." Framingham, MA: Financial Insights; Wells Fargo. 2004. "New Survey Finds That Consumers Are Confused When It Comes to 'Online Rules of the Road.'" Press release, September 23.

[69] American Express, 2004, op. cit.

[70] Krane, Light, and Gravitch, 2002, op. cit.; Milne, Rohm, and Bahl, 2004, op. cit.

[71] Kristof, Kathy M. 2005. "U.S. Policy on Medicare Cards is a Boon for Identity Thieves." *Los Angeles Times*. September 17, p. A1.

[72] This result is consistent with American Express, 2004, op. cit., and Milne, Rohm, and Bahl, 2004, op. cit., but it is at odds with Krane, Light, and Gravitch, 2002, op. cit.; Wells Fargo, 2004, op. cit.

[73] Dingboom, Teresa. 2004. Results of Dittus Communications Spyware Survey Conducted by Ipsos-Public Affairs. Available at http://www.getnetwise.org/press/2004ppressrelease

[74] ClearCommerce. 2004. "Shoppers Ignorance Increases Online Fraud." News release. Available at http://www.itsecurity.com/tecsnews/sep2004/sep31.htm

[75] America Online and National Cyber Security Alliance, 2004, op. cit.

[76] Krim, Jonathan. 2005. "Online Data Gets Personal: Cell Phone Records for Sale," *Washington Post*, July 8, p. D1.

[77] Westin, 2005, op. cit.

[78] U.S. Federal Trade Commission. 2003. "Do Not Call Registrations Exceed 50 Million." Press release, September 17.

[79] Nader, Ralph, and Other Petitioners. 2001. *Petition for Rulemaking*, July 26. Available at http://www.epic.org/privacy/consumer/glbpetition.pdf

[80] Sahadi, Jeanne. 2005. "Privacy Experts' Wish List." *CNN Money*, May 13. Available at http://money.cnn.com/2005/05/11/pf/security_privacyadvocate_wish/index.htm

[81] Houtz, Jolayne. 2005. "Blocking Access to Credit Files Aim of Bill." *Seattle Times*, March 14.

[82] Guest, Jim. 2005. "The Fight Against Identity Theft." *Consumer Reports* 70(6):5.

[83] Sahadi, Jeanne. 2005. "Breaches: Federal Law on the Way?" *CNN Money*, July 7. Available at http://money.cnn.com/2005/07/06/pf/security_bills/

[84] Ponemon, Larry. 2005, "After a Privacy Breach, How Should You Break the News?" *Computerworld*, July 5.

[85] Kandra, Anne, and Andrew Brandt, 2003, op. cit.

[86] Privacy Rights Clearninghouse. 2004. *Identity Theft IQ Test*. San Diego, CA.

[87] Wachovia. 2004. "Identity Theft Quiz." Available at http://www.wachovia.com/misc/0,,799,00.html