

WITH A GRAIN OF SALT
WHAT CONSUMER PRIVACY SURVEYS DON'T TELL US

JIM HARPER AND SOLVEIG SINGLETON

June 2001

WITH A GRAIN OF SALT

WHAT CONSUMER PRIVACY SURVEYS DON'T TELL US

Jim Harper and Solveig Singleton

EXECUTIVE SUMMARY

A tremendous amount of news coverage and analysis of privacy issues has been driven by surveys of consumers showing high levels of concern. For this study, the authors reviewed 23 privacy surveys to assess their real usefulness to policymakers. Polls rarely play as large a role in policymaking as they have in the context of privacy. The study explains why lawmakers are right to be skeptical of surveys as a guide to policymaking generally, and privacy in particular.

The design of the survey format and questions can be used to manipulate survey results. In reviewing privacy surveys, the authors found almost universal use of “push-pull” questions or prompting for certain results. By contrast, the least manipulative form of surveys, unprompted surveys, show little concern for privacy as such, and more concern for crime issues like credit card fraud. Also, privacy surveys tend to lump together issues like credit card fraud, spam, and marketing under the heading of “privacy,” making it difficult to identify consumer concerns with precision.

Surveys generally, and privacy surveys in particular, also suffer from the “talk is cheap” problem. It costs a consumer nothing to express a desire for federal law to protect privacy. But if such law became a reality, it will cost the economy as a whole, and consumers in particular, significant amounts that surveys do not and cannot reveal.

By contrast, more objective measures of consumer actions show that, whatever consumers may say, they are going online and buying online in droves. In 1999, several forecasters predicted that electronic commerce would grow slowly because of the public’s concerns about privacy. But this gloomy scenario has not come to pass, with electronic commerce revenues growing far faster than projected.

The authors conclude that the craze for privacy surveys may be chalked up partly to the fact that for much of the debate no other information about the costs and benefits of privacy has been available. They further conclude that the surveys are not a sound basis for public policy. High-quality studies are difficult to conduct and may take years to complete. By contrast, public opinion polls are easy and cheap. Policymakers are being tempted to substitute survey results for real arguments and hard data. Responsible legislators, however, will look beyond survey results.

WITH A GRAIN OF SALT

WHAT CONSUMER PRIVACY SURVEYS DON'T TELL US

Jim Harper and Solveig Singleton

INTRODUCTION

For good or bad, in recent years polls and surveys have become a common tool of policy advocates.

The privacy debate is a paradigm example of this Washington passion for surveys, and poll after poll animates the debate. Indeed, it often seems that poll results are the only justifications that pro-regulatory advocates put forward to support demands for new legislation and regulation.

Politicians at times are criticized for using a “finger in the wind” rather than real leadership. But responsible legislators are, quite rightly, skeptical of the idea that good policymaking consists of following survey results. In electoral politics, unprompted polls are important guides to understanding the concerns of the voters. But polls are considerably less relevant to making substantive policy decisions about the laws that will best address these concerns.

The defects of over-reliance on poll results are particularly evident in a field as tricky and elusive as the protection of personal privacy. For example:

- Survey questions are likely to distort or manipulate answers.
- Many different concepts are often grouped together under the heading of “privacy,” including security, identity fraud, spam, and other crimes and inconveniences. Polls often compare not only apples and oranges, but toss in pears, mangoes, and persimmons as well.
- A full picture of the trade-offs between privacy and other consumer desires is rarely offered in surveys. Polls and surveys cannot effectively replicate the choices that consumers make in the real world, where they must choose among competing desires and where nothing comes for free. Indeed, the only truly unbiased and accurate poll is the marketplace, where consumers take actions that are consistent with their interests and values.

Surveys generally, and privacy surveys in particular, suffer from the “talk is cheap” problem. It costs a consumer nothing to express a desire for a law to protect privacy.

- Surveys and polls cannot consider the full range of policy options nor the legal and economic consequences of each one. Characterizations of polls showing “support” for a particular type of legislation should be dismissed out of hand. Such conclusions cannot possibly reflect the type of considered judgment that elected legislators, garnering all the facts, must bring to bear. For good reason, the American system is a constitutional republic rather than a direct, mob-rule democracy.

SURVEY MADNESS

The privacy debate has been consumed by a sort of survey madness. Each step in Washington’s policy-making kabuki dance is punctuated by a new survey. Surely no one still believes that yet more polling data can clarify the privacy issue. Perhaps each interest hopes that the sheer number of privacy surveys supporting its points will tip the scales in its favor.

Numerous consumer surveys have been issued purporting to show that Americans are very concerned about privacy. One commonly cited survey, by Business Week/Harris Interactive, reports that 57 percent of Americans want the government to pass federal privacy laws for the Internet.¹ A recent study by the Pew Internet & American Life Project found that 86 percent think that companies should ask permission before sharing personal information with third parties; 54 percent viewed cookies as an invasion of privacy; and only 27 percent agreed that tracking consumers online helps improve content and service.² Another survey (which we were unable to obtain) reportedly found that “27 million adults gave up using the Internet for lack of privacy last year, and that over half of all ‘Net users gave up an online transaction because they were asked for information they didn’t feel comfortable giving out.”³

Other surveys show less concern, and less of a regulatory impulse, among consumers. In response to one Jupiter Consumer Survey, only 14 percent of consumers reported that legislation would make them more likely to trust a Web site with information. Eighty-six percent said they would not trust Web sites even if regulated by the government. Even among Europeans, in whose countries privacy regulation is already widespread, one survey showed that fewer citizens believe that new laws would improve Internet security (15 percent) compared to those who believe the answer lies in technological solutions like passwords or encryption (27 percent).⁴

The welter of survey data surely creates confusion for policy-makers. This can only be compounded by the fact that opinion data have shown little responsiveness to government regulation and enforcement in the past. Since the 1970s, consumers’ attitudes about the trustworthiness and helpfulness of advertising, and the need for regulation, have barely changed, even though levels of regulation and enforcement varied widely from the activist 1970s to the deregulatory 1980s. The survey data do not support the view that more regulation increases the cred-

It often seems that poll results are the only justifications that pro-regulatory advocates put forward to support demands for new legislation and regulation.

ibility of advertisers.⁵ If anything, consumer attitudes about advertising in the deregulatory 1980s were more, not less, trusting of advertising.

This might mean several things. It might mean that consumers are unaware of the law and regulatory processes, so that regulatory action or inaction has little or no effect on levels of trust. It might mean also that consumer trust is not created by government regulation but rather by factors like brand recognition, personal experience, or the experiences of friends and neighbors (which is suggested by several surveys).

Surveys illuminate no clear pathway to solving privacy problems. The only certainty is that privacy surveys are likely to continue coming out in large numbers. And they are likely to continue having limited utility in solving public policy problems, for a variety of reasons.

THE TRICKY BUSINESS OF SURVEY DESIGN

In preparing this analysis, we obtained 23 surveys or reliable summaries of survey results (see Appendix A). Information about other important surveys was accessible only through news reports. Of the 23 surveys we reviewed, many were released with the format, structure, and questions withheld. Many polling and analysis organizations understandably have proprietary polling theories or questions, but this makes it very difficult to assess their validity. Independent reviewers cannot tell whether surveys ask neutral or varied questions, or whether they effectively “push poll” their respondents. We were, however, able to identify problems typical of many of the surveys and to compile examples.

In an area as complex as privacy, it is unlikely that surveys can accurately reflect consumers’ true preferences and concerns. The design of surveys and the questions they ask can elicit inaccurate responses more easily than accurate ones. Pollsters themselves may group many different concerns under the broad heading of “privacy.” Privacy surveys do not inform respondents about all the facets of the issue, and it is unlikely that they elicit the responses consumers would have in real-world situations.

The Answers Depend on the Questions

Survey results can vary quite widely based on what questions are asked and not asked. This counsels against uncritical acceptance of survey results. Polls that lead off with provocative questions are likely to get responses that address the provocation. Other questions are phrased in such a way as to guarantee a certain response.

The UCLA “Surveying the Digital Future” survey, for example, asked whether “people who go online put their privacy at risk.”⁶ Pew’s Report, “Trust and Privacy Online,” included the question, “How concerned are you, if at all, about businesses and people you don’t know getting personal information about you and your family — very concerned, somewhat, not too, or not at all?”⁷ The answers to these questions are obvious. Only an ignoramus or sociopath would say that there is no risk in going online, or that he or she was not concerned about the privacy of loved

The privacy debate has been consumed by a sort of survey madness. Each step in Washington’s policy-making kabuki dance is punctuated by a new survey.

ones. Reviewers of the resulting data may form the impression that citizens are cowering in their homes for fear of strangers when they are not.

Some of the more extreme examples of “push” polling in the surveys reviewed include the Business Week/Harris Interactive poll, “A Growing Threat.” The poll attempts to elicit consumers’ views on unsolicited mailings by asking “how concerned are you [that] . . . the company you buy from uses personal information you provide to send you unwanted information.”⁸ Naturally enough, no one wants to be sent unwanted information, so an overwhelming 78 percent of respondents said they were “very” or “somewhat” concerned about this.

By comparison, the Harris Interactive/Privacy Leadership Initiative survey asked more neutral questions about attitudes toward unsolicited mail or banner ads. It found that 54 percent report they would at least somewhat not appreciate e-mail unrelated to their initial purchase, but 63 percent would appreciate related e-mail. Fifty-two percent would at least somewhat appreciate banner ads related to the original purchase, while 64 percent would at least somewhat not appreciate unrelated banner ads.

Many privacy surveys may be misleading as to the strength of consumers’ interest in privacy. For example, consumers are often given the option of stating whether they are “concerned” or not about privacy. As one would expect — after all, who would not state that he is “concerned” in some sense about privacy? — survey results typically show respondents reporting they are concerned or very concerned about privacy, or with particular uses of information. But this does not reveal how consumers feel about privacy in comparison to other concerns.

Do consumers actually go through their days worrying about the privacy of medical information in HMO databases, or do they worry more about the security of their homes from break-ins? How does privacy compare to the possibility that a child safety seat might be installed incorrectly? If given a choice of how to spend five minutes, would a consumer have a hot dog, opt out of the data sharing his or her bank does, look up what a “cookie” is online, or watch the sun set? This, the privacy surveys do not tell us. But choices like these are the best indicators of true levels of “concern.”

For example, some surveys show very high levels of “concern” or “discomfort” with giving out credit card numbers and Social Security Numbers. Less than 10 percent report that they are comfortable giving out either. But other surveys suggest this “concern” is not great enough to stop people from actually giving out their credit card numbers online. Reportedly, 75 percent of Internet users have provided credit card numbers online, and 52 percent have provided their Social Security Number online.⁹

Unprompted Survey Results

The least manipulative and probably most accurate form of consumer survey is an unprompted survey, in which people are asked to list the issues of concern to

them without being prompted or given a list of possible responses. This type of survey is often used to identify election issues because candidates need to know what will motivate votes, not just what voters will say to a pollster.

In recent such surveys, privacy simply does not appear among top concerns.¹⁰ Particularly in contrast with other concerns such as medical care, education, crime, or Social Security, people appear to worry about privacy only when prompted.¹¹ This is probably the best indicator of how prompted surveys can affect results.

Of the surveys specific to the privacy topic we reviewed, only one apparently asked a significant number of unprompted questions about the respondent's attitudes to online commerce. This was the Harris Interactive/Privacy Leadership Initiative survey. It asked respondents, among other things, why they did not spend more time on the Internet; why they did not spend more money on the Internet; and why they might choose to buy offline rather than online. When respondents answered, their top concerns included crime risks such as credit card theft, the desire to see the product before buying it, or problems with convenience or selection in buying online.¹² But concern with traditional notions of privacy or with freedom from marketing did not appear.

Consistent with this, legislative staff we have spoken to informally report almost no constituent mail relating to concerns about privacy per se, or the use of information in marketing. Information privacy was not a decisive issue in the presidential election or primaries, although both Al Gore and Steve Forbes issued statements about the issue in the hope of making their positions a selling point.

Focusing on One Issue at a Time

Many privacy surveys distinguish poorly among the variety of issues relating to modern uses of personal information. Thus, credit card fraud and identity fraud may be referred to as privacy problems, even though these things are crime problems unrelated to legitimate uses of information. Spam and junk mail may be referred to as privacy problems even though they are better characterized as matters of annoyance and inconvenience. "Privacy" may also be used almost interchangeably with "security." They are related, but security is any number of practices and processes that protect a company's or government's ability to function.

Many surveys asked whether respondents had ever been a victim of a privacy violation, asked about their level of concern with privacy generally, or asked whether they thought the government should be more involved with solving privacy problems. The answers to such questions are of little or no use in the policy process, for they do not identify whether the consumer is thinking of credit card fraud, identity fraud, spam, the security of e-mail, telemarketing, collection of information by traditional marketers, or the FBI's Carnivore surveillance system.

For example, the National Consumers Union/Dell survey, which asked "why haven't you bought anything online in the last 12 months," found that 57 percent were worried about credit card theft, and 57 percent were "concerned that my

After all, who would not state that he is "concerned" in some sense about privacy?

personal information might be abused.”¹³ What does the latter reflect? The same concern as credit card theft? Different concerns? It is impossible to tell.

Some of the surveys did ask specific questions about marketing and credit card fraud. Most of these, consistent with the unprompted survey results, conclude that fraud, not privacy as such, is consumers’ greatest concern. Both the Arthur Andersen survey¹⁴ and the AT&T survey¹⁵ found consumers far more hesitant to give out their Social Security Numbers and credit card numbers than any other information. Correctly, the Jupiter analysis concludes that “consumers have tangled the online privacy and security issues and are currently more concerned with security than they are with actual privacy.”¹⁶ This study found that 78 percent selected credit card security issues as most important, compared to 58 percent who selected “any type of third-party information selling.”¹⁷

Spam is another issue that some pollsters include with privacy, generally finding low- to mid-range levels of concern.¹⁸ Spam is not in essence a privacy issue, but rather one of inconvenience and annoyance. The problem with spam is not that the sender has too much information about people. Spam occurs when someone sends e-mails indiscriminately to thousands of people, knowing nothing about them at all.

Because they collapse several information issues into one, called “privacy,” many polls and surveys have limited their usefulness to policy-makers. This is only one of several problems that plague polls in the complex area of privacy. Unless they are unprompted, polls are also likely to artificially “push” privacy-related concerns, or report exaggerated results. Even a poll that survives all these challenges does not necessarily present an opportunity to see inside the minds of consumers. This can only be done by watching consumers’ decisions in the marketplace.

“TALK IS CHEAP”: SURVEYS AND THE REAL WORLD

All surveys — and especially those in the area of privacy — suffer from what one might call the “talk is cheap” problem. That is, a consumer may say one thing, but act quite differently from what his or her words suggest.¹⁹ Actions are better indicators of people’s true preferences. Having to act makes the actor consider the cost of his or her preference, as well as the anticipated benefit. Another colloquialism — “Put your money where your mouth is” — captures this well. It is what consumers do, not what they say, that matters.

This observation does not only apply to surveys of consumers’ opinions. It also applies to consumers’ predictions about what they would do. Prodigy, one of the first to offer online grocery shopping (unsuccessfully) learned this the hard way. As Chet Thompson of Prodigy noted, “Market surveys told Prodigy that people wanted to do their grocery shopping by computer. They didn’t.”²⁰

Furthermore, the “talk is cheap” problem applies to consumer self-reporting on how they have acted or are acting. Particularly when prompted by provocative

Measures of consumers’ actions do not manifest concern for privacy nearly as strongly as one would expect

questions, poll respondents may report what they think the right answers should be. Thirty-five percent of respondents in a Business Week/Harris survey reported that they “always” read privacy policies; the Privacy Leadership Initiative survey found 26 percent “always” read privacy policies. But Web site operators report quite low attention to privacy policies. The former Chief Privacy Officer of Excite@Home, for example, told a March 13, 2001, Federal Trade Commission workshop that, on the day after that company was featured in a *60 Minutes* segment about Internet privacy, only 100 out of 20 million unique visitors accessed that company’s privacy pages.²¹

Arthur Andersens’s survey reported that 12 percent of respondents “always” reject cookies — unlikely given that Web functions such as shopping carts do not work properly without them. An objective study of server traffic found that cookies were disabled only .68 percent of the time in a billion page-views.²² Though these numbers can coexist, it is more likely that respondents over-report their rejection of cookies.

These are examples where consumers are asked to report their actual behavior, and they do so inaccurately. It is not hard to imagine that the stated opinions of consumers may be even less revealing of real-world attitudes.

Measures of consumers’ actions do not manifest concern for privacy nearly as strongly as one would expect. Only a small percentage of consumers opt out of marketing lists, use encryption, or regularly change their passwords.²³ Setting one’s browser to disable or warn about cookies takes five mouse-clicks on Netscape Communicator 4.5. (It may take a few minutes at first to find “how to” information and learn the routine.) These behaviors involve effort ranging from slight to minimal. Clearly, other priorities are holding sway, priorities such as taking a few extra minutes to pay bills, watching a favorite TV show, or keeping the toddler out of the neighbor’s swimming pool. Though polls and surveys suggest that consumer demand for privacy is high, they are not backed up by evidence of consumer behavior.

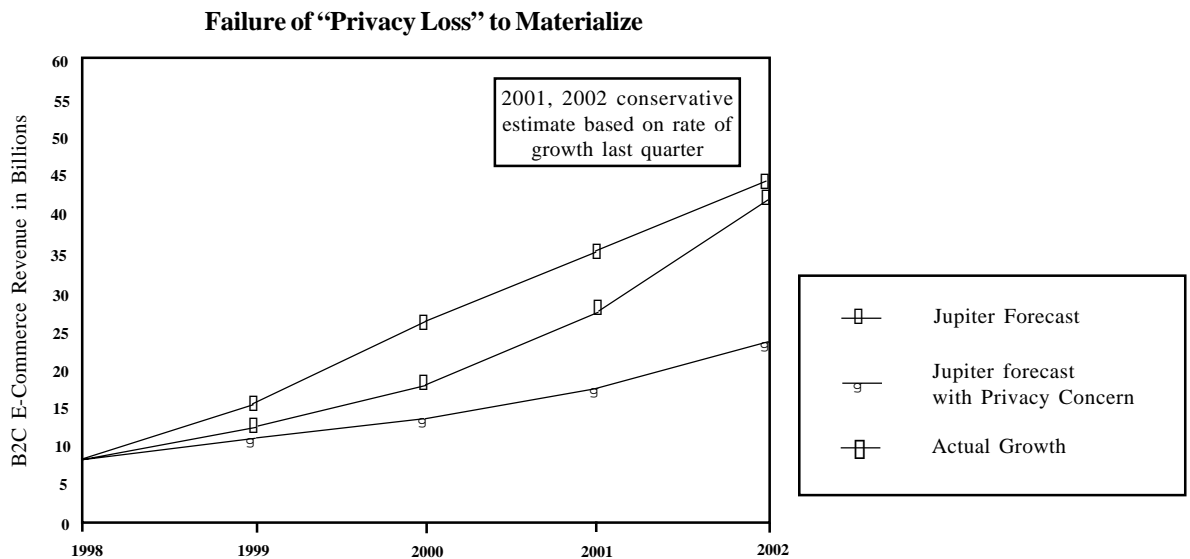
A Macro Indicator: Electronic Commerce

Privacy concerns have been highly vaunted as a hindrance to e-commerce, but the actions of consumers have not borne out predictions. In its 2000 report to Congress calling for federal privacy legislation, the Federal Trade Commission noted surveys that reported very high levels of consumer concern. It cited a study from Jupiter Research suggesting that privacy concerns would cause consumers to withhold \$18 billion in spending from e-commerce, and a study from Forrester Research that said \$2.8 billion dollars was lost to e-commerce in 1999 because of privacy concerns.

Putting aside the question of why the federal government or the Federal Trade Commission should solve the problems of e-commerce merchants, history has not borne out these predictions. As the figure below shows, current e-commerce levels exceed both the Jupiter forecasts of what would occur if nothing were done to allay

consumer privacy concerns and the forecasts of what would occur if steps were taken. Perhaps adoption of e-commerce would be still higher if more governmental privacy protections had been put in place, but the studies the FTC cites appear so far off the mark they can no longer serve as evidence of this. It is very hard to make the case that privacy concerns are destroying e-commerce when current numbers are outstripping estimates of just a few years ago.

When consumers are surveyed about privacy, they say many things. When it comes to learning consumers' true interests, the marketplace is the survey. Fifty-five percent of Americans bought something online during the 2000 holiday season, up from only 20 percent in 1998. Credit card transactions online are growing by leaps and bounds; there were 4.9 million such transactions online in 1997, 9.3 million in 1998, and 19.2 million in just the 3rd quarter of 1999.²⁴



Sources: U.S. Census Bureau, 2001; Jupiter Communications, 1999

Survey Results and Consumer Adoption Rates

In 1995, research psychologists Larry Rosen and Michelle Weil estimated that about 30 to 40 percent of the population is "resistant" to technology.²⁵ Of the remainder, 10 to 15 percent are eager early adopters, while about 60 percent wait for the early adopters to work out the bugs before they adopt technology.

Survey results show a population that is going online eagerly, with some holding back reportedly because of privacy concerns. But the surveys do not reveal to what extent the "hold-backs" are simply technology-resistant, likely to be the last on board regardless of whether there is any real danger to them in going online.

As one would expect, several surveys have found higher distrust of online commerce for security reasons among non-Internet users than among Internet users. Distrust levels are also generally lower among experienced users than they are among inexperienced users. This may mean that personal experience has reassured consumers. They have learned that Amazon.com, for example, is a motivated and talented bookseller, not a sinister enterprise that tracks customers in the hope of embarrassing them. On the other hand, differing levels of trust may indicate users' pre-formed positive attitudes toward technology and the pre-formed negative attitudes of technophobes.

In any case, to the extent polls and surveys can accurately measure them, consumers' attitudes are changing rapidly. In an August 2000 study by the National Consumers League, 91 percent of American respondents said they trust companies to follow posted privacy policies much of the time (up from 67 percent in 1998).²⁶ The percentage of users who think the Internet is secure enough for online financial transactions has reportedly risen from 34 percent to 45 percent since the summer of 2000.²⁷ Cyber Dialogue found in 1996 that 76 percent of respondents thought collecting information online was the "best way for companies to learn about customers." In 2000, that number was 88 percent. Those who thought it was "an invasion of privacy" dropped from 52 percent in 1996 to 37 percent in 2000.²⁸

The real world reflects quite different attitudes from what polls and surveys alone would suggest. Where consumers self-report on measurable actions like review of privacy policies and acceptance of cookies, there are large differences between poll results and what consumers are actually doing. On a macro level, electronic commerce continues to grow swiftly despite overwrought predictions about the negative effects of consumer privacy concerns, predictions that were accepted uncritically and foolishly by the Federal Trade Commission last year. For what they are worth, the survey numbers appear to show rapidly changing consumer opinions. The story surveys tell is incomplete, though. They are of limited utility to thoughtful policy-makers.

SURVEYS DON'T OFFER SOLUTIONS

If there remains a problem that lawmakers need to step in and solve, surveys are of no help. Surveys do not tell us what actually leads to consumer comfort or adoption in the real world. Surveys do not intelligently guide our policy choices between, for example, consumer education or new federal regulatory programs. This is one of many limits that surveys face as a part of decision-making about public policy. Surveys do not — and cannot — tell us the appropriate public policy responses to the problems they may identify.

An example from another field illustrates this well. In an October 1998 Harris Poll, 63 percent of women surveyed thought it was very likely or somewhat likely that they would get breast cancer.²⁹ In fact, the lifetime risk of developing breast cancer is about 13 percent.³⁰ In 1998, women died 43 percent more often from

If there remains a problem that lawmakers need to step in and solve, surveys are of no help.

heart disease than from all forms of cancer combined.³¹ If policy-makers were to follow poll numbers when addressing women's health, they could focus too aggressively on breast cancer, leading needlessly to the deaths of women from heart disease and other cancers. Following poll numbers may be popular, and it may even help win elections, but in this case it may kill women. Even accurate numbers about the cause of death among women do not reveal whether society should devote its resources to consumer education, medical research, or legislation and regulation.

As discussed above, the survey data on privacy do not give a clear picture of what specifically concerns the public — to say nothing of whether the public is actually being harmed or threatened with harm. (The surveys we reviewed provided some data showing, interestingly, that very few consumers have been actual victims of online credit card fraud although that is apparently their major concern.) That is only the first of many things the data do not reveal. The data do not reveal, for example whether the appropriate response is prohibitive regulation, consumer education, research and development, or leaving the responsibility for development of e-commerce to the businesses that will benefit most from it.

Polls Do Not Consider Policy Options

Many polls are touted as demonstrating public demand for new privacy laws. Such findings are hard to justify, however, because even the pro-regulation privacy advocates have not coherently described any new theory of privacy that such laws would protect. It appears, incidentally, that if they did they would depart radically from the tradition of freedom of information. Independent of polls, these advocates should be able to articulate what kind of privacy new laws would enforce, what uses of information are wrong, and why they are wrong. This alone would enable policy-makers to consider whether new laws are warranted.

If there are to be new laws, the polls certainly do not indicate what form they should take. The Second Restatement of Torts issued by the prestigious American Law Institute, summarizes the privacy law that has been adopted by statute or common law in all 50 states. It gives every consumer in the United States a cause of action in tort for “unreasonable publicity given to [one’s] private life.” This law is not limited as to subject matter or medium and it meets every outrageous revelation of private information with a cause of action. Furthermore, the FTC may enforce current laws against misrepresentation when a site violates its own privacy policy. Polls do not tell us whether privacy law reform should come from adding experimentally to the laws at the state level, from changing existing enforcement patterns, or whether there should be a new statutory regime at the federal level.

Polls obviously cannot predict how consumers would respond to education programs sponsored either by government or by the businesses that would benefit from consumer comfort with our information economy. If consumers are truly concerned, yet they are not being harmed in any recognizable way, education and information would seem to be the logical path for our public policy to follow. This is particularly true given the correlation between consumers' inexperience and

Following poll numbers may help win elections, but in the case of the Harris Poll on breast cancer, it could kill women.

unease with buying on the Internet.³² Yet, poll results showing consumer angst are almost always used as a justification to skip this step and move directly to regulation.

Consumer concerns could be allayed by breakthrough technologies. P3P³³ is one example of a technology that is being put forward to satisfy consumer demand for privacy online. Whether a technological solution will satisfy consumers cannot be gleaned from existing poll numbers, but it is one option that our policymakers should consider before introducing special legislation and regulation, especially in the absence of an articulated harm to consumers.

Polls and surveys fail to address all the policy options available to address privacy concerns. For this reason, polls fail as a robust tool of policy-makers. They certainly do not address the side effects each policy option might have.

Polls Do Not Consider Costs and Benefits

Legislation and regulation have high costs that are rarely, if ever, revealed to survey respondents. Polls do not weigh costs and benefits, though this is an essential part of policy-making today.

Pro-regulation privacy advocates are often quick to see “market failure,” and use it to support their calls for regulation. The comparison of the real world to a theoretical legal or regulatory regime can make the latter seem quite attractive. But laws and regulations are implemented in the real world, too. They have both direct, anticipated costs and unintended consequences, which may themselves be characterized as “government failure.” These include:

- The compliance costs of regulation, including direct legal costs and the heightened risk of regulatory involvement.
- The impact of new law on innovation and future ventures that might use consumer information in unforeseen beneficial ways. Had opt-in (or even opt-out) been the rule in the late nineteenth century, for example, credit reporting could never have been invented. Most people even today could have to depend on the good will of their local storekeepers or bankers to get credit.
- The reduced direct and indirect benefits to consumers from information sharing among companies. Consumers may be largely unaware of these benefits; their nature and scope are just beginning to be studied. Cost savings from information sharing in financial services alone have been estimated at \$17 billion per year for the customers of just one group of companies. (The savings would be larger still for the entire financial services industry.)³⁴ A study of the apparel industry estimates that an “opt-in” rule would effectively impose a \$1 billion dollar tax on catalog and Internet clothing sales as businesses passed on an increase in costs of from 3.5 to 11 percent.³⁵

Pro-regulation privacy advocates are often quick to see “market failure,” and use it to support their calls for regulation.

In the face of the statistical barrage on privacy, why not just pass new laws? The short answer is that not everything the public asks for is good public policy.

- Reduced choice and competition from new companies who are able to get a foot in the door because of transfer of information from established companies. The idea that information sharing means more competition is well-recognized in federal law. When opening up monopoly phone markets, the Federal Communications Commission, for example, makes sure that new competitors can access vital consumer information.
- The cost to taxpayers. Poll respondents speaking in their capacity as consumers may blithely call for new legislation and regulation, but as taxpayers they may have quite different views. In the light of experience, taxpayers would probably be disinclined to support a privacy protection bureaucracy and the permanent tax increase it would require.

The unintended consequences of new laws and regulations are often discovered only after they are put in place. The costs listed here can only be a starting point. But even good guesses about the costs and benefits of privacy laws are not incorporated into survey questions. Indeed, privacy surveys do not even weigh different approaches to the problems they identify. They should be relied on sparingly by policy-makers, who have a much higher calling than to absorb and regurgitate survey data.

THE PROPER ROLE OF SURVEYS IN A REPRESENTATIVE DEMOCRACY

In the face of the statistical barrage on privacy, why should legislators not simply go ahead and pass new privacy laws? The short answer — affront to democratic principles though it may be — is that not everything the public asks for is good public policy. Surveys may tell us what is popular, but they do not tell us what is good.

The admiration for democracy in the United States has never been unqualified. It is tempered in light of its imperfections, particularly the danger of majoritarianism. The United States is not a plain and simple democracy. It is a constitutional democracy or republic, in which elected representatives make decisions, and even the powers of this majority-elected government are bounded by a constitution representing a particular conception of individual rights and the common good.

The Framers saw representative democracy as an acceptable means to preserve the rights protected by the United States Constitution. But direct democracy, the more “pure” form of democracy, was not. In the eyes of James Madison, representatives were necessary to temper or filter the public’s tendency to act rashly. An assembly of representatives would protect the country from dangerous or foolish actions by “passing [the public views] through the medium of a chosen body of citizens.”³⁶ Direct democracy could give rise to particular moments in public affairs when the people, stimulated by some irregular passion, or some illicit advantage, or misled by the artful misrepresentations of interested men,

may call for measures which they themselves will afterwards be the most ready to lament and condemn.³⁷

This is why we have representative, not direct, democracy. Congress is a group of elected representatives, not a giant computer that tabulates votes. It is the job of these elected officials to weigh all options before them and consider the costs and benefits of each. These policy-makers should not let the many privacy polls serve as a substitute for thinking through issues.

To further protect against adventurousness in government, the powers of government are limited by the Constitution. In particular, the First Amendment protects free speech and prevents government from controlling what people may say. Many proposed privacy laws have constitutional defects when measured against the standards set by the First Amendment.³⁸ Polls do not admit to these, but lawmakers must. This is yet another reason to discount polls in the policy-making process.

CONCLUSION

There are few issues where polling and demagoguery threaten to dominate the debate in Congress to the extent it does in federal privacy policy.

Consumer privacy surveys tell us little or nothing about the right thing to do in the area of privacy. Yet surveys are not a sound basis for public policy in privacy any more than in any other area. Privacy surveys have generally prompted, pushed, or pulled respondents to consider “privacy” as a generic issue with a generic solution. The results of such surveys are not supported by unprompted surveys or by more objective measures of consumers’ actions. Based on surveys, some analysts have presented an overly pessimistic view of the future of online commerce, but it continues to grow at a rate far exceeding their projections. Furthermore, surveys do not provide any evidence that consumers are worse off in the absence of broad, new privacy regulation. Nor do they show that regulation would provide any benefits, much less that its benefits would exceed its costs.

The craze for privacy surveys may be chalked up partly to the fact that for much of the debate no other information about privacy has been available. Information privacy is a relatively new issue, and a fantastically complex one. Unlike the related issue of advertising, economists have not conducted many empirical studies showing how companies actually use information in the economy, or how it benefits consumers. High-quality studies are difficult to conduct and may take years to complete. By contrast, public opinion polls are easy and cheap. It is tempting, therefore, for policy-makers to substitute survey results for real arguments and hard data, as did the Federal Trade Commission.

Especially in fast-changing technology markets desperately trying to find business models that actually work, advocates of regulation should bear a heavy burden of proof that new laws would do more good than harm. Privacy surveys, whatever their results, cannot begin to discharge this burden.

There are few issues where polling and demagoguery threaten to dominate the debate in Congress to the extent it does in federal privacy policy.

APPENDIX A: Surveys Reviewed

Survey Group & Title	Date	Population Surveyed
Alan F. Westin/Louis Harris & Associates, "E-Commerce & Privacy: What Net Users Want"	June 1998	Telephone survey of 1011 adults
Alan Westin/Opinion Research Corporation, "'Freebies' and Privacy: What Users Think"	July 1999	Survey of 474 respondent Internet users
Arthur Andersen/KS&R, "Internet Privacy Survey"	May 2000	Online survey of 365 users drawn from panel of 2000 Internet users
AT&T Labs, "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy"	April 1999	Surveyed 381 heavy Internet users drawn from FamilyPC Magazine/Digital Research Inc. Family panel
Business Week/Harris Interactive, "Business Week/Harris Poll: A Growing Threat"	March 2000	Telephone survey of 1,014 adults
Center for Democracy & Technology Privacy Survey	1997	
Cheskin Research, "Trust in the Wired Americas"	July 2000	Online survey of 2,681 Internet users in the U.S. and Latin America
Columbus Group, "Privacy Policies Critical to Online Consumer Trust"	March 2001	Survey of Canadian Internet users
Cyber Dialogue, "Best Practices in Online Customer Privacy Protection"	April 2001	
Cyber Dialogue, "Privacy vs. Personalization: A Delicate Balance"	1999	Online survey of national sample of 500 U.S. Internet users.
Equifax/Louis Harris & Associates, Inc., "1996 Equifax/Harris Consumer Privacy Survey"	July 1996	1,005 telephone interviews of U.S. residents.
Forrester Research, Inc., "The Forrester Report"	September 1999	
Gallup Poll, "Few Users Paying Close Attention to Internet Privacy Issue"	September 2000	Telephone interviews with 1,008 Americans, including 573 online users
Graphics Visualization Usability Center, "GVU's 8 th WWW User Survey"	November 1997	Online survey of 10,000 web users
Harris Interactive/Privacy Leadership Initiative Survey	December 2000	
Jupiter Communications, "Proactive Online Privacy: Scripting An Informed Dialogue to Allay Consumers' Fears"	June 1999	
Mass Insight Corporation, "Privacy and Technology: Getting the Balance Right"	Spring 2000	Telephone survey of 500 Massachusetts residents
National Consumers Union/Dell/Harris Interactive, "E-Consumer Confidence Study"	August 2000	Online survey of 2810 Americans
The Personalization Consortium Survey	April 2000	Study sent to 20,000 U.S. Internet users randomly selected from opt-in list, with 4500 Web Users replying
Pew Internet & American Life Project, "Fear of Online Crime"	April 2001	Telephone interviews of 2,096 U.S. adults
Pew Internet & American Life Project, "New Internet Users"	March 2000	Interviews with 3533 Americans, including 1,690 Internet users
Pew Internet & American Life Project, "Trust and Privacy Online"	August 2000	Survey of 2117 Americans including 1,017 Internet users
The UCLA Center for Communication Policy, "Surveying the Digital Future"	November 2000	Telephone interviews with 2096 U.S. households
Zetetic/MBInteractive, "Consumer Internet Privacy Survey"	1999	Online poll of Zetetic's 30,000 member panel of whom 9,339 completed the survey

Notes

- ¹Stephen E. Arnold, "Internet Users at Risk: The Identity/Privacy Target Zone." *Forbes ASAP*, January 1, 2001, p. 24.
- ²Brian Krebs, "People Want More Control Over Personal Info Online," *Newsbytes*, August 21, 2000.
- ³Ryan James, "Safety on the Net," *The Toronto Sun*, June 8, 2000, p. 66 (describing Privada survey).
- ⁴"EU Preparing Plans for Battling Cybercrime," *The Deseret News*, December 13, 2000, p. A13 (also noting that 3 percent of Europeans believe the Internet is secure).
- ⁵John E. Calfee and Debra Jones Ringold, "The 70 percent Majority: Enduring Consumer Beliefs About Advertising," 13 *JOURNAL OF PUBLIC POLICY AND MARKETING* 228 (1994).
- ⁶The UCLA Center for Communication Policy, "Surveying the Digital Future," November 2000, p. 32.
- ⁷Pew Internet & American Life Project, "Trust and Privacy Online," August 2000, p. 22.
- ⁸Business Week/Harris Interactive, "Business Week/Harris Poll: A Growing Threat." August 2000, p. 2.
- ⁹Harris Interactive/Privacy Leadership Initiative Survey, December 2000, p. 15.
- ¹⁰See, e.g. Peter Raducha, "Preliminary Results of a Nationwide Survey of Youth," Global Youth Action Network, July 2000; Frank Newport, "Economy, Education, Health, Crime and Morality Most on Americans' Minds This Election Year," *Gallup News Service*, June 22, 2000.
- ¹¹See, e.g., National Consumers Union/Dell/Harris Interactive, "E-Consumer Confidence Study," August, 2000 (reporting that consumers care more about privacy than health care, crime, taxes); see also Equifax/Louis Harris & Associates, Inc., "1996 Equifax/Harris Consumer Privacy Survey," July 1996 (reporting consumer concern about privacy lower than "controlling the cost of medical insurance," "staying out of excessive debt," "reducing insurance fraud," or "controlling false advertising.").
- ¹²Harris Interactive, Inc./Privacy Leadership Initiative Survey at 12, 22.
- ¹³National Consumers Union/Dell/Harris Interactive, "E-Consumer Confidence Study."
- ¹⁴The Arthur Andersen study found only 2 percent comfortable with giving out their Social Security Number online, and only 8 percent comfortable with giving out credit card number.
- ¹⁵The AT&T study reports 1 percent of consumers comfortable with giving out Social Security Numbers, and 3 percent comfortable with giving out credit card numbers.
- ¹⁶Jupiter Communications, "Proactive Online Privacy: Scripting An Informed Dialogue to Allay Consumers' Fears," June, 1999, p. 2.
- ¹⁷See Lycos/Cyber Dialog, "American Internet User Survey," *News Release*, March 5, 1998 (reporting 85 percent very or extremely concerned about security of credit card number, with 75 percent reporting such a level of concern about "privacy"); Pew Internet & American Life Project, "Fear of Online Crime," April, 2001 (87 percent concerned about credit card theft online); Pew Internet & American Life Project, "New Internet Users," March, 2000, p. 1 ("A likely explanation for new user's reluctance to conduct transactions online is worry over the security and privacy of sending credit card information over the Internet."); UCLA Center, "Surveying the Digital Future," (91.2 percent concerned about credit card security).
- ¹⁸See, e.g. AT&T Labs, "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy," April 1999, p. 22; Cyber Dialogue, "Best Practices in Online Customer Privacy Protection," April, 2001 (in 1996, 78 percent of respondents thought that submitting personal information online was a guarantee to receive junk email; in 2000, 50 percent thought the same.)
- ¹⁹Paul Rubin & Tom Lenard, *Privacy and the Commercial Uses of Information* (Washington, D.C.: Progress and Freedom Foundation, forthcoming 2001) p. ____.
- ²⁰Peter K. Pitsch, *The Innovation Age: A New Perspective on the Telecom Revolution* (Washington, D.C.: The Hudson Institute and the Progress and Freedom Foundation 1996): 48.
- ²¹Workshop on "The Information Marketplace: Merging and Exchanging Consumer Data," Federal Trade Commission, March 13, 2001 (comments of Ted Wham) <<http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm>>.
- ²²See, e.g. "Caught With the Cookie Jar," *National Journal's Technology Daily AM Edition*, April 4, 2001, p. 4 ("Web analysis service Web Side Story found that in over 1 billion page views cookies were disabled just .68 percent of the time");
- ²³"Mining for Privacy Gold," *San Francisco Business Times*, March 9, 2001, p. 21 (3 percent of Americans opt out of marketing mailings); Carey Adams, "The Internet and Security," *Access Control & Security Systems Integration*, November 2000 (18 percent never change their

passwords, 33 percent only when forced to do so, and 17 percent change only once per year; 22 percent have passwords that can be cracked in seven minutes or less); Krebs (9 percent report using encryption, 5 percent report using software that hides their identity).

²⁴ Cyber Dialogue, “Best Practices” at 2.

²⁵ Larry D. Rosen and Michelle M. Weil, “Public Interest in the Information Superhighway,” (1995), at <http://www.csudh.edu/psych/study3.html>.

²⁶“Commissioned Research Confirms Privacy is a Key Issue Influencing Consumer Influence of Internet Billing,” *Canada Newswire*, January 16, 2001.

²⁷“Motor Insurance Gets Into Fast Lane,” *Marketing Week*, March 29, 2001, p. 59.

²⁸Cyber Dialogue, “Best Practices,” at 2.

²⁹ *Health Risks and Fears* Harris Poll, Oct. 14-20, 1998, reported at PollingReport.com <http://www.pollingreport.com/health.htm>.

³⁰ *Who’s Smarter About Cardiovascular Disease — Men or Women?: Surprising Survey Results*, Yankelovich Partners survey, Sept. 30-Oct. 19, 1998, reported at HeartStrongWoman.com http://www.heartstrongwoman.com/survey_results.php3.

³¹ *Deaths and death rates for the 10 leading causes of death in specified age groups, by race and sex: United States, 1998*, National Vital Statistics Reports, Vol. 48, No. 11, July 24, 2000, pg. 28

³²Pew Internet & American Life Project, “New Internet Users” at 15, 22 (“Length of time on the Internet is strongly correlated with willingness to conduct Internet transactions”)(Of those online a year or less, 30 percent have used their credit card to make a purchase, compared to veterans of two years or more, 56 percent); see also Zetetic/MBInteractive, “Consumer Internet Privacy Survey,” 1999; Cyber Dialogue, “American Internet User Survey,” at 2; UCLA Center, “Surveying the Digital Future” at 41.

³³ P3P stands for “Platform for Privacy Preferences Project” developed by the World Wide Web Consortium. P3P creates an interface between the web surfer and web sites that gives the user control over how and when his information is released to the web sites.

³⁴ Ernst & Young for the Financial Services Roundtable, *Customer Benefits from Current Information-Sharing by Financial Services Companies*, December, 2000, available at <http://www.bankersround.org/PDFs/custbenefits.PDF>.

³⁵ Michael A. Turner, “The Impact of Data Restrictions on Consumer Distance Shopping,” 2001, available at www.understandingprivacy.org in spring, 2001.

³⁶ THE FEDERALIST NO. 10, at 73 (James Madison) (Charles A. Beard ed., 1948).

³⁷ *Id.* at 268.

³⁸ Solveig Singleton, “Privacy Versus the First Amendment: A Skeptical Approach,” XI *FORDHAM L.J.* 97 (2000).

ABOUT THE AUTHORS

SOLVEIG SINGLETON is a lawyer and senior policy analyst with CEI's Project on Technology and Innovation. Her focus is on privacy issues, telecommunications, and free speech law. Ms. Singleton is the former director of information studies for the Cato Institute. Her articles have appeared in the *Journal of Commerce*, *The Washington Post*, *Philadelphia Inquirer*, *The Wall Street Journal*, *Internet Underground*, and *HotWired*. She is the co-editor of two books, *Regulators' Revenge* (1998) and *Economic Casualties* (1999). Her undergraduate degree is from Reed College, where she majored in philosophy. She then graduated *cum laude* from Cornell Law School and worked for two years at a telecommunications law firm before entering the world of public policy.

JIM HARPER is the editor of *Privacilla.org*, as well as the founder and principal of *PolicyCounsel.Com*, an Information Age public policy consulting firm. Previously, Mr. Harper served as counsel to committees in both the U.S. House of Representatives and Senate. He is a California lawyer and a graduate of Hastings College of the Law in San Francisco, where he was Editor-in-Chief of the *Hastings Constitutional Law Quarterly*.