
Americans, Marketers, and the Internet: 1999-2012

Abstract

This is a collection of the reports on the Annenberg national surveys that explored Americans' knowledge and opinions about the new digital-marketing world that was becoming part of their lives. So far we've released seven reports on the subject, in 1999, 2000, 2003, 2005, 2009, 2010, and 2012. The reports raised or deepened a range of provocative topics that have become part of public, policy, and industry discourse. In addition to these reports, I've included three journal articles — from *I/S, New Media & Society* and the *Journal of Consumer Affairs* — that synthesize some of the findings and place them into policy frameworks. The journals have kindly allowed reproduction for this purpose.

Keywords

surveys, marketing, advertising, privacy, surveillance, media, shopping, communication, internet, web, public opinion, public policy, controversy, shopping working papers series

Disciplines

Communication | Communication Technology and New Media | Marketing | Public Relations and Advertising | Social and Behavioral Sciences

Author(s)

Joseph Turow, Amy Bleakley, John Bracken, Michael X. Delli Carpini, Nora A. Draper, Lauren Feldman, Nathaniel Good, Jens Grossklags, Michael Hennessy, Chris Jay Hoofnagle, Rowan Howard-Williams, Jennifer King, Su Li, Kimberly Meltzer, Deirdre K. Mulligan, and Lilach Nir

Americans, Marketers, and the Internet: 1999 — 2012



Joseph Turow

Amy Bleakley, John Bracken, Michael X. Delli Carpini, Nora Draper,
Lauren Feldman, Nathaniel Good, Jens Grossklags, Michael Hennessy,
Chris Jay Hoofnagle, Rowan Howard-Williams, Jennifer King, Su Li,
Kimberly Meltzer, Deirdre Mulligan, Lilach Nir



The Annenberg School for Communication
 3620 Walnut Street
 Philadelphia, PA 19104-6220
 Tel 215.898.7041 jturow@asc.upenn.edu

Joseph Turow
 Robert Lewis Shayon Professor
 and Associate Dean for Graduate Studies

Greetings-

It's been 15 years since the first Annenberg national survey that explored Americans' knowledge and opinions about the new digital-marketing world that was becoming part of their lives. So, far, we've released seven reports on the subject, in 1999, 2000, 2003, 2005, 2009, 2010, and 2012. The reports raised or deepened a range of provocative topics that have become part of public, policy, and industry discourse.

- From 1999: “Our findings reveal that the rush to connect the Web to American homes is happening despite parents’ substantial insecurity. In certain ways, the fears parents have revealed to us are similar to the fears parents have expressed during introduction of the movies, broadcast television, and cable TV. But the concerns are not merely repeats of past litanies [...] Parents fear the Web for its unprecedented openness—the easy access by anybody to sexuality, bad values, and commercialism. They also fear the Web for its unprecedented interactive nature—the potential for invading a family’s privacy and for adults taking advantage of children. These fears are heightened among many parents because they don’t believe they understand the technology well enough to make the best use of it. Yet they believe their children need it.”
- From 2000: “American 10-17-year olds are much more likely than parents to say it is OK to give sensitive personal and family information to commercial Web sites in exchange for a free gift. Examples of such information include their allowance, the names of their parents’ favorite stores, what their parents do on weekends, and how many days of work their parents have missed. It is wrong to think that simple discussions between parents and kids about what information to give to the Web can easily resolve these tensions. Fully 69% of parents and 66% of kids say they have had these sorts of discussions. But when we specifically interviewed pairs of parents and kids in the same family, we found that most didn’t agree on whether these sorts of discussions had ever taken place.”
- From 2003: “59% of adults who use the internet at home know that websites collect information about them even if they don’t register. They do not, however, understand that data flows behind their screens invisibly connect seemingly unrelated bits about them. When presented with a common version of the way sites track, extract, and share information to make money from advertising, 85% of adults who go online at home did

not agree to accept it on even a valued site. When offered a choice to get content from a valued site with such a policy or pay for the site and not have it collect information, 54% of adults who go online at home said that they would rather leave the web for that content than do either.”

- From 2005: “Most internet-using U.S. adults are aware that companies can follow their behavior online. Almost all (89%) of those who say their supermarkets offer frequent shopper cards applied for them—and in doing it gave the stores personally identifiable information about themselves. In this retail environment where companies collect personal information, Americans do directly admit feeling vulnerable. Only 17% agree with the statement that ‘what companies know about me won’t hurt me’ (81% disagree), 70% disagree that ‘privacy policies are easy to understand,’ and 79% agree that ‘I am nervous about websites having information about me.’ Sadly, though, only about one out of three (35%) says he or she ‘trust(s) the U.S. government to protect consumers from marketers who misuse their information.’”
- From 2009: “Contrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests. Moreover, when Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages—between 73% and 86%—say they would not want such advertising....92% agree there should be a law that requires “websites and advertising companies to delete all stored information about an individual, if requested to do so.”
- From 2010: “...[E]xpressed attitudes towards privacy by American young adults (aged 18-24) are not nearly as different from those of older adults as many suggest. With important exceptions, large percentages of young adults are in harmony with older Americans when comes to sensitivity about online privacy and policy suggestions.”
- From 2012: “The 2012 election marks a watershed moment for online advertising. In unprecedented ways, and to an unprecedented extent, campaign organizations across the American political spectrum are using hundreds of pieces of information about individuals’ online and offline lives to ensure the ‘right’ people are being targeted with the ‘right’ advertising. Yet, contrary to what marketers claim, the vast majority of adult Americans—86%—do not want political campaigns to tailor advertisements to their interests. Moreover, large majorities of Americans say that if they learn a candidate they support carries out one or another real-life example of tailored political advertising, it will decrease their likelihood of voting for the candidate.”
- Over time: In our 2003 report, we first noted that “57% of U.S. adults who use the internet at home believe incorrectly that when a website has a privacy policy, it will not share their personal information with other websites or companies.” That finding came from an agree-strongly/disagree-strongly query. Surveys carried out in 2005, 20010, and 2012 posed the question in a true-false format and found remarkably similar numbers, with 59%, 62%, and 54% incorrectly answering “true.” (The 2012 finding isn’t in the report printed here, but I presented it at a Federal Trade Commission meeting on November 8, 2012.) More troubling, when the percentage of people responding to the true-false who said they “don’t know” is taken into account, we consistently find that over 70% of respondents don’t properly understand the phrase *privacy policy*. The

recommendation from the 2005 report is quite relevant today: “The Federal Trade Commission should require websites [or perhaps more specifically websites that use data without permission] to drop the label *Privacy Policy* and replace it with *Using Your Information*. [...] For many people [...] the label is deceptive; they assume it indicates protection for them. A *Using Your Information* designation will likely go far toward reversing the broad public misconception that the mere presence of a privacy policy automatically means the firm will not share the person’s information with other websites and companies.”

In addition to these reports, I’ve included three journal articles—from *I/S, New Media & Society* and the *Journal of Consumer Affairs*—that synthesize some of the findings and place them into policy frameworks. The journals kindly allow reproduction for this purpose.

As will be clear from the cover and from scanning this collection, the research was very much a collaborative activity, and I made friends that continue to this day and beyond.

The funding for most of these surveys came from two sources, The Annenberg Public Policy Center and the Annenberg School for Communication, both at the University of Pennsylvania. Kathleen Hall Jamieson, Director of the Policy Center, and Michael X. Delli Carpini, Dean of the Annenberg School, have been generous and enthusiastic proponents of the work. They have also supported a number of conferences aimed at bringing academics, policymakers, journalists, and students together to discuss the social and public-policy ramifications of our findings.

I look forward to continuing my explorations of the intersections of marketing, digital media, and society from the point of view of the public. During the past few years, though, I have received requests for past reports, so I figured it might be useful and interesting to place them next to one another. I hope you agree.

Joseph Turow
Philadelphia, Pennsylvania, March 2014

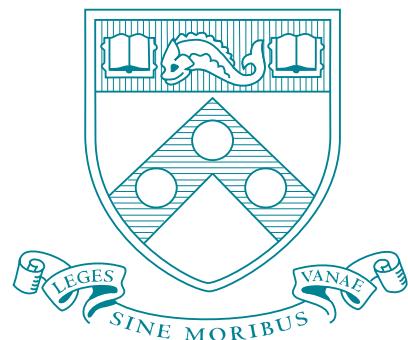
Contents

- 2 Preface
- 5 The Internet and the Family: The View from Parents / The View from the Press
- 51 The Internet and the Family 2000: The View from Parents / The View from Kids
- 89 Americans & Online Privacy: The System is Broken
- 126 Open to Exploitation: American Shoppers Online and Offline
- 164 Americans Reject Tailored Advertising, and Three Activities That Enable It
- 191 How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?
- 211 Americans Roundly Reject Tailored Political Advertising At A Time When Political Campaigns Are Embracing It
- 239 The Federal Trade Commission and Consumer Privacy in the Coming Decade
- 266 Internet Privacy and Institutional Trust
- 285 Consumers' Understanding of Privacy Rules in the Marketplace

The Internet and the Family: The View from Parents The View from the Press

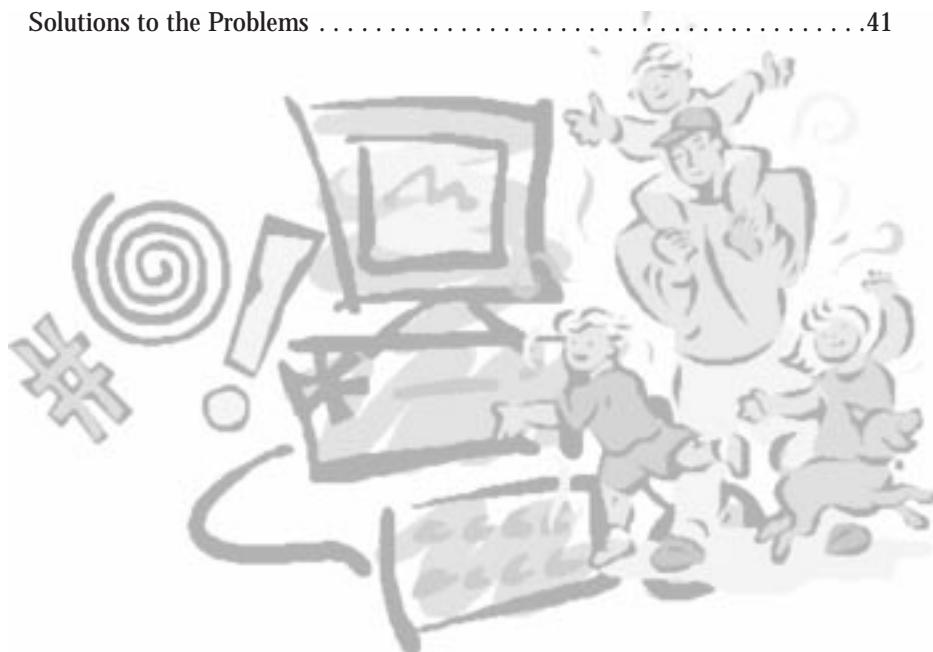
By Joseph Turow

May 1999



The Internet and the Family: The View from Parents The View from the Press

Part 1	5
Overview	6
The Study and the Population	8
Parents and the Online World	11
The Views of Parents from Online Homes	12
The Views of Parents from Homes Not Online	21
Factors Predicting Whether Households with Computers have the Internet	28
Concluding Remarks	32
Part 2	33
Overview	34
The Study and the Method	36
The Topics in the Articles	38
The People Quoted in the Articles	40
Solutions to the Problems	41



FOREWORD

The Annenberg Public Policy Center was established by publisher and philanthropist Walter Annenberg in 1994 to create a community of scholars within the University of Pennsylvania which would address public policy issues at the local, state and federal levels. Consistent with the mission of the Annenberg School for Communication, the Center has four ongoing foci: Information and Society; Media and the Developing Mind; Media and the Dialogue of Democracy; and Health Communication. Each year, as well, a special area of scholarly and social interest is addressed. The Center supports research and sponsors lectures and conferences in these areas. This series of publications disseminates the work of the Center.

Kathleen Hall Jamieson
Director

Joseph Turow is Robert Lewis Shayon Professor of Communication at the University of Pennsylvania's Annenberg School for Communication. He is the author of more than 45 articles and seven books on mass media, including *Breaking Up America: Advertisers and the New Media World* (University of Chicago Press, 1997; paperback 1998); and *Media Today*, an introductory college textbook just published by Houghton Mifflin. He currently serves on the editorial boards of the *Journal of Broadcasting and Electronic Media*, the *Journal of Communication Critical Studies in Mass Communication*, the *Encyclopedia of Advertising* and the *Sage Annual Review of Communication Research*. He is also a member of the founding editorial advisory board of a new scholarly journal, *New Media & Society: An International Journal*, to be published in London.

PART 1: THE VIEW FROM PARENTS

Capsule of findings:

The majority of American parents with computers at home juggle the dream and the nightmare of the Internet at the same time.

The rush to connect the Web to American homes is happening despite parents' substantial insecurities about it. Most parents with online connections at home are deeply fearful about the Web's influence on their children. For example, over 75% of these parents are concerned that their children might give out personal information and view sexually explicit images on the Internet.

PART 2: THE VIEW FROM THE PRESS

Capsule of findings:

"Your children need the Internet. But, if they do go online, be terrified."

From October 15, 1997 through October 15, 1998, stories in 12 newspapers presented the Internet as a Jekyll-and-Hyde phenomenon over which parents are left to take control with little community backup. Sex crimes regarding children and the Web were featured in one of every four articles. The press' portrayal of the Internet reflects the results of the national survey presented in Part 1.

PART 1: THE VIEW FROM PARENTS

By **Joseph Turow**

Annenberg School For Communication
University of Pennsylvania

With the assistance of

Annie Weber and Jennifer Mazurick

Natalia Gridina, Cory Allen, Laura Ducceschi, Eric Zimmer, and Christopher Hunter

Annenberg School For Communication
University of Pennsylvania

OVERVIEW

The majority of American parents with computers at home juggle the dream and the nightmare of the Internet at the same time.

- 60% of U.S. households with children aged 8 to 17 have home computers. Of those, 61% are connected to the Internet.
- American parents are conflicted about the Web. Across the nation, 70% of parents with computers in the home say the Internet is a place for children to discover “fascinating, useful things” and nearly 60% say that children who don’t have the Internet are disadvantaged compared to their peers who do. At the same time, over 75% of parents are concerned that their children might give out personal information and view sexually explicit images on the Internet.
- Most parents with online connections at home are deeply fearful about the Web’s influence on their children. Online parents can be categorized as *online worriers*, *disenchanteds*, and *gung ho’s*. The gung ho group, the only one with overall positive attitudes, makes up only 39% of online parents.
- Attitudes toward the Web, positive or negative, are not good predictors of whether the parent will have an online connection at home. Parents with home computers but no online connections fall into three groups that are surprisingly similar in outlook to the corresponding groups of “online” parents. The groups are *offline worriers*, *bah humbugs*, and *ready-to-go’s*.
- Education and income are also not major determinants of whether a household will have an online connection once a computer is in the home.
- Instead, the most important predictor of an online connection in a household with a computer seems to be a parent’s experience with the Web outside the home.
- 32% of parents with online connections use protective software that guards children’s access to sites—a sign that a substantial number of parents have gone out of their way to try to deal with the concerns they hold.

These are highlights from the first *Annenberg National Survey on the Internet and the Family*. The groundbreaking study of parental attitudes and activities around the Web was conducted by Roper Starch Worldwide for the Annenberg Public Policy Center of the University of Pennsylvania. 1,102 parents in households with at least one working computer and at least one child between ages 8 and 17 were interviewed by phone between November 12th and December 20th, 1998.

The purpose of the study was to understand what parents think and do about the Web. We also wanted to find out what factors determine adoption of the Internet or not, when people already have a computer at home. By limiting the research to families with computers, our analysis could look beyond the number one obstacle to being online: having the discretionary income necessary to have a computer.

- Our findings reveal that the rush to connect the Web to American homes is happening despite parents' substantial insecurity. In certain ways, the fears parents have revealed to us are similar to the fears parents have expressed during introduction of the movies, broadcast television, and cable TV. But the concerns are not merely repeats of past litanies.
- Parents are nervous about two features of Web programming they haven't seen in broadcast or cable television: its wide-open nature and its interactivity. Parents fear the Web for its unprecedented openness—the easy access by anybody to sexuality, bad values, and commercialism. They also fear the Web for its unprecedented interactive nature—the potential for invading a family's privacy and for adults taking advantage of children. These fears are heightened among many parents because they don't believe they understand the technology well enough to make the best use of it. Yet they believe their children need it.

To ask whether children *really* need to have the Web may be irrelevant, since the Internet is quickly becoming an integral part of the audiovisual environment. In a few years, there may be little real distinction between "television" and "the Internet." With that in mind, policymakers should fund research to help parents learn more about whether they should be scared of the Web at home, why, and what they can do about it. Some key questions:

- Do children's Web-surfing habits reflect their parents' values? Or are the tactics of marketers and other Web forces subverting parents' values, leading kids into areas that challenge, and even try to change, the basic precepts that parents hope their children will have?
- Do children use the Web the way their parents think they do? What are the implications of different sorts of Web use for a child's success in school and in life?
- What steps should parents take to alleviate their fears and channel their children toward Web habits that benefit them?
- Can courses for parents in Web literacy—given in schools, libraries and community centers—help offline and online parents evaluate the costs and benefits of the Web, and of filters and "safe haven" sites that aim to eliminate objectionable material?

These basic questions will become increasingly important as more and more American, and world, families, go online. The best time to start addressing them is now.

THE STUDY AND THE POPULATION

Roper Starch Worldwide conducted the research based on a set of interview questions prepared at the Annenberg School for Communication. The interviews averaged about 17 minutes in length. Through them, we sought to

- delve deeper than previous research into parents' attitudes and beliefs about the Internet and the potential impact this new phenomenon is having on their children and the entire family unit;
- understand how parents who have the Internet at home are coping with the potential uses and abuses of this new technology that is rapidly becoming a fixture in people's lives; and
- begin identifying factors that contribute to, and even predict, why parents in some computer households subscribe to an online service and others do not.

Tables 1 and 2 present basic demographic characteristics of our population of 1,102 parents. All have computers and children aged 8-17. In the tables, the population is divided into those whose households are and aren't online¹. Both groups of parents are predominantly in their 30s and early 40s, white, married, and employed. Most have a yearly household income of \$50,000 or more.

Parents from online homes are somewhat more highly educated and wealthy than parents with home computers that aren't connected to the Web. The main difference relates with respect to computer households making \$75,000 a year or more. While they make up 18% of computer households that are not online, they comprise 32% of the homes that are connected to the Web. Other differences are not nearly as large, however.

While income and education differences between the two are noteworthy, they don't seem to be big or consistent enough to explain why some computer households are online and others are not. Considering that 12% of the online parents and 8% of those not online at home refused to reveal their income bracket, the differences between the two groups may not even be as large as their answers suggest. Later we will see that parents' income and education are not, in fact, major predictors of whether or not a computer household is online. Before doing that, however, we will examine what both groups of parents say and do about themselves, their kids and the online world.

¹ The margin of error for reported percentages based on the entire sample of 1102 is approximately plus or minus 3 percentage points. For reported percentages based on parents with Web connections at home, the margin of error is plus or minus 4 points. For reported percentages based on parents with no Web connections at home, the margin of error is plus or minus 5 points. For reported percentages comparing online and offline parents, the margin of error is plus or minus 6 points. The margin of error is higher for smaller subgroups within the sample.

Table 1: Parents With Children Aged 8-17 and Computers at Home

	Online at Home (N=676)	Not Online (N=426)
	%	%
SEX		
Male	47	46
Female	53	54
AGE		
20-29	4	3
30-44	60	66
45-59	33	28
60 or older	2	2
RACE		
White	86	81
African American	5	8
White Hispanic	5	6
Black Hispanic	1	1
Asian	1	1
Native American	1	1
Other	2	2
MARITAL STATUS		
Married	86	84
EMPLOYMENT STATUS		
NUMBER OF CHILDREN, AGED 8-17		
One	47	3
Two	37	36
Three	11	15 *
Four or more	5	6

* indicates that the row difference is statistically significant. When numbers add up to more than 100%, it is because of rounding error.

**Table 2: Last Education Degree and Household Income of Parents
With Children Aged 8-17 and Computers at Home**

	Online at Home (N=676)	Not Online at Home (N=426)
	%	%
LAST EDUCATION DEGREE		
Grade school or less	—	1 *
Some high school	4	7
High school graduate	25	34 *
Some college	27	29
College graduate	26	19 *
Post graduate	18	10 *
YEARLY INCOME		
Less than \$30,000	8	14 *
\$30,000 - \$49,999	23	29 *
\$50,000 - \$74,999	25	31 *
\$75,000 or more	32	18 *
No answer	12	8

* indicates that the row difference between online and not online is statistically significant.

PARENTS AND THE ONLINE WORLD

An overwhelming majority of “online” and “offline” parents have used computers. 45% in each group consider themselves “intermediate” users, with a somewhat greater percentage of online parents saying they are experts and a somewhat greater percentage of offline parents admitting to beginner status.

The difference between the two groups is much greater when it comes to the ability to navigate the Web. While 96% of the online parents said they had “ever gone online,” only a bit over half of the offline parents said that. And while only 27% of the online parents called themselves beginners, 42% of the offline parents *who have gone online at all* dubbed themselves beginners. This means that 68% of all the offline parents have either never used the Web or consider themselves neophytes with the Internet.

On average, online parents have had the Web at home 1.8 years. They are likely to use the Web at home fairly frequently. 23% said they use it every day, with 30% saying they use it every other day or every few days. Their use of the Web outside the home tends to revolve around work. 60% of online parents said they used the Internet at work “during the past month,” but only 20% said they used it anywhere else outside the home (for example, at the library or a friend’s house).

Offline parents’ relative dearth of Web experience shows up not only in their inability to access it at home but also in their comparatively low use of the Web at work or elsewhere outside the home. Only 32% used the Web at work “during the past month,” and only 16% said they used it anywhere else. Moreover, while 41% of parents with Web connections at home said they used the Web at work at least every few days, only 19% of parents with no Web connections at home reported using the Web at work at least every few days.

Despite their major differences in uses of the Web, there were remarkable similarities between online and offline parents in their attitudes about the Web and in their supervision of children regarding the Web. To understand the similarities, we have to understand that online and offline parents were really made up of different groups of parents with dramatically different attitudes toward the Internet. In fact, each group of online parents has a corresponding group of offline parents that is more similar to it than the other online groups. To see how this works, we look at the views of parents in each segment.

THE VIEWS OF PARENTS FROM ONLINE HOMES

We presented all the parents in our survey with 21 statements about the Internet and children. For each, we asked them whether they agreed strongly, somewhat agreed, somewhat disagreed, disagreed or disagreed strongly. The statements included 8 favorable assertions about the Web, 8 unfavorable assertions about the Web and 5 opinions about the Internet's practical utility for their households. An example of a favorable assertion is "Online my children discover fascinating things they never heard of before." An unfavorable assertion is "I am concerned that my child might view sexually explicit images on the Web." A comment about the Internet's practical utility is "My computer is not powerful enough to handle the Internet well."

We used a computer technique called cluster analysis to discover if all online parents fit one profile in their answers to these statements or if there is diversity among them regarding their attitudes toward the Web. The technique determines whether there are patterns among respondents' in the extent to which certain statements deviate strongly from the average reply ("the mean"), based on a scale in which "agree strongly" is 5 and "disagree strongly" is 1. When the deviation from the mean of responses to a particular statement is strongly positive, it means that the people in the group agreed or agreed strongly with the statement more than most of the people in the sample. When the deviation from the mean of responses to a particular statement is strongly *negative*, it means that the people in the group disagreed or disagreed strongly with the statement more than most of the people in the sample.

As Chart 1 shows, we found three groups of online parents with startling differences in the six statements that deviate most from the mean. We label the groups **online worriers**, **disenchanted** and **gung ho parents**. Table 3 notes their agreement to the statements in terms of percentages. Here are their major characteristics:

Chart 1: Groups of Online Parents Based on Their Views of the Web



TABLE 3: PERCENTAGE OF ONLINE PARENTS WHO AGREE “STRONGLY” OR “SOMEWHAT” WITH STATEMENTS ABOUT THE INTERNET (N=676)

	Total %	Online Worrier %	Disenchanted %	Gung Ho %
Access to the Internet helps my children with their schoolwork.	84	92	53 *	93
Online, my children discover fascinating useful things they never heard of before.	81	87	58 *	88
I am concerned that children give out personal information about themselves when visiting Web sites or chat rooms.	77	88	87	60 *
I am concerned that my child/children might view sexually explicit images on the Internet.	76	86	87	59 *
Children who do not have Internet access are at a disadvantage compared to their peers who do have Internet access.	68	79	22 *	83
Going online to often might lead children to become isolated from other people.	60	88 *	60 *	33 *
The Internet can help my children learn about diversity and tolerance.	60	65	28 *	72
People worry too much that adults will take advantage of children on the Internet.	57	56	56	59
Families who spend a lot of time online talk to each other less than they otherwise would.	48	77 *	47 *	21 *
My children's exposure to the Internet might interfere with the values and beliefs I want to teach them.	42	72 *	44 *	11 *
Children who spend too much time on the Internet develop anti-social behavior.	40	66 *	37 *	16 *
The Internet is a safe place for my children to spend time.	40	39 *	13 *	56 *
The Internet can bring my children closer to community groups and churches.	37	39 *	9 *	50 *
Having Internet access at home is really for children whose parents know a lot about computers.	34	49 *	27	22
It is expensive to subscribe to an Internet service.	29	37	36	17 *
I have better things to do with my money than spend it going online.	28	34 *	52 *	8 *
My family can get access to the Internet from other places so we do not really need it at home.	23	30 *	32	6 *
I often worry that I won't be able to explore the web with my children as well as other parents do.	21	37 *	10	11
I do not mind when advertisers invite my children to web sites to tell them about their products.	21	20 *	9 *	29 *
My children are not interested in having an Internet connection at home.	15	18 *	27 *	6
My computer is not powerful enough to handle the Internet well.	15	20 *	13	10

* means that the percentage is significantly different statistically from the percentages of the two other parent groups in the row.

■ Online Worriers (39% of Online Parents)

These parents are more concerned than those in the other two groups about the effects the Internet might have on their children and their families. Online worriers show above average agreement with the following statements that deal with issues of *values* and *social isolation*

- 72% agree that children's exposure to the Internet may interfere with family values and beliefs.
- More than three out of four (77%) agree that families that spend a lot of time online talk to each other less than they otherwise would.
- 88% agree that going online might lead to the child's isolation.
- Two-thirds (66%) agree it could lead to anti-social behavior by the child.

But these concerns are balanced by a belief in the benefits of connecting to an online service.

These people—60% of whom have had an Internet connection at home for a year or more—are also convinced that there is real value for their kids to having access from home:

- Nearly eight in 10 (79%) agree that children without Internet access are disadvantaged.
- More than 9 in ten (92%) agree access helps children with their homework; 58% agree *strongly* with this statement.
- 87% agree children can learn fascinating and useful things online.

So these parents are highly conflicted. They feel strongly enough about the Internet's inherent importance to their children to go and stay online. But they also express a higher-than-average level of concern that the Internet may interfere with family values, and they worry that their children might expose themselves to the isolating and anti-social side of the Web.

■ Disenchanted (22% of Online Parents)

While online worriers are convinced of both the happy and scary elements of the Web, disenchanted parents are not at all sure of the Internet's value for their kids. Unlike the other two groups with Web experience, disenchanted parents reject the common wisdom that access to the World Wide Web is a near-necessity for students to succeed today.

- 67% disagree that children who do not have access to the Internet are disadvantaged. This makes these parents near polar opposites of the other two groups of parents in online homes. 81% of other online parents *agree*

- Disenchanted parents are even more despairing than the online worriers when it comes to seeing the World Wide Web as a safe haven for exploration. 77% disagree somewhat or strongly that the Internet is a safe place for kids, compared to 54% of the worriers and 30% of the gung ho's who gave that answer. In fact, more than twice as many disenchanted parents than gung ho's and worriers disagree strongly that the Web is safe.

This group's skepticism about benefits that the Web offers to their children is reflected in the parents' attitudes toward the costs involved as well. Even though their income level is comparable to that of the other online groups, disenchanted parents are much less likely to feel that the cost of an online subscription is money well spent. A minority (44%) of these parents agree that it's expensive to subscribe to an Internet service, yet a majority (52%) of this group still says they have better things to do with their money. By contrast, a substantially smaller percentage of the online worriers and gung ho parents—34% and 8%, respectively—say they have better things to do with their money.

Clearly this group is not sold on the inherent value of the Internet experience for their children. The pattern of answers suggests that disenchanted parents keep the Web more because they think it has become a requirement for up-to-date families in the late twentieth century than because they think it will bring great benefit.

■ Gung Ho Parents (39% of Online Parents)

Online worriers and disenchanted parents together comprise 61% of those with Web connections at home. Gung ho parents, who are highly positive about the Web, comprise the other 39%. What places these people in a separate group is not their strong belief in the Internet's positive effects; online worriers respond that way, too. Rather, gung ho parents stand out because in large numbers they reject nearly all statements about the Internet's alleged negative effects.

- 78% disagree that their children's exposure to the Internet might interfere with the values and belief they want to teach their kids. That contrasts with 18% of the worriers and 46% of the disenchanted parents who disagree.
- 68% disagree that going online takes away from family time—in direct opposition to the 77% of the online worriers who *agree* with this statement. 58% disagree that surfing the Web will isolate children, and 69% reject the idea that it could lead to anti-social behavior.
- Gung ho's are not wealthier than other online parents. Yet, in contrast to the disenchanted parents, 83% disagree that they have better things to do with their money; 52% disagree *strongly*, confirming their stand that the Internet offers value to children.

Gung Ho parents have had an online connection longer than other online parents. (51% have been connected from home for two years or more, compared to only a third of either of the other two groups.) They are more likely themselves to go online every day from work, and somewhat more likely to rate themselves as advanced or expert users. These parents seem to have assimilated the Internet into their homes as a benign, beneficial new technology.

Parent Supervision Regarding the Internet

We found that the different parent groups' beliefs about the Internet's influence associated with statistically significant differences in their actions. Online worriers were consistently more likely than the others to supervise their children—and to exercise the strictest supervision. Disenchanted parents were next, with gung-ho parents coming last. None of these groups' actions was so unusual, however, as to alter our basic conclusions about how online parents supervise their children regarding the Internet. Consequently, in the interest of brevity and clarity we focus in this section collectively on the respondents with Web connections at home.

In devising the survey, we recognized that parents' approaches to their children regarding the Web might depend on the age and/or sex of a particular child. Early in the interview we asked parents for the name, sex and age of their 8-to-17-year-old with the most recent birthday. A large number of the questions about child activities and parent supervision related specifically to that youngster.

47% of the children named were girls and 52% were boys (1% of the respondents refused to tell us). 49% of the children spanned ages 8 to 12, and 51% fell into the 13 through 17 category. The average age was 13.2.

As it turns out, the child's sex does not play a statistically significant role in parents' answers. Age sometimes does. In parents' reports, younger and older children differed statistically when it came to whether or not they ever went online; 93% of the older children have done it, while a smaller (but still very large) 81% of the younger ones have gone on the Web. Looking at parents' reports of the children who did go online from home, there were no age-related statistical differences in usage. 76% of them went online during the past month, 50% went online more than 10 days during that time, and 12% did it every day.

As for going online *out of* home, 36% of the parents of younger children said their kids had done it "during the past month," while 48% of the parents of older children reported that they had used the Web outside the home. Table 4A indicates that school was the most popular location, with friends' houses second and the public library third. Table 4B reveals that doing homework and e-mail were the most common tasks for the older kids, while playing games came first for younger ones, with homework second.

Note that more than half of the parents of kids in each age category mentioned conducting research and doing homework as the most common activities. Parents of both age groups clearly see school-related pursuits as central to their kids' online lives. Sociability—email and chat rooms—also take center stage, with 29% of the parents of younger children and 53% of the parents of older children mentioning it. "Buying things," creating a Web site, and listening to music received few mentions among the two most popular activities on line.

Most parents are quite sure they keep up with their children's Web activities, both in and out of home. As Table 5 shows, the percentage of confident parents did change with the child's age and whether the online computer was at home or out-of-home. Both groups of parents were more likely to feel confident of their knowledge if the Web activities were in- rather than out- of the home. And parents of the younger children were more likely than parents of older ones to believe they know where their kids go in the virtual world.

Table 4A: From Where Has the Child With the Most Recent Birthday Gone Online Outside of Home?*

(Asked of parents with online connections at home who say that the child has gone online outside of home in the past month)**

	Age 8-12 (N=115)	Age 13-17 (N=173)
	%	%
School	76	83
Public Library	14	12
At a Job	1	3
A Friend's/Relative's House	20	28
Local College/College Libraries	2	-
Community Services/Museum	-	-
Church	-	-
Other Mentions	2	-
Don't Remember	1	1

** None of the row differences is statistically significant. Numbers don't add to 100% because multiple answers were acceptable.

Table 4B: What Two Activities Does the Child With the Most Recent Birthday Most Do Online?

(Asked of parent with online connections at home who says the child goes online at home)

	(N=259)	(N=332)
	%	%
Do Homework	27	38 *
Conduct Research	26	22
Send and Receive E-Mail	18	28
Play Games or Puzzles	32	14
Participate in Chat Rooms	11	25 *
Surf to Discover Things		
He/She Never Heard of Before	12	12
Read Online Magazines or Newspapers	6	5
Create a Web Site About Her/Himself or Hobby	5	4
Listen to Music	2	6 *
Visiting Museums or Cultural Sites	2	2
Buy Things	1	3
Participate in Community or Religious Groups	-	1
Conduct Business	-	-
Other Mentions	6	3
Don't Know	7	3

* indicates that the row difference is statistically significant. Numbers don't add to 100% because multiple answers were acceptable.

But, as Table 5 also indicates, the sense by most parents that they understand their children goes beyond their assertions about their Web habits. Most parents also state that they talk to their children frequently or sometimes about their online activities, and most say they trust their kids to do the right thing on the Web. What's more, when asked whether they argue with their child about their Internet use, a huge percentage said no.

An obvious question arises: If so many of these parents are knowledgeable, trusting, communicative and non-combative with their kids, why are so many of them worried about the Web and their children? The answer seems to be that while parents trust their children, they do not trust the Web. Perhaps from news stories (see Part II of this report), perhaps from discussions with other parents, perhaps from personal experience, they have come to believe that a substantial part of the Internet has the potential of invading children's privacy while preying on them sexually and commercially.

Table 5: Parents Confidence in, Trust in and Discussions with Children about Being Online
(Asked of online parents regarding the child with most recent birthday)

	Age 8-12 (N=319)	Age 13-17 (N=357)
	%	%
CONFIDENCE ABOUT CHILD'S ONLINE ACTIVITIES OUT OF HOME		
Very confident	75	55*
Somewhat confident	19	33*
CONFIDENCE ABOUT CHILD'S ONLINE ACTIVITIES AT HOME		
Very confident	86	69*
Somewhat confident	8	26*
CHILD TALKS TO PARENT ABOUT ONLINE ACTIVITIES		
Frequently	54	46*
Sometimes	23	37*
TRUST OF CHILD'S ONLINE BEHAVIOR		
Complete	58	61
Some	31	34

* indicates that the row difference is statistically significant.

Table 6 indicates the extent to which the parents set rules for their specific child's navigation of cyberspace. A consistently higher percentage of parents noted rules for younger children than older ones. Most parents of both groups said they have rules regarding particular sites to visit, the time of day for going online, the amount of time spent online, and what the child can do online. Parents of the young children are more likely than parents of the older kids to require the child to have an adult around when going online. Going online only for schoolwork is a rule that the great majority of parents of both age groups reject, perhaps because they consider it too constraining for their children.

Table 6: Types of Rules Parents Set for a Child When the Child Goes Online
 (Asked of parent regarding child with most recent birthday who goes online at home)

	Age 8-12 (N=259)	Age 13-17 (N=332)
	%	%
The sites (child) visits online	84	71 *
The time of day or night he/she is allowed to go online	84	68 *
The kind of activities the child performs online	78	70 *
The amount of time spent online	63	55
Going online only with an adult, be it from home or outside of home	73	29 *
Being online only at home	49	35 *
Only going online if it is relevant for schoolwork	30	21 *

* indicates that the row difference is statistically significant. Numbers don't add to 100% because multiple answers were allowed.

Table 7 indicates the extent to which the parents use certain methods “to protect their children from negative influences of the Internet.” We asked the respondents to think of all their children when they gave answers, so the age of the specific child that some questions asked about does not apply here. Overwhelmingly, parents told us that they do set rules and that they “keep an eye on what the child is doing” when he/she is online. We found, however, that parents are much less likely to say they get involved in restrictive regulations that require direct intervention in their kids’ Internet use. Perhaps because of ignorance, they are also unlikely to use computer technology to control their children’s Web-surfing behavior. Still, a substantial minority of the online parents—31%—did say they use a Net Nanny-type program that guards children’s access to sites.

Table 7: Methods Parents in Online Households Use to Protect Their Children from Negative Influences on the Internet

(Asked of online parents)

	Age 8-12 (N=319)	Age 13-17 (N=357)
	%	%

answers were allowed.

THE VIEWS OF PARENTS FROM HOMES NOT ONLINE

Parents from computer households without the Web worry about their kids' use of the Web outside the home. 43% of parents of younger children said their children go to the Web outside the home. This is the same percentage as online parents. When it came to older youngsters (ages 13-17), the percentage of offline parents saying their kids use the Net outside home is actually higher than the reports by online parents—61% to 48%.

As a comparison between Tables 4 and 8 indicates, the reports by parents of where their children go online are quite similar. We did not ask parents without the Web what their children most like to do online. That is unfortunate because, as a comparison between Tables 5 and 9 shows, offline parents are similar to online parents in their confidence that they know what their children are doing on the Net outside the home. And, as with online parents, the sense by most of these parents that they understand their children goes beyond assertions that they know the kids' Web habits. Most offline parents also state that they talk to their children frequently or sometimes about their online activities, and most say they trust their kids to do the right thing on the Web. What's more, when asked whether they argue with their child about their Internet use, virtually all said no.

Table 8: From Where Has the Child with the Most Recent Birthday Gone Online Outside of Home?

(Asked of parents who do not have online connections at home and who say the child has gone online outside of home in the past month)*

	Age 8-12 (N=96)	Age 13-17 (N=122)
	%	%
School	72	75
Public Library	15	20
At a Job	7	6
A Friend's/Relative's House	18	27
Local College/College Libraries/Community Services/Museum	2	1
Church	-	1
Don't Remember	-	-
Other Mentions	-	-

* None of the row differences is statistically significant. Numbers don't add to 100% because multiple answers were acceptable.

Table 9: Parents Confidence in, Trust in and Discussions with Children About Being Online

(Asked about child with most recent birthday of parents whose households do not have online connections)

	Age 8-12 %	Age 13-17 %
CONFIDENCE ABOUT CHILD'S ONLINE ACTIVITIES OUT OF HOME**		
	(N=226)	(N=200)
Very confident	69	56*
Somewhat confident	22	32*
CHILD TALKS TO PARENT ABOUT ONLINE ACTIVITIES***		
	(N=96)	(N=122)
Very confident	48	47
Somewhat confident	25	31
TRUST OF CHILD'S ONLINE BEHAVIOR***		
	(N=96)	(N=122)
Complete	54	61
Some	39	37

* Indicates that the row difference is statistically significant.

** Asked of all offline parents.

*** Asked of parents with child who goes on the Web outside the home.

We asked parents without a Web link at home whether they think the child with the most recent birthday would be likely to use a home connection if the household had one. 88% answered yes, and only 6% said they would prohibit the child from doing so. We then asked the other 94% about rules they might have for those children. Summarized in Table 10, their answers very much parallel those of parents with the Web at home. That is, the offline parents would embrace rules that limit the time kids spend online, the times of day they go online and the kinds of activities they do online. The major difference between two groups relates to the percentages of parents that accept these guidelines. A higher proportion of offline than online parents imagines a Web household where the rules are very tough.

**Table 10: Types of Rules Parents Would Set For a Child
If the Child Could Go Online at Home**

(Asked about the child with the most recent birthday of parents who do not have online connection at home but would allow the child Internet access if they had a home connection)

	Age 8-12 (N=212)	Age 13-17 (N=194)
	%	%
The amount of time spent online	96	94
The kind of activities the child performs online	95	95
The sites (child) visits online	96	93
The time of day or night he/she is allowed to go online (for example, after homework is done)	94	91
Going online only with an adult be it from home or outside of home	87	65 *
Being online only at home	57	41 *
Going online only if it is relevant for schoolwork	44	41

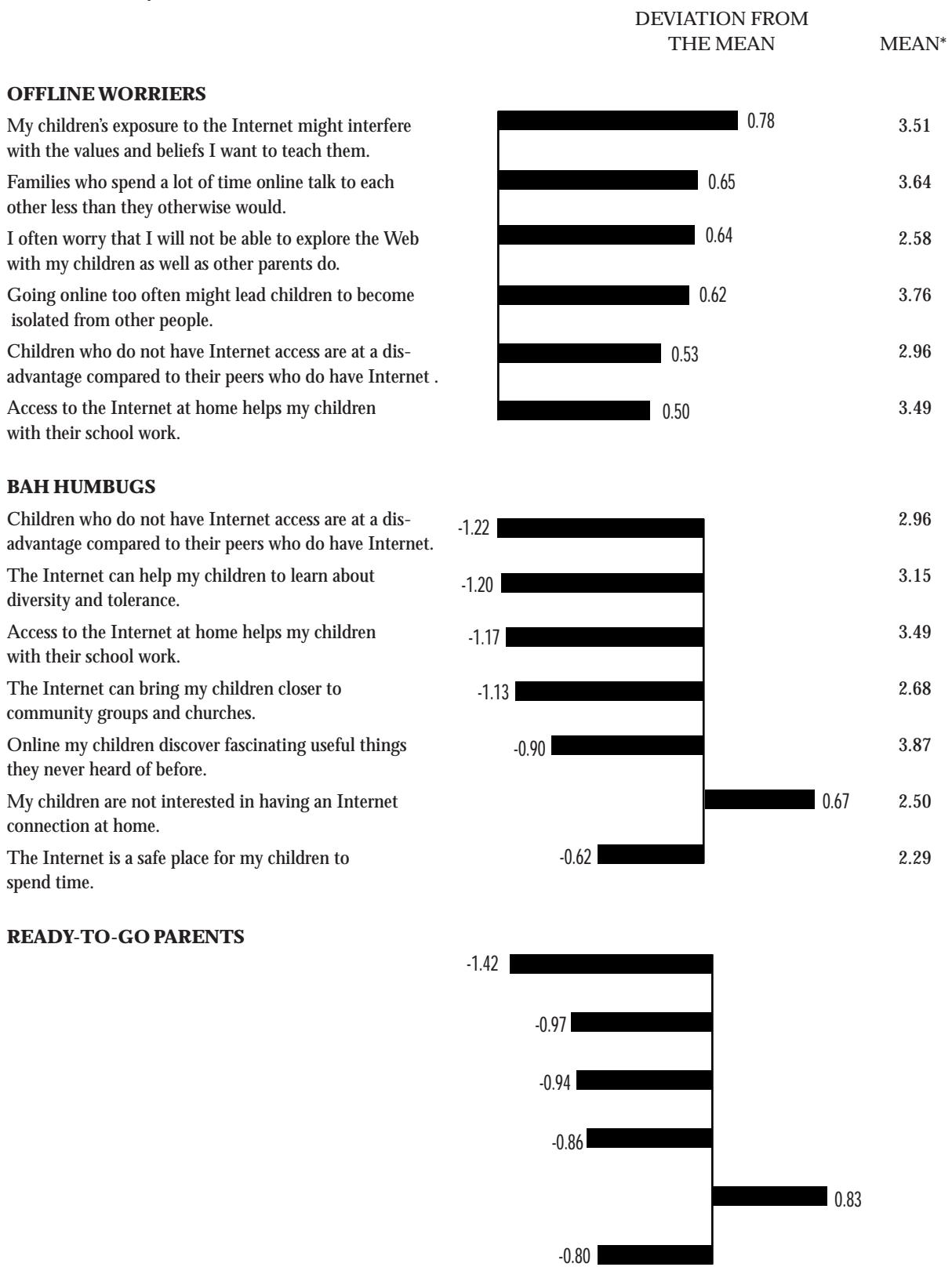
* indicates that the row difference is statistically significant. Numbers don't add to 100% because multiple answers were allowed.

The Beliefs of Parents Without Home Connections

When it comes to expressed beliefs about the Web, a higher percentage of parents without the Web at home are pessimistic compared to those with the Web at home. Offline parents are also less likely to agree strongly (as opposed to agreeing "somewhat") regarding the good points of the Web, and they are more likely to disagree strongly (as opposed to disagreeing "somewhat") regarding the bad aspects of the Web.

However, as with the online parents, our cluster analysis found three dramatically different groups among the offline parents. As a comparison between Charts 1 and 2 shows, each group has a corresponding group of online parents that is similar in beliefs about the Internet and the family. Table 11 shows that responses to the 21 statements varied dramatically depending on the segment to which parents belong. Further, as comparisons between Charts 1 and 2 and Tables 3 and 11 reveal, offline parents had a higher probability of agreeing with parents of their corresponding online group than with offline parents of other groups.

Chart 2: Groups of Parents Not Online Based on Their Views of the Web



* This is the mean (average) of responses to the statement by the entire offline sample. See text.

**TABLE 11: PERCENTAGE OF OFFLINE PARENTS WHO AGREE
"STRONGLY" OR "SOMEWHAT" WITH STATEMENTS ABOUT THE INTERNET
(N=426)**

	Total %	Offline Worrier %	Bah Humbug %	Ready To Go %
I am concerned that my child/children might view sexually explicit images on the Internet.	82	95*	83 *	63 *
I am concerned that children give out personal information about themselves when visiting web sites or chat rooms.	81	92 *	79 *	
Going online too often might lead children to become isolated from other people.	70	91*	68 *	44 *
Online, my children discover fascinating, useful things they never heard of before.	65	76	39*	79
My children's exposure to the Internet might interfere with the values and beliefs I want to teach them.	60	88*	68*	13 *
People worry too much that adults will take advantage of children on the Internet.	59	66	51 *	60
Families who spend a lot of time online talk to each other less than they otherwise would.	59	79 *	60 *	30*
My family can get access to the Internet from other places so we do not really need it at home.	58	55	71*	49
I have better things to do with my money than spend it going online.	54	64	65	30*
Access to the Internet helps my children with their schoolwork.	53	65	22*	68
The Internet can help my children to learn about diversity and tolerance.	47	58	13*	68
Children who spend too much time on the Internet develop anti-social behavior.	45	59 *	46 *	24 *
Children who do not have Internet access are at a disadvantage compared to their peers who do have Internet access.	43	60	7*	56 *
It is expensive to subscribe to an Internet service.	39	43	44	29*
Having Internet access at home is really for children whose parents know a lot about computers.	38	55 *	31 *	21 *
The Internet can bring my children closer to community groups and churches.	32	37 *	4 *	54 *
My children are not interested in having an Internet connection at home.	31	30*	45 *	19*
My computer is not powerful enough to handle the Internet well.	29	31	22	34
I often worry that I won't be able to explore the web with my children as well as other parents do.	29	49*	11 *	19 *
The Internet is a safe place for my children to spend time.	26	21*	9 *	51*
I do not mind when advertisers invite my children to Web sites to tell them about their products.	19	21	10 *	27

* means that the percentage is significantly different statistically from the percentages of the two other parent segments in the row. Bold numbers signify that the percentage is significantly different statistically from the percentage of the corresponding segment of online parents in Table 3.

Here are the offline groups and their major characteristics:

■ Offline Worriers (41% of Offline Parents)

Comparing Charts 1 and 2, we find that online and offline worriers share four of the six statements that most signal the personality of their groups. The statements reflect a bundle of concerns about the Web.

- 88% of the offline worriers (and 72% of the online worriers) agree that children's exposure to the Internet might negatively impact family values and beliefs.
- 79% of the offline worriers (and 77% of the online worriers) agree the Internet will steal family time.
- More than nine in 10 (91%) of the offline worriers (88% of the online ones) agree that the Web might isolate a child.
- 49% of the offline worriers (and 37% of the online ones) fear they won't be able to explore the Web with their children as well as other parents do.

At the same time, the offline worriers, like their online counterparts, do have positive things to say about the Web. Among the statements most deviating from the mean answers is the belief that children who do not have Internet access are at a disadvantage compared to their peers who do not have the Internet. 60% agreed strongly or somewhat with that sentiment, and 65% agreed strongly or somewhat that Internet access helps their children with their school work.

■ Bah Humbugs (30% of Offline Parents)

Like the online disenchanted parents, this group does not accept the hype about the wonders of the Web. Bah humbugs reject both that the Net is a necessary tool for school and they reject the idea that people coming together online is going to make this a better world. As with the worriers, what bah humbugs say that most deviates from the mean is remarkably similar to their online counterparts.

- 79% of these offline skeptics (and 66% of the online ones) disagree that children that do not have Internet access are disadvantaged in comparison to their peers.
- 75% of the bah humbugs (and 74% of the disenchanted) disagree that it will bring their kids closer to community or church. Both groups also disagree more strongly than the other parent segments that the Web is a safe for kids and that on it children can discover fascinating, useful things.
- 63% of the bah humbugs (and 50% of their online counterparts) disagree that the Net is a tool for teaching about diversity and tolerance—while disagreement of the other offline and online clusters is closer to 20% and 10%, respectively.
- Only 22% of the bah humbugs accept the notion that “access to the Internet helps my children with their school work,” compared to about 66% of other groups of offline parents. (54% of the disenchanted agree, but their proportion is still much lower than the approximately 90% of other online parents who acknowledge the Web's help with homework.)

On one of its six most characteristic statements, bah humbug's skepticism takes a somewhat different turn from the disenchanted parents. Even as they are paying for the Web, 21% of the disenchanted parents agreed strongly that "I have better things to do with my money than spend it on the Web." While 39% of the bah humbugs agreed strongly with the statement, that is not very different from the proportion of offline worriers who expressed the sentiment. Rather, what makes the bah humbugs stand out among the offline parents is their strong agreement that "my children are not really interested in having an Internet connection at home." 27% of them agree strongly with the proposition compared to 12% of the offline worriers and 7% of the third offline group—the one we call ready-to-go parents.

■ Ready-To-Go Parents (29% of Offline Parents)

We named this segment of offline parents ready-to-go's because the beliefs they expressed reflect a strong favorable attitude toward having the Web in the home. In fact, the statements that most distinguished it from the two other offline groups create a profile that is uncannily similar to the gung ho group of online parents.

A comparison between Chart 1 and 2 shows that the gung ho's and ready-to-go's share every one of the six top-ranked statements, and in almost the same order. Like the gung ho group, ready-to-go parents don't accept the common wisdom that the Internet might hurt their kids or families, and they don't begrudge the money it costs to subscribe.

- Only 13% of ready-to-go parents (and only 11% of gung -ho parents) agree that exposure to the Internet might interfere with their family values and beliefs.
- A relatively small 44% of ready-to-go's (and 33% of gung-ho's) believe going online too often might lead children to become isolated from other people—compared to 91% of offline worriers, 88% of online worriers, and over 60% of both groups of skeptics.
- 54% of ready-to-go's agree that the Internet can bring children closer to community and churches—far higher than any other offline group and second only to the gung ho group in the proportion that takes this position.
- 51% of ready-to-go's say that the virtual world is safe. Here the proportion is far higher than any other offline or online group, except for the 56% of gung ho parents who feel that way.
- 61% *disagree* strongly or somewhat that they have better things than the Web on which to spend money. The proportion is more than three times higher than the percentages of other offline groups that answered that way. It is smaller than the 84% of gung-ho's who disagreed, an indication that while a solid majority believes that a home Internet experience offers real value, a large number of them is still mulling it over.

Nevertheless, the similarity in attitudes between the gung ho and ready-to-go parents is remarkable, and it begs asking why many of these people (at least the aforementioned 61%) aren't connected already. In fact, the similarities between the other two online and offline groups also leads one to wonder what factors drive some parents in computer households to connect their families to cyberspace while others do not.

FACTORS PREDICTING WHETHER HOUSEHOLDS WITH COMPUTERS HAVE THE INTERNET

To answer, we turn to the results of our discriminant analysis. It sought to determine the factors that predict whether or not households with computers have online access at home. We did not find their household income, education, computer ability, their spouse's education or any other demographic variables to be major predictors of online connections when the family already has a computer.

Instead, the discriminant analysis found that the best predictors were 5 variables that describe the parent's experience with the Web outside the home and reflect their beliefs about the practical necessity of the Web in the home. Together, the following variables predict 38% of the variance—a substantial amount with these sorts of data.



The online and offline groups tended to give very different answers to this question. 96% of the parents with online connections at home told us that they have gone on line somewhere. By contrast, only 54% of the parents with no online connections at home said they have ever used the Internet.

As seen in Table 12, this variable is the highest predictor of the set. It suggests that parents' lack of experience with the Web *outside* the home is the most important single factor differentiating a computer household without the Web from one with it. Unfortunately, we didn't ask the parents with home Web connections whether they had used it consistently outside the home before they had decided to introduce it domestically. That makes it impossible to definitively suggest a causal interpretation that relates experience outside the home to Web links inside.

Table 12: Variables Correlating Most With Having an Online Connection at Home

Variable	Correlation*
Have you ever personally gone online, that is, used the Internet, the World Wide Web, and/or e-mail	.697
My family can get access to the Internet from other places so we do not really need it at home	-.593
I have better things to do with my money than spend it going online.	-.436
Access to the Internet at home helps children with their school work.	.347
Children who do not have Internet access are at a disadvantage compared to their peers who do not have Internet access.	.325

* These are pooled within-groups (online, not online) correlations between discriminating variables and standardized canonical discriminant functions. Variables are ordered by absolute size of correlation with function.

The variables together account for 38% of the variance of having or not having an online connection at home. Each correlation listed is a measure of how well the variable associates with the statistical function that explains 38% of the total variability between the two groups. The first statement, then, is the strongest variable in a discriminant function that is predicting 38% of the total variability between the two groups.

A negative correlation means that the answer was inversely related to having an online connection. So, for example, people who agree with the statement “My family can get access to the Internet from other places so we do not really need it at home” are less likely to have online connections at home than are people who disagree with it.

We do have evidence from questions we asked that a much higher percentage of online than offline parents use the Web at work. While 62% of online parents went online at work “in the past month,” only 34% of the offline parents said they did that. Moreover, while one out of every three online parents said they connect to the Web on the job every day or every other day, only one of seven offline parents said that. While still not causal, these findings lend support to our suggestion that it is the parent’s *lack* of experience using the Internet outside the home that associates with a household’s not being online.

The next four key predictors of online and offline households relate squarely to the way online and offline parents weigh the Internet pragmatically in their families’ lives.

■ **Factor 2: “My family can get access to the Internet from other places so we do not really need it at home.”**

58% of parents in offline households agree strongly or agree with this statement. Only 23% of online parents do. What we have here are fundamentally different perspectives about the practical necessity of bringing the Web into the home. Offline parents are aware that the Web is available for their children in other places. In fact, half of these parents say they know their child has gotten on the Internet in school, friends’ homes, and public libraries. These data suggest that parents in computer homes without the Web see occasional use as sufficient and prefer not to bring it home.

■ **Factor 3: “I have better things to do with my money than go online”**

54% of offline parents say they have better things to do with their money than spend it going online. That's versus 60% of online parents who disagree that there are better uses for those online subscription fees.

This response adds a second practical dimension to the calculus of decisions that online and offline parents make. The issue here does not seem to be one of basic affordability. Although parents in online households are somewhat more likely than those offline to have incomes above \$75,000 a year, the socioeconomic positions of both groups of computer owners are not that different. The key phrase here is “better things.” In the scheme of things, the Internet simply does not seem worth the price for offline parents.

■ **Factor 4: “Access to the Internet at home helps children with their schoolwork.”**

■ **Factor 5: “Children who do not have Internet access are at a disadvantage compared to their peers who do have Internet access.”**

These two final factors highlight an additional part of the Internet equation that many offline and online parents consider—the specific utility for their children. Like the third factor, these stand out not so much because offline parents overwhelmingly disagreed with them. Rather, they popped up as predictors because parents seemed so overwhelmingly to accept them while offline parents were much less united.

84% of online parents agreed that “access to the Internet at home helps children with their schoolwork”; of those, 57% agreed strongly. Contrast that with the 53% of offline parents who agreed with this statement and the 24% who agreed *strongly*. Similarly, more than two-thirds (68%) of online parents agreed that “children who do not have Internet access are at a disadvantage compared to their peers who do have Internet access.” Offline parents are split; 43% agree, 43% disagree.

The different responses to these statements reinforce the suggestion that parents assess the practical value of the Internet experience for their family in making the decision about whether or not to be online. Strong doubts about the Web play a key background role in this, but don't predict the outcome. That is because, as we have seen, both online and offline parents carry similar fears and cynicism about the Web's role in their children's lives.

In the face of concerns about the Web and kids, parents conduct a cost benefit analysis that weighs the benefits they perceive against their assessment of what their families would lose by not having it. Our data begin to suggest that it is the parent's lack of experience using the Internet outside the home that may make them more likely to downplay its utility in the face of worries about children and the Internet. By contrast, worried parents who have had repeated Web experience at work, in friends' homes or at public libraries may decide that despite their fears an online connection is on balance useful for their family.

But why do disenchanted parents continue their home links? Inertia may be one reason. It may be, too, that they may see the technology as a new kind of social leveler. That is, they may feel that while it isn't what it's cracked up to be, the Internet nevertheless is necessary if they and their children are to keep up with The Joneses.

CONCLUDING REMARKS

The overview at the start of this report raises a number of policy issues that flow out of our findings. Here it may be useful to bring up three research directions that we are pursuing in order to fill holes in our understanding of way families deal with the new Internet realities.

- **Parents' experiences with the Web:**

parents' needs as opposed to those of their children? And why do disenchanted parents keep the online connection at home?

- **What children do and say:** One of the startling findings of this study is how confident parents are that they know what their kids are doing online, at home and out. Well, is their confidence justified? What do youngsters tell us about their Web habits, and how does that compare to what their parents tell us? Compared to online worriers and disenchanted parents, are gung ho parents more or less likely to predict what their kids say? What do the similarities and differences tell us about tensions and misunderstandings between the generations—and about trends in Internet usage?

In this connection, we must recognize that a strong majority of both “offline” and “online” parents are worried or skeptical about the Web’s influence on their children. Does this skepticism and concern influence the ways their children act toward the Web? Are children with these parents likely to go to sites that are different from children whose parents are gung ho about the Web—and are the kids likely to get less enjoyment out of it? If so, teachers, librarians and even Web site producers might take the parents’ different attitudes into account when helping kids with the Web.

- **The Web and family lifestyles:** How does the Web fit into the entire intricate pattern of family activities? Do family members see it seen as leisure, work, or a combination of the two? How are the rules that parents said they are setting down actually being implemented? Do parents with different beliefs about the Web’s consequences act differently when it comes to laying down and enforcing rules? Do the children of gung ho, online-worrier and disenchanted parents adopt their parents’ perspectives on the Web? Do they act differently toward the Web as a result of it?

There is much to puzzle out, and the answers are likely to change over time. We look forward to expanding on this research in the months to come.

PART 2: THE VIEW FROM THE PRESS

By **Joseph Turow, John Bracken and Lilach Nir**

Annenberg School For Communication

University of Pennsylvania

With the assistance of

Cory Allen, Mikaila Brown, Laura Ducceschi,

Talya Gould, Rachna Patel, Brenda Sheth, Lynda Tran

Annenberg School For Communication

University of Pennsylvania

OVERVIEW

"Your children need the Internet. But, if they do go online, be terrified."

This is the message that the American press presents to parents, according to the Annenberg Public Policy Center's examination of all the articles in twelve major newspapers that mentioned the Internet and the family, parents or children from October 15, 1997 to October 15, 1998.

We did find examples of articles that tried to help families assess the problems and potential of the new Web world in a reasoned way. Overall, though, the Web presented the Internet as a Jekyll-and-Hyde phenomenon over which parents are left to take control with little community backup.

- Sex crimes regarding children and the Web were featured in one of every four articles. The most common crime topics were sexual predators and child pornographers.
- Disturbing issues relating to the Web and the family showed up in two of every three articles surveyed. The problems portrayed were rather narrow—mostly sex crimes, pornography, and privacy invasion.
- Benefits of the Web for the family came up in half the total articles, but there was little overlap with the negative pieces. The dangerous world of the Internet and the friendly, useful picture of cyberspace showed up in different articles and were unrelated to each other.
- When articles quoted people about the Internet and the family, many more sources stressed the dangers of the Web than its benefits. Government officials and law enforcement officers spoke most frequently, and most negatively, about the Web's influence on children and the family. Educators were mostly positive, but they showed up only rarely.
- Because of the focus on crime, reporters looked often to the government and criminal justice system for remedies. The solutions they represented were typically either piece-meal (for example, arresting an individual child-pornography suspect) or muddled and tentative (such as court-voided legislation to protect children from Web indecencies).
- Journalists placed the burden of dealing most immediately with Web problems on parents. Articles suggested a wide range of actions for them—monitoring their children's Web activities, going online with their kids, looking for good Web sites, using filters to block bad ones. Unfortunately, the articles did not depict teachers, librarians or neighborhood groups as resources for support. At the everyday level, the press showed parents facing a useful but scary Web virtually alone.

The press' portrayal of the Internet is particularly significant because it directly reflects the results of the national survey presented in Part 1. As we saw, the great majority of American parents with computers in the home is conflicted about the Web. Parents feel it's necessary but they fear it.

Most likely, this split view gets constructed in the press because of journalists' need to fill separate news holes—those dealing with news as conflict and those dealing with “news you can use.” Journalists separately pick up and amplify conflict-based and “news-you-can-use” topics regarding the Web. News consumers are alarmed by and interested in the concerns that the press portrays. Journalists, noting this, give them more of what becomes the conventional wisdom about the Internet through this process.

Are there alternatives?

- Instead of merely piling on instances of crimes on the Web, the press can investigate the prevalence of these crimes to give the public some perspective on the matter.
- Instead of placing so much emphasis on problems of a violent or sexual nature, the press can also highlight issues of equity, race, class and commercialism on a national and global basis. There is a world of socially critical issues regarding the Internet that journalists are hardly covering.
- Instead of focusing overwhelmingly on government officials and the police for institutional solutions to Web problems, the press can investigate whether and how teachers, parents, children, librarians, and community groups are working together to manage both the problems and opportunities of the Web.

The Internet is here to stay. So is the family. At this formative stage in the family's relationship with the Internet, it is critical for journalists to help parents and children evaluate the new world in ways that help them best make sense of their lives and their society.

THE STUDY AND THE METHOD

Our investigation was a content analysis of articles in twelve daily U.S. newspapers from October 15, 1997 through October 15, 1998. Listed in Table 13, six of the papers are among the nation's ten largest in circulation, and the other six rank between fortieth and fiftieth in circulation. In locating articles for the analysis, we decided that for our purpose a "family" was at least one parent with at least one school-age child. We then conducted a search on the Lexis/Nexis database for every article in those papers during the year that (1) mentioned the Internet, AOL, Web, or online and (2) included the words family, families, child, children, parent, parents, youth or teens. The search yielded 668 relevant articles.

Table 13: The Newspapers in the Study

Newspaper	Number of Articles	% of Total
USA Today	30	4.5
New York Times	73	10.9
Los Angeles Times	162	24.3
Washington Post	85	12.7
Chicago Tribune	53	7.9
San Francisco Chronicle		
Fort Worth Star-Telegram	58	8.7
Louisville Courier-Journal	29	4.3
Seattle Times	68	10.2
Omaha World-Herald	23	3.4
Indianapolis Star	25	3.7
Richmond Times-Dispatch	32	4.8
Total	668	100

We designed a questionnaire to answer two broad questions about the articles:

- 1 What issues do the papers raise about the Internet and the family?
- 2 What kinds of people speak about the Internet and the family in the articles, and what do they say?

Our questionnaire explored these questions in several ways. Regarding the issues, we asked about where the papers placed the articles, what topics the articles raised, whether the topics centered on problems or benefits of the Web for the family, whether the articles discussed attempts at solutions

to the problems, and more. Regarding the people in the articles, we noted their occupations, the organizations for which they worked, what they said about the Web, whether it was a problem or a benefit, whether they had solutions for the problems, and more.

We divided the entire set of 668 articles among eight University of Pennsylvania students whom we had trained to use the questionnaire and tested for reliability. They read and coded the articles according to the questionnaire. We entered the resulting data into a computer for analysis.

THE TOPICS IN THE ARTICLES

As Table 14 notes, when articles mentioned the Internet and the family, the overwhelming majority—97.2%—did so in terms of the problems and/or benefits of the Web. About two-thirds of the pieces described problems and about half related the Web's benefits. These discussions were quite separate, however. As Table 14 notes, only 16% of the pieces mixed problems and benefits.

Table 14: Were Benefits or Problems Discussed in the Articles? (N=668)

	%
Benefits only	33.2
Problems only	47.8
Mixed problems and benefits	16.0
Neither benefit nor problem	2.8

Discussions of benefits in the articles were so subtly varied that we found they could not be coded reliably into particular categories. Consequently, we divided the benefits into two broad categories, those that relate to social effects of the Web and those that relate to the Web's psychological effects. We defined social effects as those that impact on activities between people; using email to keep in touch with relatives is an example. We defined psychological effects as those that impact on the *mental*/activities of people; a Web site that helps a child read or improves the knowledge of family members are instances of psychological effects.

Table 15 presents the benefits. The numbers add up to more than 100% because coders reliably found up to two benefits in the 331 articles that noted a benefit. The table indicates that the Web's utility was noted much more often in relation to children than in relation to the family as a whole. Psychological utility received more mentions than social utility.

Table 15: The Benefits Mentioned in the Articles (N=331)*

	%
Psychological effects on children	55
Social effects on children	33
Social effects on the family	25
Psychological effects on the family	15
Other	5

* The numbers exceed 100% because some articles mentioned more than one benefit. See text.

Unlike the broad and scattered discussion of the Internet's benefits, discussion of the Web's problems centered on a small number of rather specific dangers. Table 16 presents the problems. Again, the numbers add up to more than 100% because we found that the coders could reliably record up to two problems in the 429 articles that noted one or more of them. A number of startling points emerge in the table.

First, sex and sex crimes relating to the Web and children received much attention, making up 53% of all the problems. Second, a large number of articles discussed Web sites that are improper for children because they promote activities that children should not be doing, like drinking, smoking, and drugs. Third, articles were so fixated on outside influences preying on children for purposes of sex, improper activities and privacy invasion that all other issues mentioned regarding the Internet and the family appeared in only 5% of the articles. These other issues included parents' management of children's Internet time; supervision of Internet use at home and school; commercialism and the Web; the Web and parents' careers; hate groups on the Web; income divisions between Web haves and have-nots; and negative social and psychological implications of the Web for the family. Considerations of race and the Web—problems, benefits, or just facts—were mentioned only seven times in our entire sample.

Table 16: The Problems Mentioned in the Articles (N= 429)*

Web site material that is improper for children	29
Adults preying on children through the Web	21
Pornography	18
Privacy issues	17
Child pornography	14
Difficulty supervising kids at home	9
General dangers of the Web	7
Not having the Internet	4
All other categories (see text)	5

* The numbers add up to more than 100% because some articles mentioned more than one problem. See text.

THE PEOPLE QUOTED IN THE ARTICLES

We asked how many people journalists quoted about problems and benefits of the Web, who they were and what they said. Going through the 668 articles in our sample, we found 663 people whose comments the articles cited. Of all the sources quoted, educators, journalists, and business people were the most positive in portraying the Web's relationship to the family. About 60% of the time that these individuals appeared in articles, they mentioned potential benefits of the Internet. But their positive views didn't appear very much. As Table 17 indicates, educators and journalists together made up fewer than 13% of the people who were quoted.

Table 17: Occupations of the People Mentioned in the Articles (N=663)

	%
Government	20
Criminal justice system	18
Business	17
Education	7
Advocacy organizations	7
Journalists	5
Other	10
Occupation not mentioned	16

Business people made up 17% of the sources, and they viewed the Web favorably 40% of the time. They mixed positive and negative comments about the Web's effects on the family 11% of the time. They were wholly negative 43% of the time.

In fact, the great majority of the people whom the articles cited about the Web tended to emphasize negative views of the Internet's effect on the family. Three fourths of them noted problems on the Web while only one fourth mentioned benefits. Moreover, half of the problems focused on sex—pedophilia, child pornography and pornography.

The emphasis on problems, and most particularly on sex crimes, is reflected in the occupations of people whose comments reporters cited most often in the articles. As Table 17 indicates, government and criminal justice sources (for example, police, prosecutors, and defense attorneys) made up 20% and 18% of the sources, respectively. Government and criminal justice sources also portray the Web in the most negative manner of all occupations. Their comments were unfavorable 90% of the time. Representatives of advocacy organizations were also highly negative, though they weren't nearly as common. They saw the Web's influence favorably only 3% of the time.

SOLUTIONS TO THE PROBLEMS

Articles that noted problems about the Web and the family described attempts to solve them 85% of the time. Table 18 presents the kinds of individuals and organizations involved in those attempts and the percentage of articles in which they appeared. It indicates that government, parents, business, and the criminal justice system (police, the criminal courts) figured most prominently in trying to find a way out of the frightening issues posed for parents and children by the Web. The articles mentioned the individuals or organizations by themselves a bit more than half (55%) of the time. In a bit less than half (45%) of the articles, solutions involved more than one type of actor. Parents and business and parents and government were most common.

**Table 18: Actors that Articles Note As Involved in Possible Solutions To Web Problems
(N= 366)**

	%
Parents	34
Government	36
Business	25
Criminal justice system	23
Teachers	2
Librarians	8
Advocacy/community group members	3
Children	2
Others	2

* The numbers exceed 100% because some articles noted more than one actor.

Reporters' attention to parents along with business or government in discussing answers to Web crime, pornography and privacy invasions should not be taken to mean that they showed parents working with executives and elected officials. To the contrary, the press depicted each party in its own domain. The Federal government was making laws to try to stop the scourges. Businesses were developing Web filtering software that parents could purchase. Police and the criminal courts were arresting and incarcerating pedophiliacs and child pornographers.

But the press presented the activities of these institutions as piecemeal, tentative or muddled. Arresting and convicting individual child molesters would not accomplish much if (as the articles implied) many more could be lurking in cyberspace. Using filtering software would not be helpful if (as articles related) they often blocked children from useful areas of the Web. And government actions regarding explicit sexuality and the invasion of privacy often were depicted as protracted

inaction as Constitutional free speech issues and concerns of business marketers slowed law-makers.

The upshot was that the press placed the burden of dealing most immediately with Web problems on parents. Some articles showed devastated parents interacting with police and the courts over their harmed children. Other articles suggested a wide range of actions to counter the dangers of the Web—monitoring their children's Web activities, going online with their kids, looking for good Web sites, and using filters to block bad ones. Unfortunately, the articles typically depicted themselves as the only avenues of support. They did not portray the local community—teachers, librarians and neighborhood groups—as resources. At the everyday level, the press showed parents facing a useful but scary Web virtually alone.

*Publications in the
Annenberg Public Policy Center's
Report Series*

- No.1 **Public Space: The Annenberg Scholars' Conference**
1 - 4 March 1995
- No.2 **The State of Children's Television: An Examination of Quantity, Quality, and Industry Beliefs**
17 June 1996
- No.3 **Positive Effects of Television on Social Behavior: A Meta-Analysis**
17 June 1996
- No.4 **Assessing the Quality of Campaign Discourse — 1960, 1980, 1988, and 1992**
22 July 1996
- No.5 **Call-In Political Talk Radio: Background, Content, Audiences, Portrayal in Mainstream Media**
7 August 1996
- No.6 **The First Annual Annenberg Public Policy Center's Conference on Children and Television: A Summary**
17 June 1996
- No.7 **Newspaper Coverage of Children's Television**
24 October 1996
- No.8 **Information Technology and Its Impact on Catastrophic Risks**
12-13 June 1996
- No.9 **Public Policy for a Networked Nation**
December 1996
- No.10 **Civility in the House of Representatives**
March 1997
- No.11 **Free Television for Presidential Candidates**
March 1997
- No.12 **Newspaper Coverage of Children's Television: A 1997 Update**
9 June 1997
- No.13 **Children's Educational Television Regulations and the Local Broadcaster: Impact and Implementation**
9 June 1997
- No.14 **The 1997 State of Children's Television Report: Programming for Children Over Broadcast and Cable Television**
9 June 1997
- No.15 **Free Air Time and Campaign Reform**
11 March 1997
- No.16 **Issue Advocacy Advertising During the 1996 Campaign: A Catalog**
16 September 1997
- No.17 **The Future of Fact: An Annenberg Scholars Conference**
26-28 February 1997
- No.18 **Free Time and Advertising: The 1997 New Jersey Governor's Race**
February 1998
- No.19 **"Stand By Your Ad": A Conference on Issue Advocacy Advertising**
16 September 1997
- No.20 **Civility in the House of Representatives: An Update**
March 1998

- No.21 **The Second Annual Annenberg Public Policy Center's Conference on Children and Television: A Summary**
9 June 1997
- No.22 **The Minnesota Compact and the Election of 1996**
April 1998
- No.23 **The 1998 State of Children's Television Report: Programming for Children over Broadcast and Cable Television**
22 June 1998
- No.24
22 June 1998
- No.25 **The Third Annual Annenberg Public Policy Center's Conference on Children and Television: A Summary**
22 June 1998
- No.26 **Civility in the House of Representatives: the 105th Congress**
March1999

THE ANNENBERG PUBLIC POLICY CENTER
OF THE UNIVERSITY OF PENNSYLVANIA

3620 Walnut Street, Philadelphia, Pennsylvania 19104-6220
320 National Press Building, Washington, DC 20045

Philadelphia
Telephone: 215.898.7041
Fax: 215.898.2024
Email: appc@asc.upenn.edu

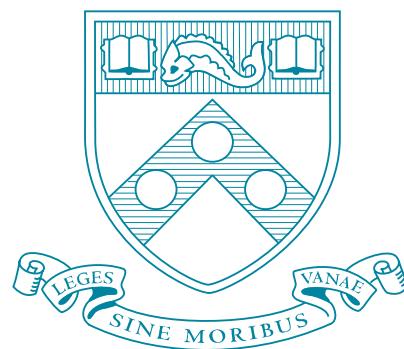
Washington
Telephone: 202.879.6700
Fax: 202.879.6707
ail: appcdc@pobox.asc.upenn.edu

Homepage: www.appcpenn.org

The Internet and the Family
2000
The View from Parents
The View from Kids

By Joseph Turow
Lilach Nir

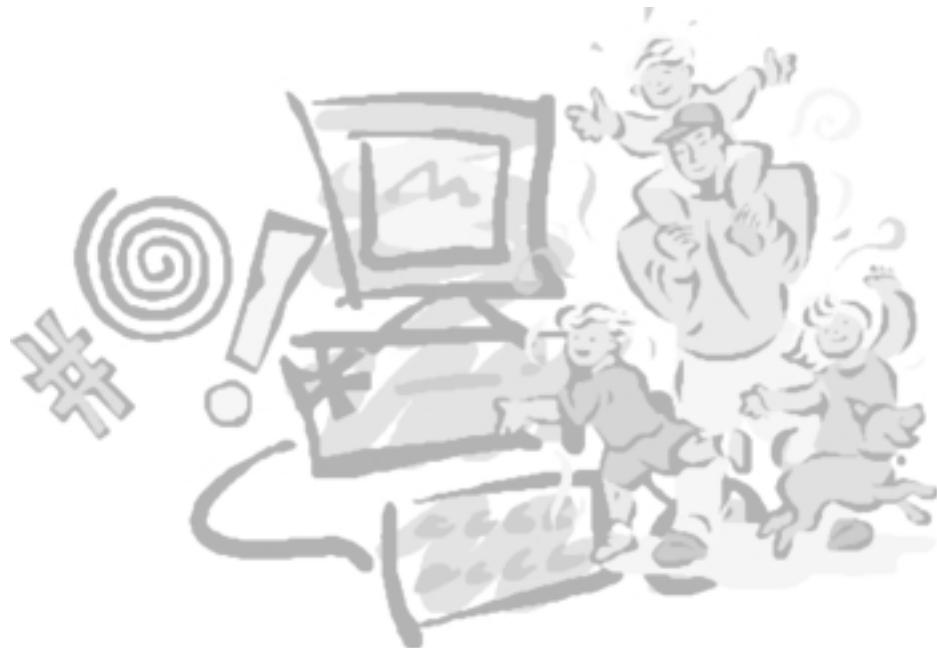
May 2000



THE ANNENBERG PUBLIC POLICY CENTER
OF THE UNIVERSITY OF PENNSYLVANIA

The Internet and the Family 2000: The View from Parents The View from Kids

Overview	4
The Study and the Population	6
Attitudes of Online Parents Toward the Web, 2000 vs. 1998	12
Families and Information Privacy on the Web	15
Comparing Kids and Parents on Information Privacy	26
Concluding Remarks	34



The Annenberg Public Policy Center was established by publisher and philanthropist Walter Annenberg in 1994 to create a community of scholars within the University of Pennsylvania which would address public policy issues at the local, state and federal levels. Consistent with the mission of the Annenberg School for Communication, the Center has four ongoing foci: Information and Society; Media and the Developing Mind; Media and the Dialogue of Democracy; and Health Communication. Each year, as well, a special area of scholarly and social interest is addressed. The Center supports research and sponsors lectures and conferences in these areas. This series of publications disseminates the work of the Center.

Kathleen Hall Jamieson
Director

Joseph Turow is Robert Lewis Shayon Professor of Communication at the University of Pennsylvania's Annenberg School For Communication. He is the author of more than 50 articles and seven books on mass media, including *Breaking Up America: Advertisers and the New Media World* (University of Chicago Press, 1997; paperback, 1998); and *Media Today*, an introductory college text published in 1999 by Houghton Mifflin. He currently serves on the editorial boards of the *Journal of Broadcasting and Electronic Media*, *Critical Studies in Mass Communication*, the *Encyclopedia of Advertising*, the *Sage Annual Review of Communication Research*, and *New Media & Society*.

Lilach Nir is a doctoral student in Communication at the University of Pennsylvania. With Joseph Turow and John Bracken, she authored "The Internet and The Family: The View From the Press," Part 2 of last year's *Internet and the Family* report.

Rebecca Dudley and Cindy Gold provided assistance to this project.

CAPSULE OF FINDINGS:

American parents and youngsters are often of very different minds when it comes to giving personal information to Web sites. Kids' release of information to the Web could well become a new arena for family discord.

OVERVIEW

American parents and youngsters are often of very different minds when it comes to giving personal information to Web sites. Kids' release of information to the Web could well become a new arena for family discord.

- American 10-17 year olds are much more likely than parents to say it is OK to give sensitive personal and family information to commercial Web sites in exchange for a free gift. Examples of such information include their allowance, the names of their parents' favorite stores, what their parents do on weekends, and how many days of work their parents have missed.
- 41% of online parents with kids ages 8-17 and 36% of youngsters aged 10-17 report having experienced incidents of disagreement, worry or anger in their family over kids' release of information to the Web.
- Almost half of US parents are not aware that Web sites gather information on users without their knowing it.
- 61% of parents say they are more concerned about 13 to 17-year olds than they are about younger children revealing sensitive information to marketers.
- It is wrong to think that simple discussions between parents and kids about what information to give to the Web can easily resolve these tensions. Fully 69% of parents and 66% of kids say they have had these sorts of discussions. But when we specifically interviewed pairs of parents and kids in the same family, we found that most didn't agree on whether these sorts of discussions had ever taken place.

These are highlights from a complex picture that we found in the second Annenberg National Survey on the Internet and the Family. The unprecedented comparison of the attitudes of youngsters and parents toward giving up family information to Web sites was conducted by a major national survey firm for the Annenberg Public Policy Center of the University of Pennsylvania. All the respondents belonged to households with at least one computer connected to the Web. 304 youngsters aged 10-17 and 1001 parents with at least one child between ages 8 to 17 were interviewed between January 13 and February 17, 2000.

One aim of this second survey was to track differences from last year's findings regarding what parents generally think and do about the Web. We found that more of them believe in the Web's power to help kids grow. In 2000, all but a small proportion of parents feel that the online world holds strong educational possibilities. Parents are rather evenly divided, though, on whether the Web will also powerfully harm young minds.

Our survey expanded into new territory in 2000 to focus on another topic of growing importance, family privacy and the Web. As teenagers have emerged as major users of the Web, commercial sites have increasingly been gleaning information from them for marketing purposes. We wanted to know whether parents and youngsters agree that releasing information to Web sites is a problem and, if so, whether they do anything about it.

The question ties into an issue that is currently the topic of much public policy discussion: the possibility that youngsters using the Web might give up information about themselves and their families to marketers that their parents would not want disclosed. On the Web, the smallest bits of information divulged by kids about their home life can be aggregated using increasingly sophisticated tracking tools. Web sites can bring the intelligence together to create detailed portraits of a family's lifestyle. Accurate or not, such portraits can profoundly influence how marketers, banks, insurance companies, government agencies and other organizations treat family members—what discounts they give them, what materials they send them, how much they communicate with them, and even whether they want to deal with them at all.

Congress responded to some of this concern about the leakage of family information when, in the 1998 Children's Online Privacy Protection Act, it ordered the Federal Trade Commission to regulate data collection on sites that target children under age 13. The Commission developed rules to ensure that Web sites get parents' permission before the sites request information from children under age 13 about themselves or their families. The FTC rules went into effect in April 2000.

Was Congress' decision to focus only on kids under 13 warranted, or should society expand the information disclosure debate to include youngsters 13 and over? We addressed the question in interviews with parents, teens, and tweens (a marketing term for 10-12 year olds). We created scenarios aimed at learning what the youngsters say would be OK for teens to reveal to Web marketers compared to what their parents say would be OK for teenagers to reveal. And we tried to understand whether those we interviewed are aware of the way Web sites track their visitors without them knowing it.

- We learned that 96% of US parents with children aged 8 to 17 believe that teenagers should have to get their parent's consent before giving information online.
- 62% of tweens and teens agree, including, curiously, more than half of the youngsters who are consistently willing to give up sensitive personal and family information.
- When faced with the scenario of a free gift, though, caution seems to go out the window for many of the kids.

The study explores the concerns parents have about teens' release of information to the Web and how parents deal with this challenge. In the final section of this report, we argue for a social policy that helps families establish clear norms for information privacy and regulates the extent to which Web sites aimed at tweens or teens can elicit information from them.

THE STUDY AND THE POPULATION

In the 2000 research, we repeated key questions from the late-1998 benchmark study “The Internet and the Family: the View from Parents, the View from the Press.” We also added new questions that explored notions of privacy on the Internet among parents and children.

According to Roper Reports and the Current Population Survey (CPS) for 1999, 71% of households with kids 8-17 now have computers and 67% of those households connect to the Internet. In all, then, 48% of US households with kids 8-17 have online connections. This year we focused on this group. In last year’s survey (conducted in November and December 1998) homes with computers but no Internet connections were also included as part of an effort to better understand why some parents choose to connect to the Internet and some did not. A second important difference in 2000 is that children 10-17 were also interviewed, providing the opportunity to compare and contrast parents’ and childrens’ visions of the Internet — and the rising wave of concern over privacy and security issues.

Telephone interviews were conducted with a nationwide cross section of 1,001¹ parents of children 8-17 in homes with Internet connections. The Random Digit Dialing (RDD) sampling methodology was used to locate respondents. During the interviews parents were asked to answer questions while thinking about their child 8-17 that had the most recent birthday. When the child the parent had focused on during the interview was at least 10-17 years old, an attempt was made to also interview that child. When that child was not available, another child 10-17 in the household was interviewed. Approximately half of the 304² children 10-17 that were interviewed were selected from same households as the parents. The other half of the childrens’ sample (for which parents were not interviewed) was located using the Random Digit Dialing (RDD) sampling methodology. All the interviews were conducted January 13 through February 17, 2000. Interviews with the adults averaged 20 minutes; the ones with the kids averaged 10 minutes.

¹ The sampling error for percentages based on the entire sample of 1001 parents is approximately plus or minus 3.5 percentage points. The sampling error is larger for smaller subgroups within the sample.

² The sampling error for percentages based on the entire sample of 304 children is approximately plus or minus 5.6 percentage points. The sampling error is larger for smaller subgroups within the sample.

THE PARENTS AND YOUNGSTERS

For the half of the children's sample whose parents we did not interview, we decided to limit our requests for background information for reasons of time. We know that the youngsters are scattered randomly across U.S. area codes. We also know that the average age is 13½ and that 52% are girls, 48% boys.

Table 1: Characteristics of Parents with Children 8-17 and Online Computers at Home

	(N=1001)	%
SEX		
Male	41	
Female	59	
AGE		
20-29	4	
30-44	57	
45-59	33	
60 or older	6	
RACE		
White	76	
African American	6	
White Hispanic	4	
Black Hispanic	1	
Asian	2	
Native American	2	
Other	3	
No answer	5	
MARITAL STATUS		
Married	79	
EMPLOYMENT STATUS		
Employed	83	
"Not employed" homemaker	10	
"Not employed" student	2	
Retired	2	
Disabled	1	
Unemployed	2	
NUMBER OF CHILDREN, AGED 8-17		
One	46	
Two	37	
Three	12	
Four or more	5	

* When the numbers don't add up to 100% it is because of a rounding error.

We learned more about the parent population (and therefore about the 150 kids linked to them). As Tables 1 and 2 indicate, the majority of parents of children 10-17 with on-line connections at home are white and between 30 and 40 years old. Seven in 10 (69%) have at least some college education; 38% have college or graduate degrees. Income distribution is hard to assess because so many parents—12% more than in our late 1998 study—refused to answer the question when it was presented toward the end of the interview. It may be that the interview's topic of information privacy sensitized many of the parents to a concern about divulging household income. Fortunately, the overwhelming majority of respondents were much more forthcoming in answering questions during the rest of the interview.

Table 2: Last Education Degree and Household Income of Parents With Children Aged 8-17 and Online Computers at Home

	(N=1001)
	%
LAST EDUCATION DEGREE	
Grade school or less	1
Some high school	3
High school graduate	25
Some college	25
College graduate	31
Post graduate	14
No answer	2
YEARLY INCOME	
Less than \$30,000	9
\$30,000 - \$49,999	19
\$50,000 - \$74,999	23
\$75,000 or more	24
No answer	26

Table 3: Patterns of Internet Use, Children Age 10-17

	Total (N=304)	Gender		Age	
	Boy (n=145)	Girl (n=158)	10-12 (n=101)	13-17 (n=203)	
Frequency of Internet use					
A lot	37	38	36	21	45*
Some	37	35	39	37	37
Not Much	19	21	17	29*	14
Not at all	7	7	7	12*	4
Don't Know/ Refused	0	0	1	2*	0
Specific Internet Usage					
Send/Receive Email?					
Yes	83	82	85	70	90*
No	17	19	15	30*	10
Visit Chat Rooms?					
Yes	43	40	46	32	49*
No	57	60	54	68*	51
Visit Web Sites?					
Yes	91	92	89	86	93*
No	9	8	11	14*	7
Play Online Games?					
Yes	32	43*	26	23	40*
No	66	57	74*	77*	61

* Means that the percentage difference is statistically significant from the percentages of the corresponding category in that variable (boys vs. girls, young vs. old children).

Table 3 shows that 37% of the youngsters in our study told us that they use the Web “a lot,” while 37% said “some.” Only 7% said that they don’t go online at all. Boys and girls reported no difference in the use of the Web. Teenagers (aged 13-17) were substantially more likely than tweens (those aged 10-12) to say they use the Web a lot. Nevertheless, of the kids who don’t go online at all, about half were teens and half tweens.

As the table shows, for virtually all the kids (91%) going online means visiting Web sites. Sending and receiving email is another hugely popular activity, with visiting chat rooms and playing games with other people online far less common. Older kids are much more likely than younger ones to participate in chat rooms and game-playing with others. Boys are more likely than girls to involve themselves in cooperative game-playing online.

Tables 4 and 5 present answers to the questions we asked the parents about online use. The majority of parents have had the Web at home for over a year. Only 6% of our respondents say they have never gone online. Three quarters of the ones who do go online say they use both email and the World Wide Web. Twenty-one percent say their Internet use is limited to email.

Table 4: Patterns of Online Use, Parents of Children 8-17

	(N=1001)*
	%
PERCENTAGE ON THE INTERNET	
E-mail only	21
Other Internet (with or without e-mail)	74
Neither	6
ABILITY TO GO ONLINE OR NAVIGATE THE INTERNET	
A beginner	24
An intermediate user	42
An advanced user	22
An expert user	8
Don't know	4
LENGTH OF ONLINE CONNECTION AT HOME	
Less than six months	15
Between six months and a year	18
More than a year, but less than two years	21
More than two years	46
Don't Know	0

* When the numbers don't add up to 100% it is because of a rounding error.

Table 5: Frequency of Web Use, for Parents of Children 8-17, Late 1998 vs. 2000

	1998 (N=676)	2000 (N=1001)
	%	%
FREQUENCY OF GOING ONLINE IN THE PAST MONTH FROM WORK		
Every day	26	30
Every other day	7	7
Every few days	8	8
A few times	11	7
One or two days	6	5
Don't know	-	1
None	40	42
FREQUENCY OF GOING ONLINE IN THE PAST MONTH FROM HOME		
Every day	30	37
Every other day	15	17
Every few days	21	18
A few times	17	12
One or two days	12	6
Don't know	-	-
None	4	10
FREQUENCY OF GOING ONLINE IN THE PAST MONTH FROM OTHER PLACES		
Every day	3	3
Every other day	1	2
Every few days	4	3
A few times	5	7
One or two days	7	5
Don't know	-	1
None	79	79

One quarter of the parents who go online consider themselves beginners, 44% see themselves as intermediates, and 31% view themselves as advanced or expert users. These percentages are almost exactly the same as the ones we found last year.

For parents in Web households, home rather than work is the place in which they report most of their online activity taking place. As Table 5 indicates, fully 42% of our respondents said they have not gone online at all from work in the past month. Moreover, while 78% say they go online at home at least every few days, a smaller 45% say they go online from work that frequently. Table 5 shows that compared to last year, parent online use is up somewhat both at work and home.

ATTITUDES OF ONLINE PARENTS TOWARD THE WEB, 2000 VS. 1998

One aim of our 2000 survey was to track differences from last year's findings regarding what parents generally think and do about the Web. We presented parents with 15 of the most illuminating statements from last year about the potential benefits and harms of the Internet for children. We asked them how much they agreed or disagreed with each of the assertions along a five-point scale, from agree strongly to disagree strongly.

Table 6: Percentage of Online Parents Who Agreed "Strongly" or "Somewhat" with statements about the Internet (Late 1998 vs. 2000)

	1998 (N=676)	2000 (N=1000)
	%	%
Access to the Internet helps my children with their schoolwork.	84	89*
Online, my children discover fascinating useful things they never heard of before.	81	85*
Children who do not have Internet access are at a disadvantage compared to their peers who do have Internet access.	68	74*
I am concerned that my child/children give out personal information about themselves when visiting Web sites or chat rooms.	77	74
I am concerned my child/children might view sexually explicit images on the Internet.	76	72*
The Internet can help my children learn about diversity and tolerance.	60	66*
People worry too much that adults will take advantage of children on the Internet.	57	59
Going online too often might lead children to become isolated from other people.	60	59
The Internet is a safe place for my children to spend time.	40	51*
Families who spend a lot of time online talk to each other less than they otherwise would.	48	50
My children's exposure to the Internet might interfere with the values and beliefs I want to teach them.	42	43
Children who spend too much time on the Internet develop anti-social behavior.	40	41
I often worry that I won't be able to explore the web with my children as well as other parents do.	21	26

* Indicates that the difference between responses of online parents in 2000 and in late 1998 is statistically significant.

As Table 6 indicates, we found a remarkable continuity in the belief that the Internet is a useful and even critical component of a child's education while at the same time it gives youngsters access to content with troublesome values. The one fairly substantial jump in agreement related to parents' view of the overall safety of the Web. While 40% agreed in late 1998 that "the Internet is a safe place to spend time," a majority—51%—agreed in the 2000 survey. Otherwise, the percentages of parents agreeing with the positive statements rose slightly while the percentages agreeing with negative statements regarding the Web remained the same.

- The statement that most parents agreed with in both 2000 and 1998 was that "access to the Internet at home helps my children with their schoolwork": 89% agreed with this in 2000, compared to 84% in late 1998.
- Number two on the list is parents' agreement that "online, my children discover fascinating things they have never heard of before": 86% of parents agreed somewhat or strongly with this statement in 2000, compared to 81% a year earlier.
- Seventy-four percent of parents in 2000 agree that "children who do not have Internet access are at a disadvantage" compared to 68% in late 1998.

This assessment that the Internet is not an interesting luxury but a near necessity is undercut, however, by concerns. For example:

- About seven in 10 parents (71%) in 2000 agree with the statement "I am concerned that my children might view sexually explicit images on the Internet." Seventy-six percent agreed with this in 1998.
- 51% (compared to 48%) agreed that "families who spend a lot of time online talk to each other less than they otherwise would."
- Sixty-two percent of parents agreed with the new statement this year "I am concerned that my children might view violent images on the Internet."

THE PARENTS' WEB ATTITUDE CLUSTERS

Last year, we used a statistical technique known as cluster analysis to group parents in on-line households according to their attitudes about the Internet. Three groups of parents emerged:

- **The Online Worriers** – parents who are most concerned about bad effects that the Internet might have on their children and their families, though they also see the Web's positive qualities.
- **The Disenchanteds** – on-line parents who are not convinced about the Internet's educational value for their children even as they are concerned about its negative consequences.
- **The Gung Ho** – on-line parents who are highly positive about the Web and reject assertions about the negative effects of the Internet.

In 2000 we attempted to see whether and to what extent these groups of online parents still exist.³ We found that they do, in percentages quite similar to those we saw last year, as the box below notes.

	Online Worrier	Disenchanted	Gung Ho
Jan-Feb 2000	40%	16%	43%
Nov-Dec 1998	39%	22%	39%

Comparing 2000 and 1998, we see a stable proportion of on-line worriers who are concerned about the negative social effects of Internet use. We see fewer disenchanted parents who are skeptical about the real benefits the Internet can bring for children. And we see a very slight increase in the proportion of gung ho parents, the ones who reject many concerns about the Internet.

Last year we noted that gung ho parents tended to have had an online connection longer than other online parents. We noted the same relationship this year, though the association was not as strong. The tendency for people who remain online for more than two years to stay positive (or develop positive inclinations) toward the Web would suggest that the stable percentage of online worriers is to some extent being replenished by newcomers.

The decline in the percentage of disenchanted parents suggests that relatively few people with youngsters discount the potential positive power of the Web for kids. Parents' thinking about the Web appears to be dividing along two views on its role in society. Both gung ho's and online worriers believe in the online world's strong educational possibilities, while online worriers insist the Web can also powerfully harm young minds.

³ A discriminant analysis was performed using the 1998 three-group online segmentation as the dependent variable; items which were used to derive the 1998 segmentation (also asked in the 2000 study) were used as independent variables. Classification rates were quite good (90% of respondents belonging to group 1 were correctly classified, 89% for group 2, 87% for group 3) with an overall cross-validated correct classification rate of 89%. The classification function coefficients were used to create an algorithm (a weighted formula) with which to classify respondents of the 2000 study into the online segments.

FAMILIES AND INFORMATION PRIVACY ON THE WEB

We move now to the new topic that we addressed in the 2000 survey: the attitudes of parents and children in online households toward giving up information to Web sites. One major question we had was whether the attitudes parents hold generally toward the Web—for example, whether they are online worriers, disenchanteds or gung ho's—are reflected directly in the attitudes they hold to information privacy in the digital domain. Or, we wondered, do parents see information privacy separately from the way they see the Web as a whole because of a special concern that their children might release sensitive family information?

We also wanted to know whether American parents and children 10-17 are similar or different in the ways that they think about family privacy and report their interactions around it.

BACKGROUND: THE WEB'S INTEREST IN TEENS' INFORMATION

Our interest in comparing parents and youngsters in this age group grew out of awareness that commercial sites have increasingly been pursuing teens. As an article in *Forbes Digital Tool* noted, "the disposable income and tech-friendly instincts of teenagers have made [this segment] the hottest target for revenue generation among web companies."⁴ "There's a "frenzy over teens," agreed Dan Pelson, chief executive of Bolt Media Inc., a Web "community" for teenagers.⁵

Like commercial sites aimed at adults, teen-oriented commercial domains gather information about their visitors for advertising, market research and electronic commerce. They use visitor data to attract sponsors who will pay for *banners* and other ads on the site to reach such individuals. Sites also sell information to marketers who need to know about the interests and habits of people whose profiles fit the visitors to the site. In addition, sites use the information themselves to help them sell products or services directly to their visitors. (Teenagers can purchase online by using their own bank cards, their parents' credit cards or money pre-deposited through that some online retailers have instituted.)

Information about visitors can be gathered on the Web in basically two ways. One is by requesting data from visitors when (and if) they register to use the site. The other is by tracking what users

⁴ Regina Joseph, "It's time for handheld wireless devices: CollegeClub.com wants to offer gadgets to your kids They won't help Johnny's grades, but they sure are cool," *Forbes Digital Tool* (www.forbes.com), May 07, 1999.

⁵ Roger O. Crockett, "Forget the Mall. Kids Shop the Net. Soon they'll spend billions online. How should marketers and parents respond?" *Business Week*, July 26, 1999, p. EB 14.

do on a site. To track, Web sites place tags, called *cookies*, on the visitor's computer disk drive. Cookies can note how often (and when) a visitor comes to a site and where the visitor clicks the mouse when there. The Web site can retrieve this *clickstream* information for an analysis called *digital profiling*. The profiling can merge information from the online registration and clickstream as well as from other information gleaned from the visitors—for example e-mails. Merchandising sites have been active in merging online data they have about their customers with "offline" (sometimes called *legacy*) data they have developed about them through such activities as telephone inquiries and credit card purchases.

To allay consumers' concerns that Web sites are selling far and wide what they know about individuals, many Web sites post privacy policies that attempt to assure their users. The standard approach is to promise that the information will not be shared or sold to others in ways that allow an association of the individual's name with the data. A careful reading of many Web-site privacy policies, however, will reveal a number of important loopholes in this promise. Chief among them is a disclaimer that information gleaned by or given to advertising banners on the site are not covered by the privacy policy. By placing a banner on a site, in fact, an advertiser can quietly insert its own cookie on the visitor's computer and follow the clickstream. If the banner encourages the visitor to fill his or her name and address on a sweepstakes form in the banner ad, the marketer now has an easy way to link the cookie to a real person with online and offline activities.

Privacy advocates have worried strenuously about the gathering of all sorts of data about individuals on the Web. They claim that although customer records always have been collected, the Web is unique because it makes it easy to connect information within and across databases and to use that data instantly. The concern that has resonated most with lawmakers is the possibility that youngsters using the Web might give up information about themselves and their families to marketers that their parents would not want disclosed. Congress responded to some of this concern about this leakage of family information when, in the 1998 Children's Online Privacy Protection Act, it ordered the Federal Trade Commission to regulate data collection on sites that target children under age 13. The Commission developed rules to ensure that Web sites get parents' permission before the sites request information from children under age 13 about themselves or their families. The FTC rules went into effect in April 2000.

FTC rules consider youngsters over 13 to be adults when it comes to the disclosure of information on the Web. We tried to zero in on what parents think of this notion and, in general, how they and youngsters differ in thinking about and dealing with information privacy.

PARENTS' APPROACH TO FAMILY INFORMATION PRIVACY

Parents' stance on treating youngsters 13 and over as adults on the Web comes through quite clearly in our survey: they don't agree. As noted at the beginning of the report, fully 96% of the parents interviewed believe that "teenagers should have to get their parent's consent before giving out information online." In fact, 84% of the parents agree "strongly" with the statement. Moreover, 60% of parents agree that they "worry more about what information a teenager would give away to a Web site than a younger child under 13."

These answers are part of a strong pattern of concern for information privacy that we found among most parents. Table 7 presents the percentages that agree or agree strongly with fifteen statements on the subject. Second on the list—just under the statement about requiring parents' consent—is parents' belief that they should have a legal right to know "everything" that a Web site knows about them; 95% agree, with 87% agreeing "strongly" with the statement.

Table 7: Percentage Of Parents Who "Agreed" Or "Agreed Strongly" to the Privacy Statements

	Total (N=1001)	Wary (n=375)	Cavalier (n=303)	Selectively Trusting (n=323)
Teenagers should have to get their parent's consent before giving out information online.	96	98#	91	98#
I should have a legal right to know everything that a Web site knows about me.	95	99#	89	97#
I am nervous about Web sites having information about me.	73	90#+	43	81#
I am more concerned about giving away sensitive information on-line than about giving away sensitive information any other way.	63	79#	29	79#
My concern about outsiders learning sensitive information about me and my family has increased since we've gone online at home.	59	82#+	22	66#
I worry more about what information a teenager would give away to a Web site than a younger child under 13 would.	61	63#	33	81*#
I look to see if a Web site has a privacy policy before answering any questions.	72	69	61	86*#
When I go to a Web site, it collects information about me even if I do not register or fill in information about myself.	54	64#	37	59#
Web site privacy policies are easy to understand.	41	18	50*	60*#
When a Web site has a privacy policy, I know that the site will take proper care of my information.	41	14	37*	76*#
I sometimes worry that members of my family give information they shouldn't about our family to Web sites.	36	46#	6	54#
I trust Web sites not to share information with other companies or advertisers when they say they won't.	37	7#	29	80*#
I like to give information to Web sites because I get offers for products and services I personally like.	18	5	14*	36*#
I will only give out information to a Web site if I am paid or compensated in some way.	9	3	5	21*#

(*) Notes that the percentage of respondents who agreed with this statement was significantly different from the group of "wary" parents.

(#) Notes that the percentage of respondents who agreed with this statement was significantly different from the group of "cavalier" parents.

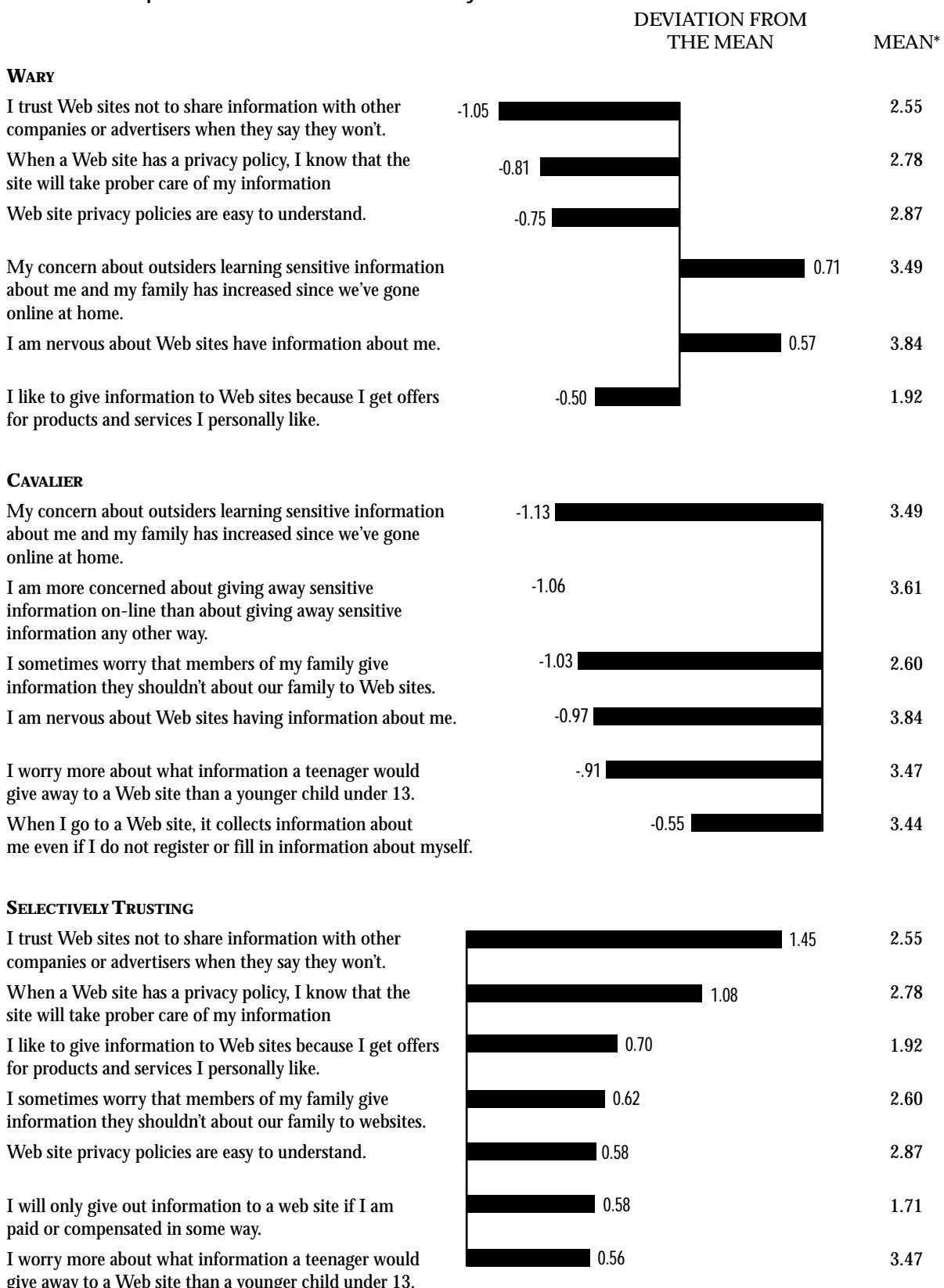
(+) Notes that the percentage of respondents who agreed with this statement was significantly different from the group of "selectively trusting" parents.

While the overwhelming number of parents agrees with these statements, there is a fair divergence in answers to the others. We used the computer technique called cluster analysis to discover if all the parents fit one profile in their answers or if there is diversity among them regarding their attitudes toward information privacy on the Web. The technique determines whether there are patterns among respondents in the extent to which certain statements deviate strongly from the average reply ("the mean"), based on a scale in which "agree strongly" is 5 and "disagree strongly" is 1. When the deviation from the mean of responses to a particular statement is strongly positive, it means that the people in the group agree or agree strongly with the statement more than most of the people in the sample. When the deviation from the mean of responses to a particular statement is strongly *negative*, it means that the people in the group disagree or disagree strongly with the statement more than most of the people in the sample.

As Chart 1 shows, we found three groups of parents with important differences in the way they state their attitudes toward family information privacy. We label the groups **wary, cavalier, and selectively trusting**.

- The wary make up 38% of the parents. They express a greater distrust of Web sites than the other two groups. It shows up in their stronger than average nervousness about Web sites having and sharing information about them; increased concern since going online that outsiders are learning sensitive information about them; disbelief that sites will adhere to privacy promises; and a sense that privacy policies are not easy to understand.
- The cavalier (30% of the parents) are much more likely than the others to reject specific concerns about Web privacy. They tend to disagree that since going online they have become more concerned about outsiders learning sensitive information about them; to dismiss worries about family members giving information to Web sites; and to deny worrying that a teen would give away more personal information on the Web compared to a child under age 13. Cavalier parents are also quite a bit less likely than wary and selectively trusting ones to know that web sites collect information about them even if they don't fill out information on the sites—a fact that perhaps suggests some naivete on the part of the Web cavaliers.
- The selectively trusting (32%) have characteristics of both groups. Like the wary, they have a higher than average concern about aspects of Web privacy—in their case, that family members might give away inappropriate information and that a teen would give away more information than a child under 13. Quite different from the wary, however, is the tendency of selectively trusting parents to say that Web sites' privacy policies are reliable and that sites will live up to their promises about not sharing information. Selectively trusting parents also stand apart from the other two groups in stating that they like to barter information for offers or compensation on the Web and in claiming that privacy policies are easy to understand.

Being wary, cavalier or selectively trusting has no association with a person's self-reported expertise with the Web, or with the amount of time the household has been online. We also found that these privacy clusters are unrelated to a parent's gender. Mothers are just as likely as fathers to report cavalier, wary, or selectively trusting attitudes toward Web privacy.

Chart 1: Groups of Parents Based on Their Privacy Views

* This is the mean (average) or responses to the statement by the entire sample of parents. See text

We noted, too, that concern about information privacy on the Web is not the same as general concern about the Web. When we examined the association between parents' Web attitude clusters—online worriers, disenchanteds and gung ho's—to these privacy clusters, we saw no statistically significant relationship between the two groups. It turns out that people who are worried, enthusiastic or disenchanted about the Web feel that way for reasons that may or may not include their opinions about information privacy on the Internet. They may, for example, be more or less concerned about Web violence, or more or less enthused about great learning sites.

PARENTS AND SUPERVISION REGARDING INFORMATION

We did find statistically significant associations between the way parents talk about Web privacy (as seen in the clusters) and the ways they say they act or would act regarding their family's information. Wary parents respond differently from cavalier ones, and they in turn answer differently from those who are selectively trusting. At the same time, the pattern of answers suggests that the cavalier and selectively trusting parents are more conservative in their actions than their stated attitudes might predict.

Table 8 provides one illustration of this tendency. It presents parents' experiences and approaches to teaching their children about information privacy. We see that wary parents are more likely than others to say that they have had unhappy experiences with information loss through theft or children's release of data. Wary parents are also more likely to say they chose not to register for a Web site that wanted personal information and that they have not read a privacy policy.

Though these findings show statistically significant differences among these parent respondents, the table also reveals important similarities. Overall the reported experiences and actions of cavalier and selectively trusting parents reflect a caution about privacy that is not so very different from the caution that wary parents exhibit. Moreover, the groups are not statistically different on a number of key actions: buying something over the web (only half of even the cavalier parents have done it); reporting tension around issues of Web information (about 40% in all groups recall it); and saying they talked to their kids about how to deal with Web requests for information (nearly two thirds in each group say they have done it). The picture that emerges generally is that selectively trusting parents are more selective than their privacy attitudes suggest and that even the cavalier parents are really not so cavalier about giving out information or letting their children do it.

This picture is reinforced in the parents' responses to questions based on our two scenarios. We designed each scenario to place the parent in a situation that encouraged the exchange of information for a free, rather valuable "gift" from a favorite store. The scenarios became our major vehicles for comparing the parents' sensitivities with those of youngsters aged 10 to 17 on concrete instances of information exchange.

Table 8: Experiences Of Parents Regarding Information Privacy

	Total (N=1001)	Wary (n=376)	Cavalier (n=303)	Selectively Trusting (n=323)
Person or company used information about them in an improper way	10	15#+	5	10
Person or company used information about them in an improper way specifically on the Web	3	4	1	3
Had incident where parent was worried about something his/her child told both a telephone marketer	4	7+	3	2
Had incident where parent was worried about something his/her child told a Web site	5	5	3	5
Had incident where parent was worried about something his/her child told a telephone marketer and Web site	3	5	0.5*+	3
Generally reports tension over his/her child giving information to the Web ⁶	41	44	38	40
Bought something over the Web	53	52	54	54
Never read a site's privacy policy	16	20#	13	14
Read a site's privacy policy one time to a few times	53	54	55	50
Read a site's privacy policy many times	24	19	25	29*
Doesn't know what a privacy policy is or whether read one	6	6	6	6
Registered on a Web site	41	38	41	44
Chose not to register on a Web site at least once because was asked for personal information	65	73	59*	62*
Talked with his/her child about how to deal with requests for information from Web sites	66	67	66	65

(*) Notes that the percentage of respondents who agreed with this statement was significantly different form the group of "wary" parents.

(#) Notes that the percentage of respondents who agreed with this statement was significantly different form the group of "cavalier" parents.

(+) Notes that the percentage of respondents who agreed with this statement was significantly different form the group of "selectively trusting" parents.

⁶We considered parents as having "experienced tension" with youngsters over kids' release of information to the Web if the parents answered any of four questions in specific ways. One question asked, "when it comes to chat rooms, or sending and receiving email, do you disagree with your children frequently, sometimes, rarely or never?" If the person said frequently or sometimes, we took that as a yes to having experienced tensions. The second question asked if the parent had ever been involved in a specific incident where the parent was worried about something that his or her child told a Web site. A third question asked "as far as you know, has any of your children been involved in a chat room or communicated with people you found unacceptable on the Web?" The fourth question asked, "Has any of your children ever given out information he or she shouldn't to Web sites?" We found that 41% of the parents answered yes to one or more of these questions.

SCENARIO 1:

The first scenario aimed to assess the tendency of the parents to say they would give out their name, address and other information under realistic conditions of a Web privacy policy considered standard in the industry. The scenario reflects what the industry-supported organization Privacy & American Business says “three out of four adult Web users” want before they give up personal information on the Web: a benefit, notice about how the firm will use their information, and an industry-accepted privacy policy.⁷

The interviewer posed the scenario in the following manner:

I'd like you to pretend that you visit the Web site of your favorite store and see that you can earn a **great** free gift if you answer some questions. In order to get the free gift, you must give your name, home address, and answer some questions about what you like and don't like. The store clearly promises not to give out the names or home addresses of people who register for the free gift — but the store may give out answers to any of the other questions to other stores or advertisers.

Would **you** answer these types of questions in return for a great free gift, or not?

If the parent said no or “it depends,” the interviewer asked, “What if the product was worth \$25?” A no to that led to a raising of the product’s value to \$50, then to \$100.

Table 9 lists the initial answers of respondents as well as the percentage of total respondents who were ultimately swayed. Clearly, the wary parents were most immediately likely to say no (80%), followed by the cavalier (66%) and then the selectively trusting (56%). The somewhat higher tendency of selectively trusting parents to say *yes* or *it depends* rather than *no* probably relates to that group’s greater-than-average belief in the truth of Web sites’ privacy policies. In the final tally, 43% of selectively trusting parents were swayed to yes, compared to 33% of cavaliers and only 17% of the wary. In all 29% of the parents said that they would accept the offer of the free gift in exchange for identifying data and “other” information.

⁷ Alan F. Westin, “Freebies’ and Privacy: What Net Users Think,” *Privacy & American Business Survey Report*, (July 14, 1999). <http://www.pandfab.org/sr990714.html>.

Table 9: Parents' Answers to Scenario 1

	Total (N=1001)	Wary (%)*	Cavalier (%)#	Selectively Trusting (%)+
Would you answer these types of questions in return for a great free product?				
Yes	18	9	21*	26*
No	68	80#+	66+	56
Depends on the product	4	4	3	4
Depends on the information they want	5	3	3	4
Depends on the product and information	4	2	4	7*
Don't know/No answer	2	3	2	2
Total additional parents who said "yes", if the product were worth \$25, \$50, or \$100 (N=1001)	7	9	12	17*
Total who said yes** (N=1001)	29	17	33*	43#

** The total is based on the accumulated number of parents who said yes to the offer, including those who said "no" or "depends" the first time. See text.

(*#, +) Means that the percentage is different from the percentage in the column designated by the mark.

SCENARIO 2:

Our goal for the second scenario was to learn what kinds of specific personal and family information parents believe is acceptable for teens to give up to Web sites. We constructed fifteen items that varied along lines of relatively public and relatively private elements involving the teen or the family. For this scenario we left the privacy policy ambiguous. The interviewer said the following:

Now (whether you currently have a teenaged child or not) suppose a Web site asked a teenager 13 to 17 years old to answer the following questions in order to get a great free gift. Do you think it is completely OK, OK, not OK or not at all OK for a teenager to give the following information to a Web site to get a free gift? If you are not sure, please just tell me.

Please remember that we are not asking for you to answer these questions now - just to tell us if you think it is OK for a teenager to answer questions like these on a web site.

Parents' responses to the 15 items are ranked in Table 10 from the items that they feel are most OK to reveal to a Web site to those they feel are least OK. Overall, it appears that parents consider information about things parents or teens do out of the home and in public most acceptable to reveal. Knowledge about the teen's personal space, embarrassments, or body are intermediate items, while disclosures about parents' personal space, embarrassments or body are least acceptable to reveal.

Table 10: Percentage of Parents Who Feel It Is “Completely OK” Or “OK” for Their Teenager to Give This Information to A Web Site, in Exchange For A Free Gift

	Total (N=1001)	Wary (n=375)	Cavalier (n=303)	Selectively Trusting (n=323)
Give out names of his or her favorite stores	44	38	43	52*#
Give out names of his or her parents' favorite stores	33	27	35*	38*
Give out whether his or her parents talk a lot about politics	25	20	28*	29*
Give out how many times his or her parents have gone to a place of worship in the past month	25	20	28*	29*
Give out whether he or she has skin problems	24	19	26	29*
Give out what types of cars the family owns	21	15	24*	27*
Give out what he or she does on the weekends	19	13	19	24*
Give out how many days of school he or she missed in the past year	19	12	22*	24*
Give out whether the family drinks wine or beer with dinner	17	13	21*	18
Give out how much allowance he or she gets	17	11	20*	21*
Give out whether he or she cheated in school during the past year	16	11	20*	17*
Give out whether his or her parents have skin problems	16	10	20*	18*
Give out whether his or her parents speed when they drive	14	12	17	14
Give out how many days of work his or her parent missed in the past year	10	7	13*	11
Give out what his parents do on the weekends	10	6	12*	12*

(*) Notes that the percentage of respondents who agreed with this statement was significantly different from the group of “wary” parents.

(#) Notes that the percentage of respondents who agreed with this statement was significantly different from the group of “cavalier” parents.

(+) Notes that the percentage of respondents who agreed with this statement was significantly different from the group of “selectively trusting” parents.

The privacy clusters roughly follow this arrangement and the pattern that we have seen previously: The wary are least likely to state that giving up the information is acceptable. The selectively trusting and cavalier dovetail each other in their somewhat more accepting responses, but in percentages that are quite a bit more conservative than their stated privacy attitudes would lead one to suspect. In fact, the average number of selectively trusting and cavalier parents who said it was acceptable to give up the personal and family information was 24% and 23%, respectively. These numbers are not all that different from the 21% “OK” rate in the sample as a whole, and not wildly different from the 16% average of the wary parents. Clearly, the great proportion of individuals in all three parent privacy groups found the notion of teenagers giving out virtually all of this information to Web sites highly problematic.

Statistical procedures allowed us to construct a *parents' information disclosure scale* that indicated the extent of a person's sensitivity to the release of information.⁸ The higher a person's score, the more likely the person was to find it acceptable for a teen to release sensitive personal and family information. Curiously, we found no significant associations between sensitivity to information disclosure and a variety of characteristics, including parents' education, income, gender, expertise with the computer, and the length of time the household has been connected to the Web. We did find that the younger the parent, the more accepting he or she is to a child's disclosure of information. However, all of these characteristics (including age) taken together were not strong enough to comprise the major factors that predict parents' answers regarding teenagers' disclosure of information. Finding these predictors is a challenge for further research.⁹

⁸ The parents' information disclosure scale was scaled from 15 different items in the data set. We employed principal components factor analysis, which is a test to assess whether the items belong to a single conceptual dimension. A principal components factor analysis of the 15 variables yielded a single factor, explaining 58.4% of the variance in responses. The 15 items were then examined for inter-item consistency, in unidimensional scaling (Cronbach's alpha=0.95). A scale of the 15 items, whose values represent the respondent's (parent) inclination to think it's OK for a teen to disclose private and sensitive information, was then computed. The higher the score, the more likely that respondent would say it's OK for a teen to disclose information. The scale mean across the total parents' sample (N=957) was 2.19, and the standard deviation was 0.82.

⁹ We used multiple regression analysis here. We also attempted to find predictors of whether a parent would be swayed in the first scenario. Here too, we did not find demographics or Internet experiences to be strong

COMPARING KIDS AND PARENTS ON INFORMATION PRIVACY

Our interviews with the 10 to 17 year olds aimed to see if their attitudes toward privacy and their decisions in the scenarios are substantially different from those of parents.

We found a striking pattern: In the attitudes they express, youngsters seem quite concerned about protecting their information privacy and nervous about Web sites' having information about them. Yet when we give them specific opportunities to get a free gift in exchange for personal or family information, a much larger proportion of kids than parents are ready to do it. Their approach is the opposite of the tendency shown by the cavalier and selectively trusting parents. These parents often express relatively blasé attitudes toward information privacy but turn out to be quite conservative when confronted with the specific scenarios. By contrast, many of the youngsters express conservative general Web privacy attitudes but turn out to be quite liberal with their information when confronted with the scenarios.

Table 11: Parents' Vs. Kids' Agreement With Privacy Statements

	Parents (N = 1001)		Kids (N = 304)	
	Agree		Agree	
	Strongly (%)	Somewhat (%)	Strongly (%)	Somewhat (%)
Teenagers should have to get their parent's consent before giving out information online	84	12	60	19
I am nervous about Web sites having information about me	41	31	38	25
I look to see if a Web site has a privacy policy before answering any questions	50	19	50	23
I trust Web sites not to share information with other companies or advertisers when they say they won't	15	21	19	22
I like to give information to Web sites because I get				

Only 41% of the kids say they trust Web sites. 73% say they “look to see if a Web site has a privacy policy before answering any questions.” 79% agree that teens should get parents’ consent before giving out information online.

SCENARIOS 1 AND 2:

This aura of caution was much less evident in the responses many of the 10 to 17 year olds gave to the first scenario. The interviewer posed the situation in the same way it was posed to the parents. That led to the question, “Would you [give name, address and answer some other questions about what you like or don’t like] in return for a great free gift, or not?” As with the parents, if the youngster said no or “it depends,” the interviewer asked, “What if the product was worth \$25?” A no to that led to a raising of the product’s value to \$50, then to \$100.

Straight off, 22% of the youngsters said they would be swayed to exchange the information for a free gift. Recall from Table 9 that the proportion of parents who said they would be swayed was similar—18%. (In fact, that difference is not statistically significant.) The real divergence between kids and parents came when the interviewer asked if the person would do it if the gift were worth different amounts of money. By \$25, 30% of the kids had said yes to the initial offer or the offer that mentioned the cash value. By \$50 the proportion was 38%, and by \$100 it was 45%. With parents, the accumulated proportions saying yes at the \$25, \$50 and \$100 offers were 21%, 24% and 29% respectively. (The differences between kids and parents *were* statistically significant at each of the money values.)

Table 12 lays out the initial and final results. As a result of the enticements, a total of 29% of parents and 45% of kids ended up saying they would exchange the information for a free gift. Part of the reason that the kids were attracted to the cash value more than the parents may be that their sense of a lot of money is different from that of adults. What parents may consider a relatively small amount for important information may seem like a gold mine to a youngster.

Table 12: Answers of Youngsters Age 10-17 to Scenario 1

Would you answer these types of questions in return for a great free product? (N=304)	(%)
Yes	22
No	63
Depends on the product	3
Depends on the information they want	4
Depends on the product and information	5
Don't know/No answer	3
Total additional kids who said “yes”, if the product were worth \$25, \$50, or \$100 (N = 304)*	23
Total who said yes (N = 304)	45

*The total is based on the accumulated number of youngsters who said yes to the offer, including those who said “no” or “depends” the first time. See text.

Fitting the pattern we have suggested, the youngsters who say the scenario would sway them nevertheless say they are concerned about privacy. On three of the privacy-attitude statements, they reveal the same strong level of caution about revealing personal information as the youngsters who would not be swayed. The same high percentages say they are nervous about Web sites knowing about them, agree that teens should have to get their parents' consent, and look for a privacy policy before answering any questions.

The two items on which the kids who would and would not barter information for a gift differ reflect a kind of enthusiasm combined with trust that begins to explain why many of the youngsters accepted the blandishment of scenario 1. 46% of the kids who say they would barter information for a gift agree that they like to go to Web sites because they get attractive offers, but only 16% of the kids who wouldn't barter said that. Similarly, 60% of the bartering group say they trust web sites to keep promises not to share information. Only 27% of those who wouldn't barter say that.

This interest in attractive offers certainly shows up in the way the kids who were swayed by the first scenario responded to scenario 2, as Table 13 shows. This "will barter" group, representing almost half of all kids, is willing to give up personal and family information in percentages far higher than the parents.

Table 13: Percentage Of Youngsters Saying It Is "OK" Or "Completely OK" For A Teenager To Give Out Information For A "Great Free Gift"

	Total Kids (N=304)	Will Barter ¹ (n=136) ²	Won't Barter (n=158) ²	Parents (N=1001)
Give out names of his or her favorite stores	65#	82*	53	45
Give out the names of his or her parent's favorite stores	54#	70*	45	33
Give out what types of cars the family owns	44#	57*	34	22
Give out how much allowance he or she gets	39#	52*	30	17
Give out whether his or her parents talk a lot about politics	39#	51	31	26
Give out what he or she does on the weekends	39#	51*	32	18
Give out how many days of school he or she missed in the past year	35#	44*	27	18
Give out how many times his or her parents have gone to a place of worship in the past month	30	39*	23	25
Give out what his or her parent's do on the weekends	26#	36*	20	10
Give out whether he or she has skin problems	24	33*	20	24
Give out whether his or her parents speed when they drive	24#	33*	18	14
Give out whether the family drinks wine or beer with dinner	23#	31	18	16
Give out whether he or she cheated in school during the past year	22#	22	23	16
Give out how many days of work his or her parent missed in the past year	21#	28*	15	10
Give out whether his or her parents have skin problems	19	24	16	15

¹ "Will barter" are those who said they would accept the free gift in scenario 1. See text.

² The percentages in the table do not include "no answer" or "don't know".

* Indicates a significant difference between the percentages of teens who agreed to the statement, in a comparison between "will barter" and "won't barter".

Indicates a significant difference between the percentage of teens and the percentage of parents who said it is "OK" or "completely OK" to give out information in exchange for a gift.

YOUNGSTERS' REPORTED EXPERIENCES WITH THE WEB

Perhaps not surprisingly, the “will barter” group is substantially more likely than the “won’t barter” group to report giving personal information to a Web site, as Table 14 shows. Youngsters willing to barter are also less likely than their unwilling counterparts to say that they have spoken with their parents about how to deal with Web requests for information. In addition, the table shows that “barter-willing” youngsters are less likely to believe that their parents trust them “completely” to do the right thing on the Web.

Table 14: Experiences Of Youngsters Regarding Information Privacy

	Total Kids (N=304)	Will Barter ¹		Gender		Age	
		Yes (n=136) ²	No (n=158) ²	Boys (n=145)	Girls (n=158)	10-12 (n=101)	13-17 (n=203)
Never read a site’s privacy policy	25	23	26	28	22	36	19*
Read a site’s privacy policy one time to a few times	42	44	40	42	41	29	44*
Read a site’s privacy policy many times	25	14	17	15	17	7	20*
Doesn’t know what a privacy policy is or whether read one	19	19	17	14	18	27	12*
Has given information to a Web site about self	31	40	24*	32	31	16	39*
Say parents trust them completely to do the right thing when it comes to using the Internet	69	60	77*	69	69	74	63
Say parents trust them some or a little to do the right thing when it comes to using the Internet	28	37	20*	25	30	23	34
Talked to parents about how to deal with requests for information on the Web	69	62	75*	63	75*	67	70
Experience tension with parents over giving information to Web	36	39	34	35	37	34	37

¹ “Will barter” are those who said they would accept the free gift in scenario 1. See text.

² These are valid responses, the percentages in the table do not include “no answer” or “don’t know”.

* Indicates that the percentage difference is statistically significant from the percentages of the corresponding category in that variable (will barter vs. won’t barter, boys vs. girls, young vs. old children).

At the same time, the barter willing and unwilling groups do not differ when it comes to reporting tensions with parents over information. Overall, 36% of youngsters aged 10-17 report that they have experienced tension -- that is, that they have disagreed with their parents frequently or sometimes over what they say in chat rooms or email, or that they have gotten their parents angry at them for giving out information elsewhere on the Web that their parents considered inappropriate. As Table 14 indicates, this number is consistent not only with respect to the barter groups

but also when it comes to gender and age. Girls, boys, older children and younger children do not differ in reporting tensions with their parents over giving information to the Web.¹⁰

In general, gender does not associate with many of answers that the youngsters gave about their experiences with the Web. Girls are somewhat more likely than boys to say they have talked to their parents about how to deal with Web requests for information. In the case of other reported activities and knowledge about the Web—including their level of expertise—boys and girls have the same confidence level.

When it comes to information-privacy attitudes and the scenarios, however, girls are quite different from boys. Girls are less likely than boys to say they would barter their name, address and information about tastes for a free gift worth up to \$100. 39% of the girls are barter-willing compared to 54% of the boys. Similarly, as Table 15 shows, boys are substantially more willing than girls when answering scenario 2 to say they would give out certain types of family or personal information for a free gift. Gender also makes a difference when it comes to trusting Web sites “not to share information” with other firms. Half of the boys agree that they can trust Web sites, while only 35% of the girls accept the proposition.

¹⁰ We considered youngsters as having “experienced tension” with parents over releasing information to the Web if they answered either of two questions in specific ways. One question asked, “when it comes to chat rooms, or sending and receiving email, do you disagree with your parents frequently (that is, a lot), sometimes, rarely (that is, not too much) or never?” If the person said frequently or sometimes, we considered him or her as having experienced tensions. The second question asked, “Have your parents ever been angry at you for giving information to a Web site that you shouldn’t have given?” If the youngster said yes to that, we considered him or her as having experienced tensions.

Table 15: Percentage Of Youngsters Saying It Is "OK" Or "Completely OK" For A Teenager To Give Out Information For A "Great Free Gift"

	Total Kids (N=304)	Gender		Age		Total Parents (N=1001)
		Girls (n=158)	Boys (n=145)	10-12 (n=101)	13-17 (n=203)	
Give out names of his or her favorite stores	65#	60	71*	51	72*	45
Give out the names of his or her parent's favorite stores	54#	48	58	43	59*	33
Give out what types of cars the family owns	44#	37	53*	37	48	22
Give out how much allowance he or she gets	39#	33	46*	27	45*	17
Give out whether his or her parents talk a lot about politics	39#	33	45	17	49*	26
Give out what he or she does on the weekends	39#	35	43	29	44*	18
Give out how many days of school he or she missed in the past year	35#	29	41*	30	37	18
Give out how many times his or her parents have gone to a place of worship in the past month	30	26	34	21	34*	25
Give out what his or her parent's do on the weekends	26#	23	30	18	31*	10
Give out whether he or she has skin problems	24	23	26	11	31*	24
Give out whether his or her parents speed when they drive	24#	23	26	11	31*	14
Give out whether the family drinks wine or beer with dinner	23#	22	25	16	27*	16
Give out whether he or she cheated in school during the past year	22#	20	24	12	27	16
Give out how many days of work his or her parent missed in the past year	21#	19	23	17	23	10
Give out whether his or her parents have skin problems	19	23	25	11	31*	15

* Means that the percentage difference is statistically significant from the percentages of the corresponding category in that variable (boys vs. girls and young vs. old teens).

Means that the percentage difference is statistically significant from the percentage of parents who agreed to that statement.

We found no link between age and gender in the answers the youngsters gave. Age alone, however, was more consistently associated than gender with Web experiences as well as with attitudes toward giving up sensitive information.

Table 14 shows that kids age 13-17 are more likely than tweens to say they have read a privacy site and to have given personal information to the Web. Table 15 shows that young age was consistently, and often strongly, associated with accepting the release of personal and family information in scenario 2. Kids 13-17 were far more likely to say it was OK to disclose the answers to 11 of the 15 statements presented to them in exchange for a free gift. Through a different type of analysis, we learned that the higher the age of the youngster (from 10 to 17), the more likely he or she

would be to say it is OK to give out personal and family information as measured in a *kid information disclosure scale* that we constructed from the 15 statements.¹¹

Table 15 suggests that on several responses 10-12 year olds are often as cautious as parents regarding personal and family information. Federal regulations refer to these children and younger ones when requiring a Web site to get parental permission when wanting to ask for, or track, information about a youngster. Ironically, though, it is the older kids, the ones who are fair game for Web sites, who are far more likely than parents to give up the kinds of information the parents would not want released.

Although we found rather strong associations between age and the answers to scenario 2, we found no relationship between age and a willingness to give up name, address and information about likes and dislikes as described in the first scenario. The reason is probably not the clearer mention of a privacy policy in scenario 1 than 2, because we found no difference between the age groups in the trust of privacy policies. Perhaps younger children consider topics such as whether their parents drink wine, what they do on weekends, and whether they cheat on tests to be more obviously sensitive than giving out one's name and address to a Web site. Moreover, both parent and child respondents may have thought that somehow the Web site could find out their names and addresses and associate them with scenario 2's answers.

Despite the basic associations we found between age and a youngster's sensitivity to releasing information, more complex regression analyses revealed the same frustrating lack of predictability that we found with parents. We failed to find any background or attitudinal characteristic—whether age, gender, attitudes toward Web privacy, or any details regarding the child's attitude or experience—that could statistically predict answers on either scenarios 1 or 2. What this means is that while we have found some key associations between age and a youngster's privacy attitude as well as between gender and a kid's privacy attitude, trying to get at the cluster of attitudes and background characteristics that can together predict a youngster's (or parent's) response to information-privacy scenarios remains a challenge.

¹¹ Like the parents' scale, the kids' information disclosure scale was created from 15 different items in the data set. We employed principal components factor analysis, which is a test to assess whether the items belong to a single conceptual dimension. A principal components factor analysis of the 15 variables yielded two factors, explaining 58.9% of the variance in responses. A closer examination of the two items revealed they were equally correlated with the main dimension, and therefore they were not omitted from the scale. The 15 items were then examined for inter-item consistency, in unidimensional scaling (Cronbach's alpha=0.92). A scale of the 15 items, whose values represent the respondent's (kid's) inclination to disclose private and sensitive information, was then computed. None of the items if deleted would have improved the alpha reliability coefficient. The higher the score, the more likely that respondent would disclose information. The scale mean across the total kids' sample (N=290) was 2.66, and the standard deviation was 0.80.

PARENT-CHILD COMMUNICATION AND THE WEB

The findings we have reported for our entire sample of 300 youngsters held up when we looked at the 150 in this group whose parents we also interviewed. While the larger sample of kids was generally more useful to test for statistical associations, the linked pairs of parents and children allowed us to see specifically if youngsters and parents tended to be on the same page when they spoke about information privacy and the Web.

When we interviewed pairs of parents and kids in the same family, we found chance rather than pattern in key communication areas. We found that kids and their parents don't necessarily hold the same attitudes or even remember the same family interactions.

- It was only a matter of chance that the parents and the kids who said they would barter information for free gifts in scenarios 1 and 2 were related.
- Whether parents agreed with their kids on whether they trusted them "completely" was also merely a matter of chance.
- Similarly, although over 60% of all the parents and kids we interviewed (including the youngsters who were open to information barter) said that they have had discussions about how to deal with Web information requests, we found in our pairs that most parents and kids didn't agree on whether these sorts of discussions had ever taken place!

The findings are sobering for those who believe that simple discussions between parents and their children can encourage a consistent family approach to dealing with requests for information on the Web. They suggest that parent-child conversations about Web privacy issues are fleeting at best, perhaps in the form of "don't give out your name" or "don't talk to strangers" that parents have traditionally urged upon their children. In view of the chance relationships between youngsters' and parents' approach to bartering information, it would seem that parent-child communication about family privacy policies is an area that deserves a great deal of attention.

CONCLUDING REMARKS

If there is one point that our study highlights it is that many—in fact, probably most—American families are filled with contradictions when it comes to the Internet. Parents fear that it can harm their kids but feel that their kids need it. Parents and kids individually say they have talked to each other about giving out information over the Web, but parents and kids in the same family don't remember doing it. Kids agree that parents should have a say on the information they give out over the Web but nevertheless find it acceptable to give out sensitive personal and family information to Web sites in exchange for a valuable free gift.

It should not be surprising that these sorts of contradictions lead to tensions. This year's Annenberg report on the Internet and the Family has focused on the contradictions and tensions surrounding the release of family information. We have found that three out of four parents say they are concerned that their children "give out personal information about themselves when visiting Web sites or chat rooms." Smaller, though still quite substantial, proportions of parents and youngsters report having experienced at least some incidents of disagreement, worry or anger in the family over kids' release of information to the Web. The proportions of families feeling such tensions will likely grow in coming years as new technologies for learning about individuals proliferate on the Internet. For media and marketers, information about teens is an increasingly valuable commodity. For logical business reasons they will pursue knowledge about youngsters and their families as aggressively as possible.

The task for civic society is to set up a counterbalance to their efforts that establishes norms about what is ethically and legally correct for media and marketers to do. We might note here that Federal and university research guidelines require academic investigators to get parents' permission to interview tweens and teens about something as benign as their general attitudes toward the Web. It is ironic that marketers can track, aggregate and store far more personal responses to questions by individuals in these age groups without getting any permission from parents at all.

Nevertheless, while one can agree (as almost all parents do) that teenagers should get permission from parents before giving information to sites, legislation that forces Web sites to get that permission raises complex issues. A clear drawback is that mandating Web sites to get parental permission from youngsters age 10 to 17 is impractical in an era when youngsters can discover ways to get around such requirements or forge their parents' permission.

Even if it becomes possible for a site to verify whether a visitor is or is not a teen, we have to question whether this sort of verification is socially desirable. What might be the consequences of the "electronic carding" of tweens and teens? Would many Web sites simply prohibit teens from entering rather than go to the trouble to turn off their tracking and profiling software for them? More controversially, would it mean that teens could not participate in chat rooms or listservs where information about users is systematically collected? If so, would that be infringing on the right of the youngsters to express their opinions in open forums?

Clearly, the new digital technologies are creating circumstances where society's interest in encouraging parents to supervise their youngsters is colliding with society's interest in encouraging youngsters' to speak out and participate in public discussions. We hesitate to suggest that the FTC rules that guide Web sites regarding children under 13 should be applied to youngsters 13 and over. At the same time, we reject the notion that teens should be approachable by Web sites as if they are fully responsible and independent adults in need of no parental supervision. We believe that the best policy in this area lies in aggressively encouraging family discussions of privacy norms along with limited Federal regulation.

- Our study points to the importance of urging parents and their children to talk in detail about how to approach requests by Web sites for personal and family data. Parents should not take for granted that traditional cautions such as "don't give out your name" or "don't talk to strangers" will be enough for the Web. Family members need to understand how all sorts of information about their interests can be tracked through cookies and related software without their even knowing it.
- Many parents cannot develop norms about family privacy alone. Our study and others have found that parents simply do not know enough about the Web to be aware of the way Web sites gather information and what to do about it. Here is a terrific opportunity for community groups, libraries, schools, and state and Federal agencies to work together on campaigns aimed at making information privacy a hot family topic and bringing community members together to learn about it.
- One way to get family members talking about these issues when children are relatively young (say, aged 6 through 12) is to convince parents and kids to surf the Web together. Encouraging family Web surfing, and family discussions about Web surfing, ought to be a priority of government and nonprofit organizations that care about enriching Americans' Internet experiences.
- Logically connected to encouraging community and family discussions of information privacy is the need for individuals to know what Web sites know about them. Our research shows that virtually all parents believe that they should have a legal right to that information. A Web Freedom of Information Act should be passed that allows every person access to all data, including clickstream data, that a Web site connects to his or her individual computer or name. Whether parents should have the right to access their youngsters' data should be a matter of public discussion.
- Our finding that youngsters are substantially more likely than parents to give up personal information to a Web site when increasing values are associated with a free gift supports suggestions for another Federal regulation: Web sites aimed at tweens and teens should be prohibited from offering free gifts, including prizes through sweepstakes, if those gifts are tied in direct or indirect ways to the youngsters' disclosure of information.

We fully expect that some of these suggestions will be more controversial than others. All of them will take a lot of work. But then, it will take a lot of work from many quarters of society to help maximize the benefits of the Internet for the family.

- | | | | |
|-------|--|-------|---|
| No.1 | Public Space: The Annenberg Scholars' Conference
1 - 4 March 1995 | No.18 | Free Time and Advertising: The 1997 New Jersey Governor's Race
February 1998 |
| No.2 | The State of Children's Television: An Examination of Quantity, Quality, and Industry Beliefs
17 June 1996 | No.19 | "Stand By Your Ad": A Conference on Issue Advocacy Advertising
16 September 1997 |
| No.3 | Positive Effects of Television on Social Behavior: A Meta-Analysis
17 June 1996 | No.20 | Civility in the House of Representatives: An Update
March 1998 |
| No.4 | Assessing the Quality of Campaign Discourse — 1960, 1980, 1988, and 1992
22 July 1996 | No.21 | The Second Annual Annenberg Public Policy Center's Conference on Children and Television: A Summary
9 June 1997 |
| No.5 | Call-In Political Talk Radio: Background, Content, Audiences, Portrayal in Mainstream Media
7 August 1996 | No.22 | The Minnesota Compact and the Election of 1996
April 1998 |
| No.6 | The First Annual Annenberg Public Policy Center's Conference on Children and Television: A Summary
17 June 1996 | No.23 | The 1998 State of Children's Television Report: Programming for Children over Broadcast and Cable Television
22 June 1998 |
| No.7 | Newspaper Coverage of Children's Television
24 October 1996 | No.24 | Latino American Preschoolers and the Media
22 June 1998 |
| No.8 | Information Technology and Its Impact on Catastrophic Risks
12-13 June 1996 | No.25 | The Third Annual Annenberg Public Policy Center's Conference on Children and Television: A Summary
22 June 1998 |
| No.9 | Public Policy for a Networked Nation
December 1996 | No.26 | Civility in the House of Representativies: the 105th Congress
March 1999 |
| No.10 | Civility in the House of Representatives
March 1997 | No.27 | The Internet and the Family: The View from Parents, The View for the Press
May 1999 |
| No.11 | Free Television for Presidential Candidates
March 1997 | No.28 | The 1999 State of Children's Television Report: Programming for Children Over Broadcast and Cable Television
28 June 1999 |
| No.12 | Newspaper Coverage of Children's Television: A 1997 Update
9 June 1997 | No.29 | The Three-Hour Rule: Insiders' Reactions
28 June 1999 |
| No.13 | Children's Educational Television Regulations and the Local Broadcaster: Impact and Implementation
9 June 1997 | No.30 | The Three-Hour Rule: Is it Living up to Expectations?
28 June 1999 |
| No.14 | The 1997 State of Children's Television Report: Programming for Children Over Broadcast and Cable Television
9 June 1997 | | |
| No.15 | Free Air Time and Campaign Reform
11 March 1997 | | |
| No.16 | Issue Advocacy Advertising During the 1996 Campaign: A Catalog
16 September 1997 | | |
| No.17 | The Future of Fact: An Annenberg Scholars Conference
26-28 February 1997 | | |

Philadelphia
Telephone: 215.898.7041
Fax: 215.898.2024
Email: appc@asc.upenn.edu

Washington
Telephone: 202.879.6700
Fax: 202.879.6707
Email: appcdc@pobox.asc.upenn.edu

Homepage: www.appcpenn.org

AMERICANS & Online Privacy

The System is Broken

A Report from the Annenberg Public Policy Center
of the University of Pennsylvania



By Joseph Turow, Ph.D.

Americans and Online Privacy The System is Broken

**By Joseph Turow
June 2003**

Americans and Online Privacy

The System is Broken

Overview	3
Background	5
The Study and the Population	12
Enduring Concerns about Web Privacy	16
Not Understanding Data Flow	19
Not Taking Steps to Learn	25
Agreeing With Straightforward Solutions	28
Conflicted About Whether Institutions Will Help	30
Concluding Remarks	33

OVERVIEW

This new national survey reveals that American adults who go online at home misunderstand the very purpose of privacy policies. The study is also the first to provide evidence that the overwhelming majority of U.S. adults who use the internet at home have no clue about data flows—the invisible, cutting edge techniques whereby online organizations extract, manipulate, append, profile and share information about them. Even if they have a sense that sites track them and collect individual bits of their data, they simply don't fathom how those bits can be used. In fact, when presented with a common way that sites currently handle consumers' information, they say they would not accept it. The findings suggest that years into attempts by governments and advocacy groups to educate people about internet privacy, the system is more broken than ever.

- 57% of U.S. adults who use the internet at home believe incorrectly that when a website has a privacy policy, it will not share their personal information with other websites or companies
- 47% of U.S. adults who use the internet at home say website privacy policies are easy to understand. However, 66% of those who are confident about their understanding of privacy policies also believe (incorrectly) that sites with a privacy policy won't share data.
- 59% of adults who use the internet at home know that websites collect information about them even if they don't register. They do not, however, understand that data flows behind their screens invisibly connect seemingly unrelated bits about them. When presented with a common version of the way sites track, extract, and share information to make money from advertising, 85% of adults who go online at home did not agree to accept it on even a valued site. When offered a choice to get content from a valued site with such a policy or pay for the site and not have it collect information, 54% of adults who go online at home said that they would rather leave the web for that content than do either.
- Among the 85% who did not accept the policy, one in two (52%) had earlier said they gave or would likely give the valued site their real name and email address—the very information a site needs to begin creating a personally identifiable dataset about them.
- Despite strong concerns about online information privacy, 64% of these online adults say they have never searched for information about how to protect their information on the web; 40% say that they know "almost nothing" about stopping sites from collecting information about them, and 26% say they know just "a little." Only 9% of American adults who use the internet at home say they know a lot.
- Overwhelmingly, however, they support policies that make learning what online companies know about them straightforward. 86% believe that laws that forces website policies to have a standard format will be effective in helping them protect their information.

- Yet most Americans feel unsure or conflicted about whether key institutions will help them with their information privacy or take it away. Only 13% of American adults who use the web at home trust that the government will help them protect personal information online while not disclosing personal information about them without permission.
- Similarly, only 18% trust their banks and credit card companies and only 18% trust their internet service providers (ISPs) to act that way.
- Parents whose children go online are generally no different on these attitudes, knowledge or actions than the rest of U.S. adults who use the internet at home. Like the others, most parents are concerned, confused, and conflicted about internet privacy.

These are highlights from the most recent Annenberg national survey of internet attitudes and activities. The survey raises questions about the usefulness of trying to educate American consumers in the growing range of tools needed to protect their online information at a time when technologies to extract and manipulate that information are themselves growing and becoming ever-more complex. Our findings instead indicate that consumers want legislation that will help them easily gain access to and control over all information collected about them online. At the end of this report, we therefore suggest that the federal government needs to require online organizations to unambiguously disclose information-collection policies as well as to straightforwardly describe at the start of every online encounter what has and will happen to the specific user's data.

Our examination of online Americans' attitudes, knowledge, and actions regarding their online information was carried out by ICR/International Communication Research for the Annenberg Public Policy Center of the University of Pennsylvania.¹ The study was conducted by telephone from February 5 to March 21, 2003 among a nationally representative sample of 1,200 respondents 18 years and older who said they use the internet at home. 516 (43%) of the respondents were parents of a child age 17 or younger.

Our aim was to address two critical public policy questions that had not previously been explored in depth: What level of understanding do Americans have regarding the way organizations handle information about them on the internet? And how much do they trust social institutions to help them control their information online?

¹ Thanks to Tara Jackson, Melissa Herrmann, and Jill Glather and Carol Cassel of ICR for survey and statistical help. Susannah Fox, Robert Hornik, Steve Jones, Mihir Kshirsagar, Deborah Linebarger, Mihaela Popescu, Lee Rainie, and Judith Turow generously listened at various stages of this project and provided useful suggestions. All responsibility for presentation and interpretation of findings rests with the author of this report.

BACKGROUND

An important reason that policy analysts need to know the answer to these questions relates to the absence of U.S. laws to control much of the extraction, manipulation, and sharing of data about people and what they do online. With the exception of certain personal health information,² certain types of personal financial information held by certain types of firms³, and personally identifiable information from children younger than 13 years,⁴ online companies have virtually free reign to use individuals' data in the U.S. for business purpose without their knowledge or consent. They can take, utilize and share personally identifiable information—that is, information that they link to individuals' names and addresses. They can also create, package and sell detailed profiles of people whose names they do not know but whose interests and lifestyles they feel they can infer from their web-surfing activities.

Companies continually troll for, and exploit, personally identifiable and non-personally identifiable information on the internet. They often begin by getting the names and email addresses of people who sign up for web sites. They can then associate this basic information with a small text file called a cookie that can record the various activities that the registering individual has carried out online during that session and later sessions. Tracking with cookies is just the beginning, however. By using other technologies such as web bugs, spyware, chat-room analysis and transactional database software, web entities can follow people's email and keyboard activities and serve ads to them even when they are off-line. Moreover, companies can extend their knowledge of personally identifiable individuals by purchasing information about them from list firms off the web and linking the information to their own databases. That added knowledge allows them to send targeted editorial matter or advertising to consumers. More specificity also increases the value of the databases when they are marketed to other interested data-trollers.

Marketers and media firms use consumer information in a broad gamut of ways and with varying concerns for how far the data travel. Some websites unabashedly collect all the information they can about visitors and market them as aggressively as they can to advertisers and other marketers. Though many of these emphasize personally identifiable

² These regulations relate to Health Insurance Portability and Accountability Act of 1996 (HIPPA). They resulted in the first set of federal privacy rules to protect medical information online and elsewhere. See <http://www.consumerprivacyguide.org/law/hipaa.shtml>

³ These "opt-out" regulations relate to the Financial Modernization Act (Graham-Leach-Bliley Act). For an explanation, see the Privacy Rights Clearinghouse site: <http://www.privacyrights.org/fs/fs24a-optout.htm>

⁴ The Children's Online Privacy Protection Act, which went into effect in 2000, requires online services directed at children 12 and under, or which collect information regarding users' age, to give parents notice of their information practices and obtain their consent prior to collecting personal information from children. The Act also requires sites to provide parents with the ability to review and correct information that they collect about their children. See Joseph Turow, *Privacy Policies on Children's Websites: Do They Play By the Rules?* Philadelphia: Annenberg Public Policy Center, 2001.

<http://www.appcpenn.org/internet/family/>

information, not all of them do. Tracking people anonymously can still lead to useful targeting. An important example is the Gator Corporation, which places its tracking files into people's computers when they download free software such as the KaZaA music-sharing program.

The company claims to be in 35 million computers and says that once there, "The Gator Corporation has the ability to ride along with consumers as they surf the Web. That allows us to display targeted ads based on actual behavior and deliver incredible insights."⁵ A pitch to potential clients continues:

Here's an example: Gator knows this consumer is a new parent based on their real-time and historical online behavior—looking for information on childbirth, looking for baby names, shopping for baby products. . . .⁶

Let's say you sell baby food. We know which consumers are displaying behaviors relevant to the baby food category through their online behavior. Instead of targeting primarily by demographics, you can target consumers who are showing or have shown an interest in your category. . . . Gator offers several vehicles to display your ad or promotional message. You decide when and how your message is displayed to consumers exhibiting a behavior in your category.⁷

Many individual sites aim to provide similar services to marketers, though on a more limited scale. Many collect names and email addresses and use an "opt out" approach to gather targets for email advertising by themselves or "affiliates" on topics that ostensibly relate to the site themes. Some sites link their online knowledge of individuals with data collected offline. Typically, the more prestigious sites sell that information only in aggregate to advertisers. So, for example, an online newspaper may offer to send an ad for a client to all its users who are male and own a home. Because the newspaper site serves the ad, the advertiser does not know the names of those who receive it—unless they click on the ad and respond with their names to an offer. Some well-known sites may also have deals with companies that serve ads on their sites and share the revenues. These firms place their own cookies into the computers of those who visit the websites and then track people's activities into the many other sites that affiliate with the ad-serving firms. Some of them may try to coax names and email addresses from consumers that click on their ads even if the site on which their ads appeared did not.

The idea that consumers' electronic actions are increasingly transparent has alarmed some. Critics of these sorts of activities come at them with a variety of concerns from a variety of viewpoints. Many emphasize the danger that some kinds of personal information may fall into the hands of companies or people who could take advantage of the consumer. In the wake of the anti-terror PATRIOT Act, critics also worry that various government agencies will expand the tracking and generalizing about consumers on the web that had until recently seemed to be the domain of business. They point out

⁵ [http://www.gatorcorporation.com/advertise/qtr/page_2.html?mp14], accessed on May 29, 2003.

⁶ [http://www.gatorcorporation.com/advertise/qtr/page_3.html?mp14], accessed on May 29, 2003.

⁷ [http://www.gatorcorporation.com/advertise/qtr/page_4.html?mp14], accessed on May 29, 2003.

the profound damage that errors or names on suspect lists can cause individuals and families.

Others note that sites' application of email addresses in the service of marketing has helped the proliferation of unwanted email on the web, adding to a spam epidemic that has internet users and their service providers steaming. More sociologically-inclined analysts underscore that the invisible nature of much of the tracking and sorting can lead marketers to make generalizations about consumers that the consumers don't know and don't agree with. Inferences drawn from demographics and web-surfing habits can encourage discrimination in the kinds of editorial and advertising materials a site shows consumers. Such activities will become more intense as technologies to mine data, analyze data, and tailor based on the conclusions become more efficient and cost-effective. As they expand, the activities may well lead people to feel anxious not only that they are being tracked but that they are being treated differently—for example, given different discounts—than others because of who they are and what their “clickstream” says about them.

Law professor Jeffrey Rosen poses the humanistic critique bluntly. Paraphrasing the Czech writer Milan Kundera, he suggests that “by requiring citizens to live in glass houses without curtains, totalitarian societies deny their status as individuals.” He goes on to note that spying on people without their knowledge is an indignity. It fails to treat its objects as fully deserving of respect, and treats them instead like animals in a zoo, deceiving them about the nature of their own surroundings.”⁸

Those concerned about the secondary use and sharing of data about individuals point to the European Union's rather stringent prohibitions against using data in ways for which they were not originally gathered. In the U.S., no such broad rules apply, though in the late 1990s the Federal Trade Commission advanced a set of “Fair Information Practices” reflective of principles that had been advanced in the early 1980s by the Office for Economic Cooperation and Development. These would mandate certain levels of data security on websites, provide notice to potential users of sites about the way data will be collected and used, give the users choice about allowing that collection, and provide them with access to data that have been collected to find out what firms know and determine their accuracy. They, in turn, had been the basis for guiding the FTC's enforcement of a “Safe Harbor” agreement with the European Union, whereby U.S. companies wanting to use personally identifiable data about EU citizens in the U.S. had to recognize these practices in the EU though not in the U.S.⁹

As FTC Commissioner Orson Swindle recalled in late 2002, U.S. regulatory officials tended to encourage industry self-regulation rather than the legislative mandating of these practices. “Use of the Internet for marketing and attempts to address online privacy concerns were still in their infancy, and the Commission believed that the private sector

⁸ Jeffrey Rosen, “The Eroded Self,” *New York Times Magazine*, April 30, 2000.

⁹ See D. Brown, and J. Blevins, “The safe-harbor agreement between the United States and Europe: a missed opportunity to balance the interests of e-commerce and privacy online?” *Journal of Broadcasting and Electronic Media* 46:4 (December 2002), p. 565.

would continue on its own toward better privacy practices than what federal regulation might require. More specifically, it seemed inappropriate in these formative years to prescribe regulations that would impose nontrivial costs without also achieving clear benefits.”¹⁰

By 2000, however, three of the five members of the Commission believed that industry had made insufficient progress toward developing genuine, pragmatic privacy protections for consumers. They formally recommended that the Congress enact laws to codify the Fair Information Practice principles. Congress agreed with the naysayers, however, and no such law was passed. Instead, the Federal Trade Commission has used Section 5 of the Federal Trade Commission Act (which deals with unfair and deceptive practices) to prosecute websites that present fraudulent claims about information protection.¹¹

An extreme example of the computer industry’s riposte to such concerns about privacy came from Sun Microsystems chief executive Scott McNealy in February 1999 when someone pointed out that a new Sun product might allow people to track its users’ movements. “You have zero privacy anyway,” McNealy told a questioner. “Get over it.”¹² The comment, which *The New York Times* used as its quotation of the day not long after he made it,¹³ raised consternation within the business community as well as outside it.

The more typical corporate response to concerns about online consumer privacy has been to express agreement with the goal of protecting personal information while at the same time arguing that government intervention on consumers’ behalf could be catastrophic to industry growth. A *New York Times* report in 2001 concluded that “Lawmakers . . . are bolstered in their efforts to slow the march of legislation by a flood of new studies and surveys sponsored by high-technology companies, questioning consumer attitudes about privacy and giving multibillion-dollar estimates of the costs of complying with such laws.”¹⁴ So, for example, a study in 2001 by Robert Hahn of the American Enterprise Institute, a conservative research center in Washington, concluded that complying with privacy legislation proposals would cost companies \$30 billion. A spokesperson for the Association for Competitive Technology, which paid for the Hahn study, used the findings to argue that “the costs associated with regulation appear to be higher than the benefits achieved by regulation.”¹⁵

¹⁰ Orson Swindle, “Perspectives on Privacy Law and Enforcement Activity in the United States,” *Privacy & Information Law Report*, 3:4 (December, 2002).

¹¹ Critics have argued that U.S. legislative venues for reinforcing consumer privacy rights in general are insufficient. The United States does not have a federal privacy law. Moreover, tort law does not protect the disclosure of personal data unless the data could be construed as libel or potentially embarrassing. The mere gathering of data is not actionable in courts unless the practice of gathering itself is arguably too intrusive. See Jessica Litman, “Information privacy/information property,” *Stanford Law Review*, (2000) vol. 52, pp. 1283-1313.

¹² Richard Morochove, “Sun Microsystems Lets Jini Out Of Bottle ,” *Toronto Star*, February 4, 1999.

¹³ “Quotation of the Day,” *New York Times*, March 3, 1999, Section A; Page 2; Column 6.

¹⁴ John Schwartz, “Government is Wary of Tackling Online Privacy,” *New York Times*, September 6, 2002, Section C, page 1.

¹⁵ Schwartz, “Government is Wary of Tackling Online Privacy,” page 1.

The *Times* report pointedly mentioned surveys “sponsored by high technology companies, questioning consumer attitudes about privacy.” These studies argue consistently that although much of the public had certainly become concerned about online privacy, Americans are quite alert to the particulars of their information environment. They typically understand their information options, are aware of privacy policies, and are willing to negotiate privacy demands with companies who could offer them something in return.¹⁶ Alan Westin’s Privacy and American Business consultancy has been an important promulgator of this notion that Americans make cost-benefit analyses about whether to release their information online. Beginning 1995, his analyses of surveys conducted with the Harris research organization have promulgated a tri-partite division of the online public—*privacy unconcerned*, *privacy fundamentalists*, and *privacy pragmatists*.¹⁷

Looking back in 2003, Westin noted a sharp drop in the percentage of his *privacy unconcerned* group from 22% in 1999 to 8% two years later. A correspondingly higher percentage of Americans (56% in 2002 versus 34% in 1999) believed that most businesses did not “handle personal information they collect in a proper and confidential way.” Nevertheless, Westin noted that the privacy pragmatists still formed by far the largest group of internet consumers, 58% in 2002. His description of their outlook reflects his position that most Americans take an informed cost-benefit tack in relation to their online information: “They examined the benefits to them or society of the data collection and use, wanted to know the privacy risks and how organizations proposed to control those, and then decided whether to trust the organization or seek legal oversight.”¹⁸

This description of most Americans as aware of their online privacy options supported the line by internet industry players that an accurate privacy policy on every site is sufficient for allowing consumers to understand their information options in different sites. As a result of the Children’s Online Privacy Protection Act (COPPA), the Federal Trade Commission mandated specific privacy practices and disclosures regarding children younger than 13 years. With respect to everyone else, however, the presence, form and content of privacy policies is optional, subject only to broad prescriptions for members of industry groups such as the Internet Advertising Bureau and the Direct Marketing Association. The result is a world of legalistically phrased privacy policies that typically start by assuring the consumer that the site cares about his or her privacy. The policies then run for many paragraphs; hedge with respect to many of their assurances; are ambiguous when it comes to the “affiliates” with whom they share information; don’t necessarily report whether a site purchases data offline about its registered users; generally caution that the privacy policy can change at any time (sometimes telling consumers that the site will inform them when that happens); and

¹⁶ On the development of this contention, see Oscar Gandy, “Public Opinion Surveys and the Formation of Public Policy,” *Journal of Social Issues* 59:2 (2003) 283-299.

¹⁷ A good summary is in Alan F. Westin, “Social and Political Dimensions of Privacy,” *Journal of Social Issues* 59:2 (2003) 431-453.

¹⁸ Westin, “Social and Political Dimensions of Privacy,” pp. 445-446.

often note that by clicking on an ad link a consumer may be entering a world with a privacy policy totally different from the one they are reading.

Anecdotal conversations suggest that internet experts find privacy policies hard to read and difficult to understand.¹⁹ A bold technological solution that has gained industry traction during the past few years is the Platform for Privacy Preferences (P3P). Its goal is to provide a web-wide computer-readable standard manner for websites to communicate their privacy policies automatically to people's computers. In that way visitors can know immediately when they get to a site whether they feel comfortable with its information policy.²⁰ A recent report by an AT&T Labs group found that while P3P's adoption by websites is growing, especially on the most popular sites, fewer than 10% of websites offer it.²¹

One reason that sites eschew P3P is that it requires them to transform their privacy policies into a number of straightforward answers to multiple choice questions. P3P consequently does not allow for the ambiguities, evasions and legal disclaimers that are hallmarks of such documents. Note, too, that the P3P approach does not have a facility for ensuring that websites answer the questions accurately or truthfully.

In the absence of a widespread technological solution, those concerned about the state of information privacy on the internet lobby for legislation²² at the same time that they try to educate people about how to understand what goes on. There certainly are lots of places for people to learn what happens to their information online and how to keep it secure. The popular press continually beats a refrain about the dangers of the internet for information privacy, sometimes with links to online locations to learn more. Websites of organizations as varied as the Electronic Privacy Information Center (EPIC), Privacy.org (a joint project of EPIC and Privacy International), the Center for Democracy and Technology, Internet Education Foundation, AARP, Consumer's Union and the U.S. Federal Trade Commission have exhorted consumers (and citizens) to take specific steps to protect their privacy online.

¹⁹ For an examination of privacy policies in children's websites, see Joseph Turow, *Privacy Policies on Children's Websites: Do They Play By the Rules?* Philadelphia: Annenberg Public Policy Center, March 2002. [<http://www.appcpenn.org/internet/family>]

²⁰ P3P "user agents" are built into the Internet Explorer 6.0 and Netscape Navigator web browsers. An ingenious AT&T program called *Privacy Bird* is a P3P user agent that works with Internet Explorer 5.01 and higher. It displays a bird icon on the browser that changes color and shape to indicate whether or not a web site's P3P policy matches a user's privacy preferences. The beta-version software is free. See <http://www.privacybird.com/>.

²¹ Lorrie Faith Cranor, Simon Byers, and David Kormann, "An Analysis of P3P Deployment on Commercial, Government and Children's Web Sites as of May 2003." Technical report prepared for the May 14, 2003 Federal Trade Commission Workshop on Technologies for Protecting Personal Information. [<http://www.research.att.com/projects/p3p/>]

²² For a list of "privacy, speech, and cyber-liberties bills in the 108th Congress," see the Electronic Privacy Information Center's site: http://www.epic.org/privacy/bill_track.html

ConsumerPrivacy.org, for example, provides an online guide to help readers “take control of the way your information is used.”²³ Sections include a “*how to*” guide to privacy, *top things you can do to protect your privacy*, *kids’ privacy*, *frequently asked questions*, and a *privacy glossary*. The Internet Education Foundation has a similarly wide-ranging resource called GetNetWise that is supported by various corporations. AARP provides a guide called “Online Shopping: A Checklist for Safer Cybershopping.” The Federal Trade Commission issues *FTC FACTS for Consumers* that deal with internet privacy with such titles as “Dialing Up to the Internet: How to Stay Safe Online” and “Safe at Any Speed: How to Stay Safe Online If You Use High-Speed Internet Access.” And EPIC provides an online guide to “practical privacy tools” that help internet users with such activities as surfing anonymously, eliminating cookies, achieving email and file privacy, and deleting files so that they can never be read.²⁴

A question unanswered through all the debates about information privacy and the web is whether consumers understand these approaches and how to implement them. Marketers argue that privacy notices are invaluable in helping to ease concerns over sharing information. They look with optimism to a study conducted in Spring 2001 for the Privacy Leadership Initiative (a coalition of CEOs and organizations dedicated to improving consumer privacy online). It found that consumers were increasingly paying attention to online privacy statements (82% in April 2001 vs. 73% in December 2000).²⁵

- But does concern over privacy and increased “attention” to privacy policies mean that people really understand what is happening to their information on the web?
- Are writers such as Alan Westin correct to suggest that Americans make knowledgeable, pragmatic cost-benefit analyses when they disclose data about themselves online?

This study explores these and other key questions.

²³ “Protect Your Privacy Now—Welcome to ConsumerPrivacyGuide!” ConsumerPrivacyGuide.org [<http://www.consumerprivacyguide.org/>], accessed on May 28, 2003.

²⁴ Electronic Privacy Information Center, EPIC Online Guide to Practical Privacy Tools,” [<http://www.epic.org/privacy/tools.html>], accessed May 28, 2003.

²⁵ Beth Mack, “Keep It To Yourself,” *Marketing News*, November 25, 2002, p. 21..

THE STUDY AND THE POPULATION

We decided to focus on U.S. adults who have and use internet connections at home. Surveys indicate that they can be found in about half of U.S. homes.²⁶ Of course, many people go online both at home and elsewhere, especially work, and we included them in our sample. We did not include adults who use the web only outside the home—at work or in the library, for example. The reason is that using the web in the home raises issues of personal control over information that may not be true elsewhere. Information technology personnel at work may install firewalls and filters so that employees may feel that their information is protected from outside intruders in ways that people who go online at home do not. At the same time, office workers may worry primarily about their company's surveillance of their internet activities. Adults who go online exclusively from non-domestic locations may consequently hold different concerns about privacy, and have different ways to deal with them, than those who also go online at home. This is an important topic that ought to be explored in a separate study.

Our survey was carried out by International Communication Research/ICR from January 30 to March 21, 2003. To get a rough comparison of changes in privacy concerns we repeated questions that we had asked of a nationally representative sample of parents in 2000. We added new questions that explored people's understanding of privacy policies on the internet, whether they know how to protect their online information, whether they take steps to do that, what institutions they believe will help them control their information online, and whether or not they agree that certain policy approaches would be effective in helping people to protect information about themselves on the web.

Telephone interviews, which averaged 20 minutes, were completed with a nationally representative sample of 1,200 adults age 18 and older who said responded "yes" when asked "do you use the internet at home?" We used a nationally representative RDD (random digit dial) sample to screen households for adults age 18 or older who use the internet at home. We were able to determine that 53.3% of households that we phoned had at least one household member who met our eligibility requirements. Among those households, the percentage of eligible individuals who completed an interview, or the cooperation rate, was a remarkable 66.4%. The data were weighted by age, education, and race to the 2001 consumer population survey (CPS), which asked adults ages 18 or older questions similar to that used in the internet privacy study to ascertain internet use at home.²⁷

²⁶ The CPS Internet and Computers survey (September 2001, N=143,000) found adults who use the internet at home in 54.9% households. A Centris study is more recent (February 1-28, 2003, N=7342) but also a bit more conservative because it asked respondents if they personally accessed the internet at home in the past 30 days. It found an incidence of 41%. For this survey we asked "do you use the internet at home?"

²⁷ Our unweighted data was actually remarkably similar on these categories to the CPS as well as Centris and Pew Internet and American Life surveys from 2002. We used the CPS because of its huge number of respondents (143,000) and reputation as the gold standard for weighting. The margin of error for reported percentages based on the entire sample of 1,200 is plus or minus 2.86 percentage points at the 95% confidence level. The margin of error is higher for smaller subgroups within this sample.

Tables 1 and 2 provide an introductory snapshot of the population we interviewed and its internet use. As Table 1 indicates, men and women are about equal in number; 77% designate their race as white (blacks and Hispanics together make up 13% of the total); about half are under age 45; and about half are parents of children under aged 18. Most have had at least some higher education, and while a substantial percentage say their household brings in more than \$75,000 annually, a firm claim about this population's income distribution is difficult because one fifth of the respondents did not want to reveal it.

Table 2 indicates that almost half the adult population (46%) who use the internet at home has been going online from home for fewer than five years. Currently, 62% say they use dial-up phone connections to go online, but 36% of these individuals report already being connected via cable or DSL broadband. 97% of our sample has gone online at home during the past month; 49% say they have also used it at work during that time.

Adults who go online from home also seem to enjoy the experience. As Table 2 notes 77% agreed or agreed strongly with the statement that "the more years I have the web, the more interesting it becomes." It is understandable, then, that this population also reports being quite active on the internet. 53% of the adults say they go online several times a day from home or outside home (for example, at work or the library). Fully 75% report going online from somewhere at least once a day, and 47% say they do it from home for an hour or more on a "typical" day.

The table also indicates that the great majority of adults who use the web at home rank themselves in the middle (intermediate or advanced) rather than lowest or highest range (beginner or expert) of abilities when it comes to navigating the internet. Only 14% consider themselves beginners and only 13% call themselves experts. 42% consider themselves intermediates and 30% say they are advanced. More years online, using the Internet daily, staying online an hour or more, or going online at work all increase the likelihood a respondent will increase in expertise "at navigating the web. So do higher income levels and being male.²⁸

²⁸ The optimal scaling regression method was used to explore these relationships with the ordinal dependent variable. The eight variables explained 32% of the variance. Interestingly, age shows a curvilinear relationship of age impact self-reported internet skill. That is, young people report high expertise; it drops as people get older; but then it rises again. Perhaps reported expertise increases because time spent with the internet increases among less busy older adults. More research is needed here.

**Table 1: Characteristics of U.S. Adults
Who “Use the Internet at Home”**

	US Adults, Home Internet* (N=1,200)
Sex	%
Male	49
Female	51
Age	
18-34	33
35-44	24
45-54	21
55-64	11
65+	08
No answer	03
Race	
White	77
Black	07
Hispanic	06
Other	07
No answer	04
Education	
Less than high school (HS) grad	07
High school/tech school graduate	32
Some college	22
College graduate or more	39
Family Income	
Less than \$40,000	24
\$40K but less than \$50K	10
\$50K but less than \$75K	19
\$75K but less than \$100K	13
\$100K or more	13
No answer	21
Parental Status	
Parent of child below age 18	56
Not parent of child below age 18	44

* When the numbers don't add up to 100% it is because of a rounding error.

Table 2: Internet activity, interest and self-ranked expertise of U.S. adults who “use the internet at home”

	(N=1,200)
Online connection	%
Dial-up telephone	62
Cable modem	23
DSL	13
Another method	01
Don't Know	01
Years online at home	
One or less	09
Two	09
Three or four	28
Five	13
Six	08
Seven or more	28
Don't know	04
Response to “The more years I have the web, the more interesting it becomes.”	
Agree strongly	44
Somewhat agree	33
Somewhat disagree	13
Strongly disagree	08
Neither agree nor disagree	02
Frequency online from anywhere	
Several times per day	53
About once a day	22
A few times per week	19
About once a week	04
About once a month	02
Few times a year	01
Went online last month at home or work**	
At home	97
At work	49
Typical daily time online at home	
Less than 15 minutes	12
More than 15 minutes, less than 1 hour	39
Between 1 and 2 hours	29
More than 2 hours	18
No response	03
Self-ranked expertise in navigating the internet	
Beginner	14
Intermediate	42
Advanced	30
Expert	13

* When the numbers don't add up to 100% it is because of a rounding error.

** These numbers don't add up to 100% because going online at work and home are not mutually exclusive.

ENDURING CONCERNS ABOUT WEB PRIVACY

Comparing this study with one of parents in 2000 suggests enduring concerns about web privacy. When presented with the statement “I am nervous about websites having information about me,” 76% of the beginners, 74% the intermediates and 70% of advanced users agreed. The self-designated *experts* were more likely than the others to dispute the statement, but even 57% of them agreed that they are nervous. Overall, our population confirmed what other studies have found: a clear majority of Americans express worry about their personal information on the web.

This survey went beyond a one-question expression of concern, however, to explore the attitudes and knowledge that adults who go online at home hold about what happens to their information on the internet. To begin with a rough sense of whether ideas on this topic have changed in the past few years, we included thirteen statements that we had used in a study of a more limited population in the year 2000--online parents (see Table 3). For each of the assertions, we asked our respondents how much they agreed or disagreed along a five-point continuum, from agree strongly to disagree strongly.

Table 3 allows comparison of the answers given by adults who either don't have kids or whose kids are younger than age 6 with parents with youngsters at home who fall into an age bracket (6 through 18) that make them likely to use the internet. The table also allows comparison of the current sample of parents of “internet age” children their counterparts in our 2000 study. What is most interesting is how close the percentages are, not just between parents and non-parents of internet age kids in 2003 but also between the parents of 2000 and those of today. Quite logically, the two areas of greatest difference between those with and without internet-age kids relate to a somewhat greater likelihood that the parents of those who could go online worry about what teens and “family members” might reveal to websites. Perhaps the most interesting difference between 2003 and 2000 is that a smaller percentage of people three years ago agreed that that they trust websites not to share information when they say they won't (37% vs. 50%). Parents, at least, appear to have gotten more rather than less trusting. In general, though, the responses across groups and time were strikingly parallel to one another.

Beyond reflecting concerns about outsiders invading their privacy, the pattern of answers are a springboard to four themes that speak to the major questions posed earlier:

The great majority of adults who go online at home reject the general proposition that their information is a currency for commercial barter. Only 21% agree that they like to give information to websites in exchange for offers, and only 16% agree that they will give out information only if paid. The answers mirror responses by the parent sample in 2000. They contradict analysts who characterize most Americans as quite open

Table 3: Among Adults Who Go Online at Home, the Percentage Who “Agreed” or “Agreed Strongly” With the These Statements:

	Total (N=1,200)	Non- Parents* in 2003 (N=775)	Parents* in 2003 (N=425)	Parents* in 2000 (N=902)
I should have a legal right to know everything that a web site knows about me.	94	94	95	95
Teenagers should have to get their parent's consent before giving out information online.	92	92	93	95
I am nervous about websites having information about me.	70	68	73	72
I look to see if a web site has a privacy policy before answering any questions.	71	69	72	72
My concern about outsiders learning sensitive information about me and my family has increased since we've gone online.	67	67	68	61**
I am more concerned about giving away sensitive information online than about giving away sensitive information any other way.	68	66	68	64
When I go to a web site it collects information about me even if I don't register	59	58	59	57
I would worry more about what information a teenager would give away to a web site than a younger child under 13 would.	58	53++	66	59
I trust web sites not to share information with other companies or advertisers when they say they won't.	49	50	50	37**
Web site privacy policies are easy to understand	47	45++	53	45**
I sometimes worry that members of my family give information they shouldn't about our family to web sites.	28	25++	35	37
I like to give information to web sites because I get offers for products and services I personally like.	23	21	25	17**
I will give out information to a website only if I am paid or compensated in some way.	16	16	17	10**

*Parents with children six to eighteen years. “Non-parents” means adults who do not have children six to eighteen years. ** indicates that the difference between the two samples of parents is significant statistically at the .05 level using the chi square statistic. ++ indicates that the difference between the 2003 sample of parents and non-parents is significantly statistically at the .05 level using the chi square statistic.

to giving up their information if the price is right. Philosophically, if not always in practice,²⁹ adults who use the web at home do not see their personal information as a commodity to be traded for online offers.

- **Most adults who go online at home know that websites track their behavior, but two in five are ignorant about the most basic aspect of information collection on the internet.** 59% are aware of what cookies do; they know that when they go online sites collect information on them even if they don't register. The flip side of the finding is that 40% of U.S. adults who use the internet at home are not aware of this most basic way that companies track their actions when they go online. Yet 76% of them say that "they look to see if a website has a privacy policy before answering any questions." In addition, 69% say they "always" or "sometimes" give their real email address to a website when it asks for personal information. Because privacy policies almost always mention cookies, the answers suggest that even though these people say they "look to see if a website has a privacy policy," the great proportion of online adults who aren't aware of what cookies do either don't actually read the policies or don't understand them.
- **The attitude statements also reveal that beyond being nervous over their sense of being tracked, most Americans want help to control their information.** 95% agree that they should have a legal right to know everything a website knows about them. Moreover, contrary to the U.S. government policy that teens are adults online, 92% of our respondents overwhelmingly agreed that teenagers should have to get parents' consent before giving out information online.

Comparison with the sample of parents in 2000 suggests that these key ideas are stable and generalizable. The current wider survey of all adults who use the web at home asked additional questions that aimed to deepen our understanding of them. The answers allow us to marshal more data to support the themes and add to them. We start with a question that relates to the second theme: What do adults who use the internet at home know and don't know about the way information about them is used on the web?

²⁹ Our 2000 study of parents found that 29% of parents with online connections at home said they would give their names, addresses, and preferences to a site of their "favorite" store in return for "a great free gift" worth up to \$100 and a promise not to share the information with other companies. 71% of the parents said they would not. A Forrester report concluded in 2002 that one-third to one-half of consumers are willing to give up such information as their TV viewing history and their online surfing in exchange for a \$5 monthly discount on their cable or ISP bill. Jed Kolko with James McQuivey and Jennifer Gordon, "Privacy for Sale: Just Pennies Per Day," Forrester Research *Technographics Research Brief*, June 11, 2002. The key question the Forrester study raises involves whether the respondents understood the uses that could be made of their data. The issue will be taken up in the conclusion to this paper.

NOT UNDERSTANDING DATA FLOW

Despite strong concerns about government and corporate intrusions, American adults who use the internet at home don't understand the flow of their data online. Our survey reveals a disconnect between their concern about information about them online and their knowledge about what websites do with it. Though they possess basic knowledge about the websites' acquisition and use of information about individuals, adults with internet connections at home are ignorant, even naïve, about the way data about them flows between companies behind their screens.

First, some additional privacy concerns: Our current study aimed to assess opinions about government surveillance that have arisen since the 2000 survey because of the World Trade Center destruction and the consequent "war on terrorism." As Table 4 indicates, a bit more than half of the adult population that goes online from home believes that "government agencies" are collecting information about them without their knowledge or consent. The online adults see some utility of for government surveillance. Depending on how the statement is phrased, 66% or 45% believe that the government should have the wherewithal to track evildoers (and even potential evildoers) online.

Table 4: Among Adults Who Go Online at Home, the Percentage Who "Agreed" or "Agreed Strongly" With the Following Statements:

	Total (N=1,200)
	%
Because of the war on terrorism, the government needs to make it easier for law enforcement to track users' online activities without their knowledge or consent.	66
US government agencies are collecting information about me online without my knowledge or consent.	52
In the interest of national security, the federal government should have the technology to find out what anyone is doing on the Internet at all times.	45
When a web site has a privacy policy, I know that the site will not share my information with other websites or companies.	57

And yet, the online-from-home population did not take this to mean that they were giving anyone the OK to collect information about *their* domains. Elsewhere in the interview, we asked respondents in two separate questions how concerned they would be if they found that the "US government" and "marketers" were "collecting information about

your household members' online activities without your knowledge or consent." 83% said they would be concerned if the government did it; 92% said they would be concerned if the snoopers were marketers.³⁰

Although large proportions of the online-at-home adults voiced concern about their loss of privacy on the internet, much smaller percentages seem to have had actually tangled with the issue personally. Fully 82% of those interviewed said they had never had an incident where they worried about something a family member told a website. It may be that the concerns they described in the interviews came from media or interpersonal discussions without first hand experience to make them real. This seeming lack of a direct connection to personal privacy issues may explain how in a population where high proportions of adults who say they know how to register on sites (88%), understand that sites can track them (59%), and know how to change the privacy settings on their browser (64%), 57% mistakenly agree that the mere presence of a privacy policy means that a website will not share their information with other websites or companies.

The ignorance about privacy policies is, however, only the tip an iceberg of confusion about what goes with personal information behind the computer screen. The reactions of most online-at-home adults to a common way websites handle visitors' information indicate that they do not grasp the way their identifiable and anonymous data is collected, interrelated and used.

We presented the people interviewed with a supposed change in the information policy of a website that they had previously said they "like most or visit regularly from home." The goal was to gauge the acceptability of a common version of the way sites track extract and share information to make money from advertising. Unfortunately, it is impossible to determine an "average" or "typical" approach to information by websites. One reason is that it is not clear how to determine an average or typical website. More important, a website's approach to its visitors' information is by no means fully described in its privacy policy, long and tortuously worded though it may be. No law requires websites to disclose all aspects of their relationship to their visitors' information. The advertising trade press and conversations with people in the business, for example, makes clear that more than a few sites purchase offline data about individuals to append to data gathered during registration. The sites rarely divulge such transactions in their privacy policies, however.

Coming up with the description of a rather common privacy policy involved combining the experience of reading hundreds of privacy policies with a wide reading of the trade press on privacy-policy issues. The goal was to reflect the complex ways in which websites intend to explore patterns of visitors' personal and clickstream data with an eye toward selling them to advertisers. Most of the transactions using visitors' data are offered to advertisers in aggregate—that is, anonymously lumping people with one or another characteristic together for ad-targeting purposes. Some sites, however, do offer

³⁰ 50% of the respondents said they would be "very concerned" and 33% said they would be "somewhat concerned" if the government tracked them. 68% said they would be "very" and 24% "somewhat" concerned if marketers tracked them.

personally identifiable information directly to advertisers and say so in their privacy policies. Many sites say they share personally identifiable information only with so-called “affiliates”—though they rarely name them. Many more sites make it clear that if visitors click on advertising links, names given there (in contest registration, for example) may be used in ways counter to the website’s policies. Websites also point out that they may change their policy at any time, and not all promise to keep previously collected data under the old regime. We strove to create an approach to personal information that would embody these data transactions along with their typical uncertainties and ambiguities without being too long.

We read the result to five web experts from academia, business, government and social advocacy groups who agreed that what we would be presenting was a common version of a site’s approach to information. Accordingly, we integrated the hypothetical scenario into the questionnaire. After several questions asking them about the type of website, whether or not they registered to get in, whether or not they pay a subscription to use it, and if so, how much, we posed the situation this way.

SUPPOSE THE WEB SITE THAT YOU LIKE MOST AND USE REGULARLY SAYS THAT IN ORDER FOR IT TO CONTINUE OPERATING IT MUST CHARGE USERS \$6 A MONTH.³¹ IF YOU PAY, THE SITE WILL SHOW YOU ADS BUT IT WILL NOT USE PERSONAL INFORMATION ABOUT YOU TO MAKE MONEY FROM OUTSIDE ADVERTISERS. OR YOU CAN GET THE SITE FOR FREE IN EXCHANGE FOR ALLOWING THE WEB SITE TO USE PERSONAL INFORMATION ABOUT YOU TO MAKE MONEY FROM ADVERTISERS. IT WILL LEARN ABOUT YOU BY GETTING YOUR NAME AND MAIN EMAIL ADDRESS, BY BUYING PERSONAL INFORMATION ABOUT YOU, AND BY TRACKING WHAT YOU LOOK AT ON THE SITE. THE SITE WILL NOT DIRECTLY TELL ADVERTISERS MOST OF THE INFORMATION IT LEARNS, THOUGH IT MAY TELL ADVERTISERS YOUR EMAIL ADDRESS. IT WILL SEND ADS TO YOU FOR ITS ADVERTISERS BASED ON THE INFORMATION IT LEARNS. FOR EXAMPLE, IF YOU CLICK ON FOOTBALL LINKS, IT MAY CONCLUDE THAT YOU LIKE SPORTS, BELONG TO A PARTICULAR AGE GROUP, AND PROBABLY DRINK BEER. THE SITE WILL SEND YOU ADS ON THE SITE, THROUGH EMAIL AND MAYBE THROUGH POSTAL MAIL, BASED ON THE INFORMATION IT LEARNS.

SO, IF THE SITE YOU LIKE MOST AND USE REGULARLY SAYS IT MUST CHARGE YOU OR USE YOUR INFORMATION TO MAKE MONEY FROM ADVERTISERS,
WHAT WOULD YOU DO? WOULD YOU

- 1 AGREE TO PAY TO USE THE SITE SO THAT THE SITE CANNOT USE YOUR PERSONAL INFORMATION TO MAKE MONEY FROM ADVERTISERS?
- 2 AGREE TO GET THE SITE FOR FREE IN EXCHANGE FOR ALLOWING THE SITE TO USE YOUR PERSONAL INFORMATION TO MAKE MONEY FROM ADVERTISERS?

³¹ If the respondent was already paying, we changed this amount to the number he/she had previously given plus a sliding extra number of dollars based on the existing payment; it typically came to \$2 extra. 11% of the respondents told us they were paying to use their valued site. Monthly payments ranged from \$2 to \$100; the average monthly payment reported was \$21.

- 3 LOOK FOR A SUBSTITUTE WEB SITE THAT DOES NOT CHARGE? OR
- 4 GIVE UP LOOKING FOR THAT TYPE OF CONTENT ON THE WEB?

[IF THE RESPONDENT CHOSE #3, WE THEN EXTENDED THE SCENARIO TO FORCE A CHOICE, AS FOLLOWS:]

SUPPOSE YOU CANNOT FIND A SUBSTITUTE WEB SITE THAT DOES NOT CHARGE,
WHAT WOULD YOU DO THEN? WOULD YOU--

- 1 AGREE TO PAY TO USE THE SITE SO THAT THE SITE CANNOT USE YOUR PERSONAL INFORMATION TO MAKE MONEY FROM ADVERTISERS?
- 2 AGREE TO GET THE SITE FOR FREE IN EXCHANGE FOR ALLOWING THE SITE TO USE YOUR PERSONAL INFORMATION TO MAKE MONEY FROM ADVERTISERS?
- 3 GIVE UP LOOKING FOR THAT TYPE OF CONTENT ON THE WEB?

Table 5 presents the initial answers from the respondents who could think of websites that they “like most or visit regularly from home.”³² Note that only 10% agreed to continue getting the site for free in return for agreeing to this common version of the way sites handle personal information from advertising. Oddly, 21% said straight out they would give up looking for that type of content on the web when presented with such a choice. Perhaps they were angry that a site would give them this sort of choice. 18% said they would rather pay to use the site than agree to give up their information, while almost half—48%—suggested that they would try to retain their information and money by looking for a substitute site.

Table 5: If the site ... says it must charge you or use your information ..., what would you do?”*

	Total (N=919)
	%
Agree to get site for free and give up information	10
Agree to pay to use the site	18
Look for substitute site that doesn't charge	48
Give up looking for that content on the web	21
Don't know / refused	03
Total	100

* See text for explanation.

When the second question blocked this way out, only a small percentage of those stymied decided to use the marketing deal for free access to the valued site. Table 6 presents the

³² Approximately 12% (140) of the 1200 people in the same could not think of such a site, so they were not asked the questions. In addition, an error caused another 142 people in our sample were not to get the questions. (The error did not systematically bias the kinds of people who received the hypothetical scenario.) Overall, then, 918 respondents answered this set of questions.

final decisions of all the respondents—the people who did and those who did not first say they would look for a substitute site. The central finding is that 85% of our sample did not accept an approach to privacy that is common on today's internet. Moreover, while 27% said they would pay for the site, a bit more than half—54%—contended that when presented with this website approach to their information they would rather give up looking for that type of content on the web than either pay or accept the information policy.

Table 6: Final decisions of all respondents regarding scenario*

	Total (N=919)
	%
Agree to get site for free and give up information	15
Agree to pay to use the site	27
Give up looking for that content on the web	54
Don't know / refused	04
Total	100

* See text for explanation.

The massive rejection of what is actually a common version of the way sites track, extract, and share information to make money from advertising suggests that adults who go online at home overwhelmingly do not understand the flow, manipulation and exchange of their data invisibly during and after they go online. Other findings indicate that a substantial subset of the people who refused to barter their information is especially ignorant about information activities on the web. Among the 85% who did not accept the marketing deal, about half (53%) had earlier said they gave or would be “very” or “somewhat” likely to give the valued site their real name and email address. Yet those bits of information are what a site needs to begin creating a stream of data about them—the very flow (personally identifiable or not) that they refused to allow in response to the scenario. Moreover, 63% of the people who said they had given up these data had also agreed that the mere presence of a website privacy policy means that it won’t share data with other firms. Bringing these two results together suggests that least one of every three of our respondents who refused to barter their information either do not understand or do not think through basic data-collection activities on the internet.³³

³³ As it turns out, the 15% of our sample who accepted the marketing deal did understand privacy policies and data collection any better than the others. 67% believed that when a web has a privacy policy it will not share knowledge (not a statistically significant difference from those who rejected the deal), though 58% indicated an awareness of cookies (not a statistically significant difference with the others). 39% both knew of cookies and misunderstood the presence of privacy policies—also not different from the other group. What makes these people stand from the 85% is not their knowledge; they too seem ignorant and confused. It is, rather, their seeming willingness to give up data whether or not they know what is happening to that information: 80% of this group (compared to 53% of the other) had earlier indicated they had or would likely give their real name and email address to the site.

The converging results point to a confusion about the nature of information gathering on the web. Although web users seem to be responding to public discussions of cookies as repositories of specific data about them—and while that in itself (rather than bad personal experience) seems to make them concerned—they do not understand that this collection of individual bits of information relates to a larger set of activities that involve the tracking, mining, and sharing of data. When they learn about it—as when we read them the scenario—they refuse to accept it as legitimate.

We found additional evidence that a substantial majority the online-at-home adults does not understand—and would reject—the complex ways websites and marketers extract and interrelate data about them. Those findings came as the result of a second scenario we created for the 440 people who said that they would go to a substitute site for favored content rather than pay or give up information. We told them to suppose that they agreed to let the substitute site track their movements and link them to other information about them. We then asked what their reaction would be if the focus of the information tracked would be their fashion preferences, political interests, health or medical history, gender, and financial information. Would they agree to pay so as not to be tracked, allow tracking and get the site for free, or give up looking for that content on the web?

As other studies have found, we noted variations in people's sensitivities to different topics when it comes to privacy. For both financial information and health or medical history, 84% of the respondents said they would give up looking for favorite content on the web than pay for the site or allow that information to be tracked and shared by marketers. When it came to political preferences, 75% said that if those were tracked they would give up looking for their favorite content on the web. With gender and fashion preferences, a smaller percentage contended they would abandon favorite content on the web. Even there, though, substantially more than half of the respondents (63% and 67%, respectively) say they would leave the web rather than pay or be tracked was high.

When one considers that people often give out their gender, fashion preferences, and even political preferences to websites and pollsters, these numbers appear bizarrely high. That is particularly the case considering that an average of 61% of those who said they would give up looking for content earlier said that they had or would likely share their real name and email address with the site. The pattern of answers suggests that their concern went beyond the nature of the information that would be released about them. Rather, it reflected worries about—perhaps even indignation over—what they learned regarding the website's tracking, manipulation, and sharing of data about them.

NOT TAKING STEPS TO LEARN

Not only do adults who use the web at home tend to be confused about data-collection activities, they tend not to take steps to learn about ways to control their information online. When asked how often they searched for “instructions on how to protect information about yourself on the web?” 64% answered never, while 25% said “a few times; 5% said “only once” and 6% said “many times.” In answer to another question, 40% of adults who use the internet at home also told us that they know “almost nothing” about how to stop websites from collecting information about them.

We turned to the 60% of the population who said that they know more than “almost nothing”—that is, those who indicated at least some understanding about controlling their online information. We asked them whether they feel they have applied what they do know in ways that are sufficient. Only 5% agreed that they had carried out “everything that needs to be done” to stop websites from “collecting personal information” without their “knowledge or consent.” The majority of people who have at least some knowledge about privacy control said they have done “some but not enough” to stop information collection. 20% said they have carried out either very little or nothing of what needs to be done.

Table 7 presents specifics about what all our respondents said they have actually ever carried out in relation to controlling their information. Fully 65% said that they have erased unwanted cookies at least once. This finding is consistent with our earlier realization that a clear majority of the sample is aware that cookies are a key component of information retrieval. The percentage applied other privacy tools drops steeply from there, however. 43% said that they have used filters to block unwanted email, 23% said they have used software that looks for spyware, and an even smaller percentage said they have used anonymizers—“software that hides your computer’s identity from websites that they visit.”

To gauge how experienced individuals are with the range of these practices, we gave them scores based on the number they reported performed. Four points went to people who said they have carried out all of these activities, three to those who have done three of them, and so on. We found that fully 25% had not carried out any of these information-controlling activities (we called them *highly inexperienced*). 31% had carried out one task (*inexperienced*). 25% were in the middle with two of the four (*neither experienced nor inexperienced*), only 11% fell into the *experienced* slot, and an even smaller 8% claimed to be *highly experienced*—having at least some skill at carrying out four of the four information-controlling activities.

Table 7: Have you ever--

	Yes %	No %	Don't Know %	Total % **
Erased all or some of the unwanted cookies on your computer?* (N=1200)	65	33	2	101
Used filters to block unwanted email? (N=1200)	43	57	1	101
Used software that looks for spyware on your computer.* (N=1200)	23	76	2	101
Used software that hides your computer's identity from web sites that you visit. (N=1200)	17	81	2	100

* If respondent asked what cookies are, the interviewer said, "Files internet firms place in your computer to track your movements on the web. If respondent asked what spyware is, the interviewer said, "Software that records every keystroke made on a computer."

** Total percentages exceed 100 because of rounding error.

One might expect that the amount people say they know or do to control their information would relate to the way they rank their ability to navigate the internet. And, in fact, a much higher proportion of those rated as highly experienced or experienced compared to everyone else (27% versus 8%) said that they know "a lot" about stopping web sites from collecting their personal information without consent. Similarly, 40% of the experienced categories compared to 20% said they know "some" about the subject. The same tendencies applied when we asked the people who said they knew more than "almost nothing" about how to control their information. People who were ranked *highly experienced* or *experienced* were far more likely than the others to say they carry out "everything that needs to be done" or "some but not enough" as opposed to very little or nothing.

For those who want to encourage more citizens to control their information online, an obvious path is to cultivate internet users who are experienced with privacy-protecting technologies. At present only 19% of adults who go online from home fall into either the *highly experienced* or *experienced* categories. The rest—from *neither experienced nor inexperienced* through *highly inexperienced*—are both much less knowledgeable and much less active about controlling their online data.

Unfortunately, we could not find out what characteristics or activities foretell whether or not a person will be more or less experienced in this regard. We used a statistical technique called optimal scaling regression. It helped us explore whether a variety of background characteristics that we expected would encourage concern with online privacy would, in fact, predict a higher score on privacy-tool experience. In addition to demographic characteristics such as age, income, race, education, and gender, and region of the country, we were interested in whether having a child aged six to seventeen who uses the internet leads someone to learn more privacy tools. We also thought that incidence of internet use and self-reported ability to navigate the web might pay important roles in leading a person to be privacy-tool experienced.³⁴

³⁴ In our model, *incidence of internet use* involved three variables—years on the internet (prior to 1997 to present—2003), use/non-use of the internet at home during the past month, daily vs. weekly use of the

It turned out that among all the variables, only the time spent online (specifically, weekly versus daily and spending more than one hour on the internet) could be seen to impact involvement with privacy tools. Our statistical technique indicated, however, that even these variables predicted only 7% of the factors that drive experience with them. Overall, our model accounted for just 11% of the variance and so explains little about why certain individuals learn a number of ways to control their information online and others do not.

internet, and spending minutes vs. hours online. Linear relationships were test for age and income. Curvilinear relationship was also tested for age.

AGREEING WITH STRAIGHTFORWARD SOLUTIONS

Possibly because of their ignorance of what happens to their information online and how to control it, adults who use the internet at home agree widely and strongly when presented with solutions that let them know straightforwardly what is going on.

They strongly support regulations that force more disclosure from online entities. We have already seen in Table 3 that 95% of adults who use the internet at home agreed or agreed strongly that they should have the legal right to know everything websites know about them. 92% agreed or agreed strongly that teens should be required to get their parent's consent before giving out information online. The table does not reflect the intensity of those answers: 86% percent agreed *strongly* with the first proposition and 76% agreed strongly with the second. 80% also agreed strongly and an additional 14% simply "agreed" with the statement, not presented in Table 2, that "websites should be required to ask my permission before sending ads to me."

The respondents also agree that government regulations would be effective if they gave people leverage with online entities to control information about themselves. That sentiment came through in a series of questions toward the end of the interview. As the next-to-last questions before requesting basic demographic information, we asked about three potential policies in the following way:³⁵

COMPANIES SOMETIMES COMBINE ALL OF THE PERSONAL INFORMATION THEY COLLECT ABOUT YOU FROM YOUR ONLINE ACTIVITIES AT DIFFERENT SITES INTO A PROFILE OF YOU WITHOUT YOUR KNOWLEDGE OR CONSENT. PLEASE TELL ME IF YOU THINK A **LAW THAT REQUIRES WEBSITE PRIVACY POLICIES TO HAVE UNDERSTANDABLE RULES AND THE SAME FORMAT** WOULD BE VERY EFFECTIVE, SOMEWHAT EFFECTIVE, NOT VERY EFFECTIVE, OR NOT AT ALL EFFECTIVE WAY TO REGULATE THESE ACTIVITIES.

[AFTER THE ANSWER:] HOW ABOUT A **LAW THAT REQUIRES COMPANIES THAT COLLECT PERSONAL INFORMATION ONLINE TO HELP PAY FOR COURSES THAT TEACH INTERNET USERS HOW TO PROTECT THEIR PRIVACY ONLINE?**

[AFTER READING THE CHOICES AND GETTING THE ANSWER:] HOW ABOUT A **LAW THAT GIVES YOU THE RIGHT TO CONTROL HOW WEBSITES USE AND SHARE THE INFORMATION ABOUT YOU?** [READ CHOICES AND GET ANSWER.]

As Table 8 indicates, broad support emerged for all three policies. There is an important difference, however, in the response to the third policy in relation to the first two.

³⁵ The policies in italics were actually rotated so that different respondents received them in a different order. The actual last question before soliciting the demographic information was "when the current generation of teenagers in America reaches adult hood, do you think it will be much more, a little more, a little less or much less concerned about protecting information collected online than adults today?"

Compared to a law that would help them learn how to control their privacy, substantially more of those interviewed believed that legislation requiring easy-to-understand rules and the right to control information would be “very effective.” Although people do not dismiss the possibility that formal learning about privacy tools can help society deal with information control, they seem to believe that government and corporate action that helps them learn straightforwardly what is going on is preferable.

Table 8: Among adults who go online at home, the percentage responses to the policies’ probable effectiveness

	How Effective?*				
	Very %	Somewhat %	Neither Effective nor Ineffective* %	Not Very %	Not at All %
A law that requires website policies to have easy to understand rules and the same format. (N=1200)	40	46	0.5	8	4
A law that gives you the right to control how websites use and share the information they collect about you. (N=1200)	41	43	0.5	10	5
A law that requires companies that collect personal information online to help pay for courses that teach internet users how to protect their privacy online. (N=1200)	28	46	0.5	15	10

* Those small numbers who said “don’t know” (2% and less) are not included. The people who said “neither effective nor ineffective” volunteered that answer.

CONFlicted about whether institutions will help

Yet online-at-home adults feel conflicted about whether the government or key corporate institutions will help them with their information privacy or take it away. We learned that by comparing two related sets of answers in our interviews. Each set asked about the same six institutions—the respondent’s internet service provider (ISP), banks or credit card companies, major advertisers, Microsoft³⁶, privacy protection software, and “the government.” We asked the person interviewed to “think about your ability during the next five years to control personal information online.” In the first question set, the respondent was asked for every institution to note on a “on a scale of 1 to 5, with 5 being most important and 1 being least important, how important a role” that institution “will play in helping or teaching you to protect your information online.” In the second set, for every institution the respondent was asked to note on a “on a scale of 1 to 5, with 5 being most likely and 1 being least likely, how likely will” that institution “be to release or share information about you by accident or on purpose without your knowledge or consent.”

Table 9 lays out the average (mean) answers on the scale of 1 to 5 that each institution received for each question. In the interviews, numbers 1 and 2 indicated low levels of importance on the set of questions about the institution’s role in protecting information. The numbers also indicated low levels of likelihood on the set of questions about the institution’s likelihood to disclose information. 4 and 5 indicated high levels of importance or likelihood. We interpreted a response of 3 to mean neither high nor low.

As Table 9 indicates, adults who go online at home tend to consider major advertisers the least important of the six institutions to help them protect their information and the most likely to disclose it without consent. The adults also tend to see makers of privacy protection software as the most important of the six institutions to help them protect their information and the least likely to disclose it without consent.

The findings about advertisers and makers of privacy protection software are not really surprising. Concern about spam, the popular press’ focus on marketers’ use of cookies on the web, and a long history of distrust of advertisers in U.S. society make it logical that people would consider them least helpful in protecting information and most likely to disclose it. Similarly, constant injunctions in the press about the importance of virus protection software have given that part of the internet industry a favorable image that may well have rubbed off on “privacy protection software makers.” It should be noted—and the means suggest—that these sentiments were by no means unanimous. Only 45% of the respondents indicated through a 1 or 2 that advertisers would be unimportant to helping protect their privacy. 32% thought they would be important (a 4 or 5), while 21% believed neither. And, while 64% did agree that advertisers would likely share their information, 17% said it was unlikely and 18% said neither. Roughly the same

³⁶ Though it is only one company, Microsoft’s fundamental influence on the digital world led us to include it here even though our other examples were groups of organizations.

numbers—but reversed for the two questions—apply to the privacy-software manufacturers.

Table 9: How important will institutions be for helping protect your information? How likely will institutions be to release your information?

	Mean Response on Protect	Mean Response on Release	Difference Between Means	Effect Size
Major advertisers (N=1175*1185)	2.78	3.79	-1.01	-.88
Microsoft (N=1165*1156)	3.45	3.20	.25	.10
The government (1179*1171)	3.53	3.26	.27	.24
Banks/credit card companies (N=1189*1181)	3.75	3.32	.43	.34
Internet service providers (N=1189*1183)	3.68	3.19	.49	.47
Makers of privacy protection software (N=1177*1165)	3.86	2.97	.89	1.18

On “protect”: 5 is “most important.” On “release”: 5 is most likely. See text. The means in every pair are statistically significant using the paired-samples t test. Standard deviations going down the first column of means are 1.471, 1.331, 1.382, 1.390, 1.247, and 1.164. Standard deviations going down the second column of means are 1.371, 1.284, 1.411, 1.413, 1.283, and 1.350. The different N for each variable and column reflects that “don’t know” and “refused” were not calculated in the means.

Lack of homogeneity in these answers also applies to the other institutions in Table 9. What is particularly noteworthy about Microsoft, the government, banks/credit card companies, and internet service providers, however, is that all their means in the table exceed 3 (that is, they fall in the “important” and “likely” range) on both the first and second of questions. Moreover, the differences in these means, while statistically significant, are small—less than .5. Their *effects size*, a widely accepted measure of the extent to which these differences between means really make a difference, range from relatively small (for Microsoft and the government) to small-to-moderate (banks/credit card companies and internet service providers).³⁷

Taken together, these findings indicate two related points: First, respondents tend to rank the institutions as somewhat more important for protecting their information as for having the likelihood to disclose it. But two, the effect sizes reflect that the proportions of respondents who believe the institutions are important for helping them protect their information are not that different from the proportions who believe that they will likely disclose their information without people’s knowledge or consent. An example with percentages might make the point a bit clearer: While 51% of the respondents said that the government would be important to helping protect privacy, 44% said that the government would likely disclose information about them.

An obvious question then arises: What proportion of respondents believes both? That is, how many suspect an institution that actively helps them pursue their privacy concerns also surreptitiously discloses their information? By contrast, how many respondents trust

³⁷ The effects size was calculated by dividing each mean in the pair by its standard deviation (to standardize it) and then subtracting the resulting two numbers.

an institution to actively help them pursue their privacy concerns without then disclosing their information? And more: How many do not trust the institution to help them, are caught in a conflict about the institution's information protecting and disclosing activities, or for some reason have not formed a strong opinion on the relationship between the institution and their privacy?

To answer, we created a new variable that merged the answers to the two sets of questions on each institution. If a respondent answered that an institution would be important in helping to protect information online and then said it would be unlikely to disclose information, we considered that the person *trusts* the institution to actively help with information privacy. If a respondent answered that the institution were unlikely to help in protecting information but then said it would be likely to disclose information, we considered that the person *does not trust* the institution to actively help with information privacy. If the person indicated that the institution was “unimportant” with helping to protect information *and* “unlikely” to release it—or “neither”—we considered the respondent felt *neither trusting nor untrusting* toward the institution when it came to information privacy. Finally, if the respondent indicated that the institution would be important in helping to protect online information but then also indicated that the same institution would likely disclose personal information, we considered that person *conflicted*.

Table 10: Trust / distrust that institution will help protect information online and not release it without knowledge or consent.

	Distrust %	Neither %	Trust %	Conflicted %
Major advertisers (N=1198)	40	34	4	23
Microsoft (N=1189)	15	50	12	23
The government (N=1191)	17	43	13	26
Banks/credit card companies (N=1198)	16	35	18	31
Internet service providers (N=1196)	16	35	18	31
Makers of privacy protection software (N=1188)	8	45	25	23

The different N for each variable reflects when respondents said “don’t know” or “refused” on both “protect” and “release.” See text.

Table 10 presents the results of this analysis for all six institutions. It shows that with the exception of major advertisers, straight trust or distrust is not the mode when it comes to information privacy. Between one-third and half of the respondents simply sit on the fence, not believing that they can trust or distrust an institution when it comes to privacy. Between one-third and one quarter of the rest are conflicted about how these key institutions of the digital world relate to their privacy. They seem to feel that while institutions will help them with control their information online, those same institutions (or other parts of them) will also take that information privacy away.

CONCLUDING REMARKS

The findings in this report must be dispiriting for those who believe in giving citizens the wherewithal to control their information on the internet. We found that despite their strong concerns about online privacy, most adults who use the internet at home misunderstand the purpose of a privacy policy. Just as important, our findings indicate that despite fairly wide awareness that websites collect information about them, adults who use the internet at home are fundamentally unaware of data flow: how organizations glean bits of knowledge about individuals online, interconnect those bits, link them to other sources of information, and share them with other organizations.

This ignorance of data flow stands at the heart of the imbalance of power that currently exists when it comes to controlling personal information online. In many ways, it is the ability to mine and manipulate data about individuals that makes interactive digital media such as the internet so attractive to marketers and governments. The activity is in relative infancy, but it is likely to grow enormously in presence and profits during the coming decades. Marketers and media firms, for example, see increased sophistication in real-time transactional databases as critical to the success of audience targeting, content-tailoring, and customer relationship management activities of the twenty-first century.³⁸

When consumers are unaware of the data flows that take place behind their screens, they cannot really engage in the kinds of informed cost-benefit analyses that writers such as Alan Westin suggest take place when consumers “pragmatically” give up information about themselves. What consumers can’t evaluate are the costs involved when marketers or governments hitch seemingly trivial information the consumers have allowed them to track, such TV viewing habits or fashion interests, to other knowledge in order to create powerful profiles about them. Correct or not, the profiles can impact people’s lives in ways they can’t control for lack of knowledge. Online and offline media might change content depending on what the media firms and their advertisers “know” about them. The consumers might receive different ads and different discounts than they had in the past. Government agencies might pay more or less attention to them than to others.

This study found that when adults who use the internet at home are brought face-to-face with a common approach to collecting, interconnecting and using their online information, they overwhelmingly reject it. It is also important to note, however, that these people don’t go out of their way to learn what is going on with their online information. 64% say they have never searched for instructions on how to “protect information” about themselves on the web. Large percentages of online-at-home adults have little, if any, experience with basic internet privacy tools.

Why haven’t these people tried to understand what happens to their information online and what to do about it? One reason may simply be that they have many other things to

³⁸ See Joseph Turow, “Marketing Trust and Surveillance in the New Media World,” presented at *The New Politics of Surveillance and Visibility* conference, University of British Columbia, May 23-25, 2003.

do—56% are parents of a child under age 18, for example. Our survey also suggests a more basic, though related, reason: so far, they personally haven't suffered from it.

Recall that 82% of those interviewed said they had never had an incident where they worried about something a family member told a website. Recall, too, our finding that 77% of the respondents said that the more years they have the web, the more interesting it becomes. Add to those findings both a misperception that all privacy policies provide at least some security and the fact that data flows take place invisibly, behind the screen, while a person is engaged with what is on it. In this context, it is not at all difficult to understand why adults who say they are concerned about the collection of information online without their permission nevertheless know and do little about it.

Based on these findings, one wonders whether it is realistic to believe that most American consumers can be educated successfully about ways to protect their online information. The ignorance we found comes at a time when news and entertainment media constantly din people about online dangers. Moreover, there are currently many places online and off for people to learn about privacy protection tools. It may be that it will take a data-gleaning disaster—with publicity matching that of Enron's meltdown—to energize people to learn how to control their information. An alternative view is that technologies to extract and manipulate information about audiences for digital interactive media are becoming ever-more complex. Competitors vie with each other for the best approaches while trying to get around privacy-enhancing technologies. Perhaps it may be too much to expect ordinary people to keep up. It seems clear that, at the very least, that people need active help in protecting their information.

From that standpoint, it is particularly disconcerting that we found that such a small percentage of adults who use the internet at home trust key internet-related institutions to actively aid them protect their information while not also disclosing it without their consent. The largest percentage claims no strong stance on the subject—they neither trust nor distrust—while the second-largest proportion believes that institutions talk differently from different sides of their mouths: one side helps protect personal information while the other accidentally or purposefully releases personal information to outsiders without permission.

Adults who use the internet at home, then, know that they do not have the knowledge to control their information and are not sure whether major entities who have that knowledge will act in consumers' best interests. It therefore makes sense that when offered policy choices our respondents overwhelmingly agree with solutions that let them know straightforwardly what is going on. They strongly support regulations that force more disclosure from online entities. They also strongly agree on the effectiveness of government regulations that give people leverage with online entities to control information about themselves.

Bringing together this study's findings suggests that three policy initiatives are needed to address citizens' desire to control their information in direct, straightforward ways:

- First, federal legislation ought to require all websites to integrate the P3P protocols into their privacy policies. That will provide a web-wide computer-readable standard for websites to communicate their privacy policies automatically to people's computers. Visitors can know immediately when they get to a site whether they feel comfortable with its information policy. An added advantage of mandating P3P is that the propositional logic that makes it work will force companies to be straightforward in presenting their positions about using data. It will greatly reduce ambiguities and obfuscations about whether and where personal information is taken.
- Second, federal legislation ought to mandate data-flow disclosure for any entity that represents an organization online. The law would work this way: When an internet user begins an online encounter with a website or commercial email, that site or email should prominently notify the person of an immediately accessible place that will straightforwardly present (1) exactly what information the organization collected about that specific individual during their last encounter, if there was one; (2) whether and how that information was linked to other information; (3) specifically what other organizations, if any, received the information; and (4) what the entity expects will happen to the specific individual's data during this new (or first) encounter. Some organizations may then choose to allow the individuals to negotiate which of forthcoming data-extraction, manipulation and sharing activities they will or won't allow for that visit.
- Third, the government should assign auditing organizations to verify through random tests that both forms of disclosure are correct—and to reveal the results at the start of each encounter. The organizations that collect the data should bear the expense of the audits. Inaccuracies should be considered deceptive practices by the Federal Trade Commission.

The three proposals follow the widely recognized Federal Trade Commission goals of providing users with access, notice, choice, and security over their information. Companies will undoubtedly protest that these activities might scare people from allowing them to track information and raise the cost of maintaining databases about people online. One response is that people, not the companies, own their personal information. Another response is that perhaps consumers' new analyses of the situation will lead them to conclude that such sharing is not often in their benefit. If that happens, it might lead companies that want to retain customers to change their information tracking-and-sharing approaches.

The issues raised here about citizen understanding of privacy policies and data flow are already reaching beyond the web to the larger digital interactive world of personal video recorders (such as TiVo), cell phones, and personal digital assistants. At a time when technologies to extract and manipulate consumer information are becoming ever-more complex, citizens' ability to control their personal information must be both more straightforward and yet more wide-ranging than previously contemplated.

OPEN TO EXPLOITATION:

American Shoppers Online and Offline

JOSEPH TUROW,
LAUREN FELDMAN,
&
KIMBERLY MELTZER

A Report from the Annenberg Public Policy Center
of the University of Pennsylvania

Joseph Turow is Robert Lewis Shayon Professor of Communication at the University of Pennsylvania's Annenberg School for Communication. His published work includes more than sixty articles and nine books on the mass media, including *Niche Envy: Database Marketing and American Life* (MIT Press, forthcoming), *The Wired Homestead* (MIT Press, 2003, edited with Andrea Kavanaugh); and *Breaking Up America: Advertising and the New Media World* (University of Chicago Press, 1997; Chinese edition, 2004). He currently serves on the editorial boards of *Journal of Broadcasting and Electronic Media*, *New Media and Society*, *Journalism*, and *Poetics*.

Lauren Feldman and Kimberly Meltzer are both Ph.D. candidates at the University of Pennsylvania's Annenberg School for Communication.

Open to Exploitation:
American Shoppers Online and Offline

By Joseph Turow, Lauren Feldman, and Kimberly Meltzer
June 2005

Open to Exploitation: American Shoppers Online and Offline

Overview	3
Background	6
The Study and the Population	13
Lacking the Knowledge	17
Concerns and Objections	21
Linking Attitudes and Backgrounds to Knowledge	27
Concluding Remarks	30

OVERVIEW

Most Americans who use the Internet have little idea how vulnerable they are to abuse by online and offline marketers and how the information they provide can be used to exploit them.

That is one conclusion from this unprecedented national phone survey conducted by the Annenberg Public Policy Center. The study indicates that many adults who use the internet believe incorrectly that laws prevent online and offline stores from selling their personal information. They also incorrectly believe that stores cannot charge them different prices based on what they know about them. Most other internet-using adults admit that they simply don't know whether or not laws protect them.

The survey further reveals that the majority of adults who use the internet do not know where to turn for help if their personal information is used illegally online or offline. The study's findings suggest a complex mix of ignorance and knowledge, fear and bravado, realism and idealism that leaves most internet-using adult American shoppers open to financial exploitation by retailers.

Americans' lack of knowledge about marketplace rules puts them at risk. We found that:

- 68% of American adults who have used the internet in the past month believe incorrectly that "a site such as Expedia or Orbitz that compares prices on different airlines must include the lowest airline prices."
- 49% could not detect illegal "phishing"—the activity where crooks posing as banks send emails to consumers that ask them to click on a link wanting them to verify their account.
- 66% could not correctly name even one of the three U.S. credit reporting agencies (Equifax, Experian, and TransUnion) that could keep them aware of their credit worthiness and whether someone is stealing their identity.

Consumers are also vulnerable to subtle forms of exploitation online and offline.

- 64% of American adults who have used the internet recently do not know it is legal for "an online store to charge different people different prices at the same time of day." 71% don't know it is legal for an *offline* store to do that.
- 72% do not know that charities are allowed to sell their names to other charities even without permission.
- 64% do not know that a supermarket is allowed to sell other companies information about what they buy.
- 75% do not know the correct response—false—to the statement, "When a website has a privacy policy, it means the site will not share my information with other websites and companies."

This lack of knowledge signals that the great majority of U.S. adults who use the internet is unprepared to deal with two hot trends that are rapidly becoming facts of life in stores,

yet have hardly received attention beyond the trade press. One trend, which marketers call behavioral targeting, involves buying or collecting information about a customer's activities in order to know how to best sell to him or her. The second development is price discrimination: when a seller charges different prices to different customers based on data the seller has about them.

We asked a nationally representative sample of 1,500 adults who used the internet during the past month 17 true-false questions about key aspects of these new developments and where they can turn for help if their personal information is used illegally. Among them were the statements noted on page 3 as examples of Americans' lack of knowledge. In fact, we found that the respondents know correct answers to an average of only 7 of the 17 of the true-false questions. We also found that they overwhelmingly object to most forms of behavioral targeting and all forms of price discrimination as ethically wrong.

- 76% agree that "it would bother me to learn that other people pay less than I do for the same products."
- 64% agree that "it would bother me to learn that other people get better discount coupons than I do for the same products."
- 66% disagree that "it's OK with me if the supermarket I shop at keeps detailed records of my buying behavior."
- 87% disagree that "it's OK if an online store I use charges people different prices for the same products during the same hour."
- 72% disagree that "if a store I shop at frequently charges me lower prices than it charges other people because it wants to keep me as a customer more than it wants to keep them, that's OK."

Most internet-using U.S. adults are aware that companies can follow their behavior online. Almost all (89%) of those who say their supermarkets offer frequent shopper cards applied for them—and in doing it gave the stores personally identifiable information about themselves. In this retail environment where companies collect personal information, Americans do directly admit feeling vulnerable. Only 17% agree with the statement that "what companies know about me won't hurt me" (81% disagree), 70% disagree that "privacy policies are easy to understand," and 79% agree that "I am nervous about websites having information about me." Sadly, though, only about one out of three (35%) says he or she "trust(s) the U.S. government to protect consumers from marketers who misuse their information."

In the face of all this nervousness and seeming confusion, it is startling that 65% of internet-using adult Americans nevertheless say they "know what I have to do to protect myself from being taken advantage of by sellers on the web." Judging by their scores on the true-false test, they have a misplaced sense of confidence. People who say they know how to protect themselves score just as poorly on the questions—and even the ones specifically regarding the online marketplace—as the people who don't think they know how to protect themselves. By contrast, those with a higher education tended to be more modest about knowing how to protect themselves but were more likely to score better on the test.

In fact, of all characteristics in people's backgrounds, having more years of education is the best predictor of understanding basic realities about power to control information on them and the prices they pay when shopping online and offline. Yet even having more general schooling doesn't necessarily mean really knowing this world well. People whose formal education ended with a high school diploma know correct answers to an average of 6.1 items out of a possible 17. People with a college degree do better—8.1—but that still means they get only 45% right. Even people with graduate school or more average 8.9 correct—just 51% correct.

As U.S. society moves further into the twenty-first century, prices that vary based on firms' information about us could become an increasing feature of the marketplace. Database-driven price distinctions could spread as growing numbers of retailers use information consumers never knew they revealed to draw detailed conclusions about their buying patterns that they would not have wanted. Consumers who are not aware of how behavioral targeting and price discrimination work, of what rights they hold when it comes to companies' using knowledge about them, and of how to respond to these circumstances may not know they are not getting the best deals. They may consistently be paying more than others for the same products.

At the end of the report we therefore suggest three courses of action. First, the Federal Trade Commission should require websites to drop the label *Privacy Policy* and replace it with *Using Your Information*. The new designation will likely go far toward reversing the broad public misconception that the mere presence of a privacy policy automatically means the firm will not share the person's information with other websites and companies. Second, U.S. school systems—from elementary through high school—must develop curricula that tightly integrate consumer education and media literacy. Paying new attention to these much-neglected subjects is critical if society is to succeed in preparing young people for the increasingly challenging twenty-first century marketplace. Third, the government should require retailers to disclose specifically what data they have collected about individual customers as well as when and how they use those data to influence interactions with them. The survey found that Americans are begging for openness in their relationships with marketers.

Our examination of internet-using American adults in the new online/offline marketplace was carried out by ICR/International Communication Research for the Annenberg Public Policy Center of the University of Pennsylvania. The study was conducted by telephone from February 8 to March 14, 2005, among a nationally representative sample of 1,500 respondents who said they had used the internet within the past thirty days.

Our aim was to address two critical public policy questions that have not previously been explored: How much do Americans know about who is allowed to control information about them when they shop online and offline? And what do they know and feel about those two rather secretive activities, behavioral targeting and price discrimination, that are increasingly affecting American shoppers on- and offline?

BACKGROUND

These questions are important because it is becoming clear that shopping in the twenty-first century will be quite different from the way it was in the twentieth. One does not have to turn to the movie *Minority Report* for an idea of futuristic gizmos consumers will confront in local malls. Activities are already underway across the retailing spectrum—in banks, high-end boutiques, supermarkets, and discounters—that are fundamentally altering the relationship Americans have with stores.

Two particular developments stand out: behavioral targeting and price discrimination. Behavioral targeting in a retail environment takes place when a firm keeps track of a customer's shopping history in order to know how to best sell to him or her.¹ Price discrimination comes in a variety of forms, economists note.² The ones that most attract retailers involves using information to change prices based on what the seller knows about individual consumers or consumer segments.³

Retailers consider behavioral targeting and price discrimination crucial tools to cope with the hypercompetitive online and offline circumstances in which they find themselves. Critics of the trend worry that it may well put many consumers at financial and even social disadvantage unless they understand what is happening. This study explores whether they do.

The term *behavioral targeting* is often associated with the virtual world but the activity it describes takes place offline as well.⁴ Online stores can closely follow movements of visitors—for example, to see what products they viewed and whether they started to buy something but didn't complete the purchase. Stores can save the records of these actions and, by placing text files called cookies in the visitors' computers, maintain a collection of what the people who use that computer have looked at on the site over time.

Of course, following activities on a computer does not reveal whether they reflect the clicks of more than one person—several members of a household, for example. Stores do keep records of the online purchases of individuals, and they try to encourage their customers to identify themselves when they visit their sites by “signing in” with a password. Getting the password typically means registering—providing name and email address in addition to other information such as gender, birthdate, and zip code.⁵

The consumer's reward for offering personally identifiable information and signing in is the opportunity to receive quick checkout, “special offers” and attention via email. The store gains a gold mine of information. Each time registered visitors enter the online stores using their passwords, stores can add information about their specific activities to a database. That allows the store's data analysts to categorize the consumer in terms of preferences and long-term value.

Based on sales and tracking information, the merchant can also decide whether it is useful to buy additional information about those customers from data brokers. Over the

past few decades, the sale and purchase of information on individuals has become big business. Recent news reports about the theft or accidental loss of personally identifiable information by data brokers Choicepoint⁶ and Lexis Nexis Group⁷ shined an unusual public beacon on an industry that is aided by the absence of U.S. laws to control much of the extraction, manipulation and sharing of data about people and what they do online or offline. Without customer permission, organizations not “affiliated” with each other are prohibited from sharing certain personal health information, certain types of personal financial information held by certain types of firms, certain information that video stores and cable systems collect about their customers’ viewing, and personally identifiable information from children younger than thirteen years.⁸ Generally, though, companies have virtually free reign to use data in the U.S. for business purposes without their customers’ knowledge or consent. Merchants can therefore easily buy information on valued customers’ backgrounds and activities with an eye toward better understanding their interests and purchasing power.

A retailer will often hire behavioral-targeting firms to bring together for analysis all the data the retailer is collecting about customers. The firms create profiles of the individuals, often placing them into labeled segments of consumers with similar buying characteristics. Then, based on rules for data handling that include scoring individuals on various characteristics, the firms customize interactions with customers and the customer segment in ways intended to be the most profitable possible.

The behavioral targeting firm Epiphany, for example, claims that it “offers a complete solution for optimizing interactions with customers over online channels such as the Web, e-mail, and SMS [i.e., short text messages on cell phones].” In a “case study” on its website, Epiphany claims that by using its expertise and software, American Airlines has gained “a comprehensive view of its customers across all [electronic communication] touchpoints . . . to enhance customer relationships.”⁹ For the American Airlines website, AA.com, Epiphany implements personalization and content management software to analyze customer profiles as customers move through the site and then proceeds to “match them to relevant content and offers on the site.”¹⁰ Epiphany does that with an electronic newsletter sent to millions of customers. Called *AAirmail*, the publication provides customized content and offers tailored to the individual profiles Epiphany has created. As an example, newsletter articles vary to help individual customers reach their next top-tier status—Gold, Platinum or Executive Platinum.¹¹

As an American Airlines marketing executive describes them, these activities are part of a larger “unified view of customer behavior” that allows the company to “integrate data about past transactions and interactions, online or otherwise.”¹² Increasing numbers of merchants are going beyond the digital realm and using Epiphany or larger database firms such as Oracle-PeopleSoft, or Acxiom to create central customer databanks for the instantaneous use of all customer information. As one writer put it, the repositories “collect data from all points” and then “tailor permission-based offerings to accommodate customers’ finely segmented demands, wherever they originate.”¹³

In tune with this idea, retailers increasingly act as if their selling arena has merged into one integrated online/offline marketplace. Consumers, they believe, are “multi-channel”—they shop both online and offline.¹⁴ Acxiom tells its clients that “The ability to best serve your customers when it matters most—during the interaction—is critical to achieving customer growth and retention goals. Acxiom’s customer recognition solutions enable companies to distinguish customers accurately and consistently, providing complete and instant access to relevant customer data across all channels of communication.”¹⁵

Growing numbers of merchants are therefore merging the data they have about their customers from the web, the phone, and the store floor in a bid to give their desired customers a seamless experience. In the process, behavioral targeting is taking place offline, online and across both areas. The offline activity has actually been going on for quite a while. As early as the 1980s, financial and leisure firms as well as elite retailers were following the logic of developing relationships with customers based on digital repositories and then treating them differently based on what they learned. They created the databases by soliciting information from their customers, buying information about their lifestyles from data brokers, and tracking their interactions with them.

Mid-priced department stores and supermarket chains took longer to adopt this strategy. By 2000, though, that was changing rather quickly. A major reason had to do with the enormous price competition that they confronted in discount retailer Wal-Mart. Wal-Mart uses an aggressive “everyday low prices” strategy supported by a legendary efficiency, strong pressure on suppliers, and a huge investment in databases to track the movement and sale of products. The approach often determines the price of products in an area and consequently frightens retailers that sell the same or similar items. The phenomenon is so pervasive and powerful that it has become a noun—Wal-Martization—in the Forrester Research consultancy’s lexicon.¹⁶

In the absence of an ability to compete on price with Wal-Mart and similar discounters, many retailers have been searching for the best strategies with which to survive. Some consultants suggest that the answer lies in adapting to the varied needs of the area better than Wal-Mart can in terms of the right quality, convenient locations, and variety of offerings. Another stream of analysis sees Wal-Mart’s long-term Achilles heel in terms of its difficulty in getting close to the individual customer or small-customer niches. This view emphasizes that with the exception of its Sam’s Club wholesale setup, the company does not keep track of individual customer purchases or reach out to them in unique ways.

Increasingly, retailers see a key competitive advantage in the Wal-Mart age as knowing and rewarding profitable customers better than Wal-Mart or any other competitors. The goal is to sell products that those consumers will perceive as valuable not primarily because of the price but because the product quality and service consistently matches what they need. Analytics firms with the expertise of finding patterns in purchase data develop profiles of “best” or at least “good” customers so as to focus on wooing them.

The idea is that as important as prospecting for new customers is, retailers should pay more attention to the good customers they already have. One reason is the belief that a high percentage (sometimes 80%) of a company's profit comes from a small percentage (often around 20%) of repeat purchasers and that it costs several times more to get a new customer as it does to retain a loyal one. Another belief is that the best new customers will be those who are similar to the best old ones. The more the retailer uses databases to find out about its desirable clientele, then, the better it can keep them, find others like them, and not pursue "low-value" consumers who tend to shop only for bargains or who return too many goods.

So, for example:

- The Claritas company's P\$ycle database helps banks figure out whom to keep and pursue as customers by statistically linking their customer to what Claritas knows about the background and behavior of types—segments—of people it concludes are like them. When fed a bank's customer data, P\$ycle software segments them "by evaluating the economic and demographic factors that have the greatest effect on their financial behavior." The 8 major groups into which P\$ycle divides the population reflects a slide from high prosperity to virtual penury: Wealth Market, Upscale Retired, Upper Affluent, Lower Affluent, Mass Market, Midscale Retired, Lower Market, and Downscale Retired. The trick with all the groups and segments, according to Claritas, is to link the data to the bank's "house file" to create "actionable" information—for example, whether or not to invite certain people as customers and, if so, what packet of materials to send.¹⁷
- According to *Direct* magazine, the Bloomingdales department store, which keeps transaction records of all its customers, uses database software called Klondike to focus on the store's 15,000 most valuable patrons. It contains their transactions, the history of promotional materials sent to them, and basic household information. Klondike presents the data about these people to Bloomingdale's telephone call center and sales floor personnel. By swiping the best customer's credit card at a point of service terminal—a cash register—salespeople can get an overview of the shopping interests of individual customers. The idea is to "enable salespeople to custom-build merchandise suggestions."¹⁸
- In 2005 the CEO of data-mining firm IRI noted that for years, food and drug retailers have been compiling data from frequent-shopper cards but doing little with it. That, he said, was starting to change quickly. IRI signed a deal with a major grocery chain to mine shopper data to help it target marketing toward the most profitable customers. He expected more supermarkets to do the same.¹⁹ A columnist in *Progressive Grocer* magazine noted that a small but growing number of chains are pursuing strategies that both invite "very good customers" and push away "cherry pickers." He opined that behavioral targeting—"creating a profile of their customers and then performing triage on the market to save their most valuable purchasers"—is a wise competitive stance in a Wal-Mart world, where "competing on price is out of the question."²⁰

Price discrimination is a logical corollary to behavioral targeting. Economists commonly identify three types of bias. First-degree price discrimination occurs when a different charge is tailored to a specific buyer based on what the seller knows about the customer. With the second-degree type, sellers openly offer a variety of fee options—for example, grocery discounts for buying large quantities or lowered bank fees for keeping large account balances—to induce consumers to choose the one that matches their interests or abilities to pay. In third-degree price discrimination, the seller decides what segments of the market have different levels of price sensitivity and charges the groups accordingly. Examples of third degree price discrimination are senior-citizen and student discounts.

But while retailers grant senior citizen and student discounts openly, in a growing number of circumstances they are categorizing consumers into statistical segments without their knowledge. People in certain niches may then get different discount offers for the same products and services—as well as for different products and services—compared to those in other niches. For example, banks that use the Claritas P\$ycle system vary the deals they present customers based on the lifestyle segments into which they slot them.

Many financial institutions also carry out first-degree price discrimination without notifying their customers. They do it by scoring them based on their financial abilities and payment activities in the marketplace. Department stores and even supermarkets have been moving swiftly into this area, as well, though they don't discuss it publicly. With Bloomingdale's Klondike, for example, "aggregate spending information atop each customer's file allows the floor rep to make snap decisions about offering special services" that increase the value of that person's purchases compared to other customers.²¹ On the flip side, stores have been trying to find ways to discourage shopping from what some retailers call "bottom feeders"—consumers who visit them mostly for bargains and return products too often.²²

As for supermarkets, the frequent-shopper or "loyalty" card (held by far more than 50% of U.S. households) is currently their central way for keeping track of individual household purchases and charging them differently. One common supermarket price-discrimination tactic involves the Catalina database system that gives different value coupons based on analyses of consumer's purchases using the store's loyalty card for 104 weeks.²³ Tests of in-store computer tracking technologies by Albertsons and Stop and Shop aim to customize the consumer's discounts based on shopping history from the moment the consumer enters the store. In both cases being a loyal customer doesn't automatically mean getting the lowest prices. Computer analyses of shopping histories might determine that a person's allegiance to some products means that he or she would buy them even without the discounts, or with smaller discounts than others might get for the same items at the same time.

Merchants consider the online environment a particularly ripe area for such "dynamic pricing"—that is, for first-degree price discrimination driven by behavioral targeting. Writing in *Harvard Business Review*, associates from McKinsey & Company chided online companies that they are missing out on a "big opportunity" if they are not tracking customers' behavior and adjusting prices accordingly.²⁴ Consultants urge retailers to

tread carefully, though, so as not to alienate customers.²⁵ The most public revelation of price discrimination online centered on customer anger at Amazon.com in September 2000 when it offered the same DVDs to different customers at discounts of 30%, 35%, or 40% off the manufacturer's suggested retail price. Amazon insisted that its discounts were part of a random "price test" and not based on customer profiling. After weeks of customer criticism, the firm offered to refund the difference to buyers who had paid the higher prices.²⁶

Though website executives are wary of discussing the subject, it seems clear the practice continues. Consumer Union's Webwatch project found many bewildering and seemingly idiosyncratic price differences, sometimes quite large, in its investigation of airline offers on travel sites.²⁷ When asked whether travel websites vary prices based on what they know about customers' previous activities, one industry executive told Webwatch advisor and University of Utah professor Rob Mayer, "I won't say it doesn't happen."²⁸

All this, it should be noted, is usually quite within the law. In the *Virginia Journal of Law and Technology*, Robert Weiss and Ajay Mehrotra conclude that "as long as the price differences are based on reasonable business practices such as rewarding loyal customers and do not discriminate against race, gender, or other impermissible categories, dynamic pricing appears to be legal."²⁹ Some economists argue, in fact, that certain types of price discrimination may in certain circumstances promote an efficient use of society's resources. The classic case is that of the dedicated, but by no means rich, country doctor who charges rich people more than poor people so that he can continue to serve both and make a reasonable living. More relevant to the current discussion, supporters of price discrimination that is tied to behavioral targeting and other types of personal profiling argue that is part of a larger process through which companies get to know and serve individual customers in ways that benefit both sides.

Consumer advocates dispute this claim. They argue that while database-guided price discrimination might well help some businesses, it is considerably harmful to individuals and society. Of particular concern to critics are issues of privacy, reduced personal autonomy, misuse of data, and financial harm. Price discrimination based on profiling, they say, invariably means using information about individuals in ways that do not involve their permission. Further, retailers do not tell customers what information they have about them, so that price-discrimination decisions based on errors are quite possible. But even if the private information is correct, there still is the ethical issue of not allowing customers a say in the profiles stores create about them or the niches in which stores place them.

Writing about behavioral price discrimination in the financial industry, Janet Gertz states in the *San Diego Law Review* that "many characterize the commercial exploitation of consumer transaction data as a classic example of a market failure." She explains that "statistics indicate that the power shift facilitated by predictive profiling has proven highly profitable for the financial services industry. However, there is little evidence that indicates that any of these profits or cost savings are being passed on to consumers."³⁰

Chris Hoofnagle of the Electronic Privacy Information Center suggests that the same argument can be made regarding retailers in general. He notes that the *Wall Street Journal* found that frequent shopper cards do not generally save consumers money. He implies that giving stores the opportunity to vary discounts by what they know customers have paid in the past might increase this imbalance even more, especially for certain consumers. Hoofnagle also suggests that stores are acting unethically when they try to push customers away because data show they are frugal or sharp shoppers. At the very least, they are disallowing what many consumers have been taught throughout their lives by schools, parents, and ads that exhort them to follow storewide sales. From this perspective, database-driven price discrimination is against the American Way—at least as it was practiced in the twentieth century.³¹

The arrival of behavioral targeting and price discrimination in a severely competitive offline/online marketplace indicates that the U.S. is entering a new Way. Retailers in the twenty-first century are basing their relationships with consumers on fundamentally new assumptions and technologies. Underlying these changes are crucial issues of social fairness and marketplace transparency. A few experimental studies have shown that when researchers confront consumers with situations featuring price discrimination, the consumers reduce their trust in the retailers doing the discriminating.³² Until now, however, no one has asked what consumers would say if retailers justified price discrimination to consumers with arguments that sometimes they may benefit from it.

In fact, until now no one has explored what the U.S. public knows and thinks about these activities that promise to be key parts of twenty-first century marketing. How much do Americans know about who is allowed to control behavioral and other personal information about them in the online/offline marketplace? Are consumers aware of the existence of price discrimination based on behavioral targeting and other profiling? If they are aware of it, do they accept it as part of economic life, do they resent it, or do they simply believe that the government places limits on it in the interest of fairness?

THE STUDY AND THE POPULATION

Because our questions relate to both the online and offline marketplace, we decided to focus on U.S. adults who use the internet. We cast our net broadly. We included people 18 years or older in our study if they said yes to the question, “Have you used the internet in the past month at home, work, or anywhere else?”

Our questions aimed to focus on two areas. One was people’s knowledge of the law when it comes to a company’s right to collect information about them online or offline and to charge them and others different prices for the same items at the same time. The second area centered on people’s attitudes regarding these activities. The interview schedule itself had seven parts beyond the introductory screening material. Part 1 asked about the person’s internet use. Part 2 solicited people’s views about companies’ having access to their personal information, profiling them behaviorally, and charging them different prices—sometimes to their benefit—based on what they learn. In Part 3 the interviewee was given a series of statements about the rules of price discrimination and profiling—especially behavioral targeting—in the marketplace and asked whether each was true or false. Part 4 involved three short scenarios describing different types of behavioral targeting and soliciting the person’s opinions about their ethical acceptability. Part 5 asked people to agree or disagree about statements regarding privacy and personal information. Part 6 asked about the person’s everyday privacy-protecting activities and concerns online and offline. And Part 7 requested background data such as age, education, and ethnicity.

ICR/International Communication Research of Media, Pennsylvania, carried out the field work for our survey from February 8 to March 14, 2005. ICR used a nationally representative RDD (random digit dial) sample to screen households for adults age 18 or older who said that they used the internet in the past month. Using the American Association of Public Opinion Research (AAPOR) RR3 method, a standard for this type of survey, the overall response rate for this study was a very good 58.4%.

The telephone interviews, which averaged 20 minutes, were completed with a nationally representative sample of 1,500 adults. The process involved Computer Assisted Telephone Interviewing System (CATI), which ensures that questions follow logical skip patterns and that attitude statements are automatically rotated, eliminating question-position bias. The resulting data were weighted to population estimates of people who say they used the internet during the past month that were calculated from ICR’s large daily rolling cross-sectional study, Centris.³³ The margin of error for reported percentages based on the entire sample of 1,500 is plus or minus 2.51 percentage points at the 95% confidence level. The margin of error is higher for smaller subgroups within the sample.

Tables 1 and 2 provide an introductory snapshot of the population we interviewed. As Table 1 indicates, women slightly outnumber men; 73% designate themselves as non-Hispanic white, 8% call themselves non-Hispanic blacks; Hispanics (white and black) comprise about 10% of the sample; Asian Americans make up 3%; and Native

Americans comprise about 1%. About 60% are under age 45, 57% are married, and 44% have children under age 18. Most have at least some higher education, and while a substantial percentage say their household brings in more than \$75,000 annually, a firm claim about this population's income distribution is difficult because 17% of the population refused to reveal it.

Table 2 indicates that 91% of the respondents have at least one way of connecting to the internet from home. Fully 42% of the respondents say they have been online at home for seven years or more, an indication of the maturing of this medium. Several say they can use more than one method from home, typically dialup and DSL. Three quarters of the respondents go online at least once a day, and about half say they connect several times during the course of the day. When they "navigate the internet," 46% call their level of expertise "advanced" and "expert" while 54% consider themselves "beginner" and "intermediate."

Because this survey centers on the marketplace, we asked the people we phoned basic questions about their offline and online shopping. As Table 2 shows, 81% say they bought something in the supermarket during the past month, while 54% say they bought something online in the past month. Not surprisingly, the supermarket is also more popular than the internet in terms of the number of times people go there to buy. Further analysis shows no significant differences between men and women on this score. Similar percentages of both genders are shoppers both offline and online, and they shop with similar frequency.

**Table 1: Characteristics of U.S. Adults
Who Used the Internet “In the Past Month”(N=1,500)**

	%*
Sex	
Male	48
Female	52
Age	
18-34	37
35-44	22
45-54	18
55-64	10
65+	12
No answer	2
Race and ethnicity	
White non-Hispanic	73
White Hispanic	9
Black non-Hispanic	8
Black Hispanic	1
Asian-American	3
Native American	1
Other	1
No answer	4
Education	
Less than high school graduate	8
High School/tech school graduate	31
Some College	27
College graduate or more	34
No answer	1
Family Income	
Less than \$40K	26
\$40K but less than \$75K	29
\$75K but less than \$100K	13
\$100K+	14
Don't Know/No answer	17
Parental Status	
Parent of child below age 18	44
Not parent of child below age 18	54
No answer	2

*When the numbers don't add up to 100% it is because of a rounding error.

Table 2: Internet activity, internet expertise, and shopping frequency (N=1,500)

	%*
Online connection(s) at home	
Dial-up connection only	31
Cable modem with/without dialup	18
DSL with/without dialup	25
Cable or DSL with another method	13
Don't Know	4
No internet connection at home	9
Frequency online from anywhere	
Several times a day	56
About once a day	20
A few times a week	16
About once a week	5
About once a month	2
Just a few times a year	1
Years online at home	
One or less	6
Two	4
Three or four	11
Five or six	25
Seven or more	42
Don't know	3
No internet connection at home	9
Self-ranked expertise navigating the internet	
A beginner	14
Intermediate	40
Advanced	34
Expert	12
How many times bought item online in past month?	
Once or twice	30
From 3 to 6 times	18
From 7 to 10 times	3
More than 10 times	3
Never	46
How many times bought in supermarket in past month?	
Once or twice	7
From 3 to 6	26
From 7 to 10	15
More than 10 times	33
Never	18

*When the numbers don't add up to 100% it is because of a rounding error.

LACKING THE KNOWLEDGE

We did find statistically significant differences between the way internet users with certain background characteristics and attitudes performed on the true-false test. Yet our results also showed that even better scorers typically do not have strong basic knowledge of the subject.

The statements for the test evolved from a wide-ranging review of academic, trade, and public policy literature as well as discussions with individuals in the Federal Trade Commission and public advocacy organizations. The goal was to generate a series of propositions about what consumers ought to know regarding three topics: who is allowed to *control* the profiling information about them that can lead to price discrimination, whether the law *protects* them from secret forms of price discrimination offline and online, and where they can turn for *help* if they worry that their information is being abused. We created dozens of statements, shared them with colleagues and policy experts, and tested them on college students. We chose the 17 in the survey because they speak to basic, everyday issues involving banks, supermarkets, travel sites, video stores and credit; cover the three topics of control, protection, and help; and offer a balanced attention to both the offline and online marketplace. When taken together to form a knowledge scale, the 17 true-false items demonstrate good internal reliability, as indicated by a Cronbach's Alpha of 0.74. This means that all of the individual items are statistically associated with one another and thus all appear to be measuring the same underlying concept. By convention, scales that obtain Alpha scores of 0.70 or higher are considered reliable.

In introducing this section of the interview, the ICR representative stated that "For the next series of statements, please tell me if each one is true or false. If you're not sure, just say, "not sure." Table 3 presents the statements, the responses, and the percent that got them wrong. "Wrong" here means the number who said "don't know" added to those who gave the incorrect true or false answer. *Don't know* indicates a willingness to frankly admit ignorance. The proportion of people who said they don't know tends to hover between one between around one-fifth and one-third of the responses. Fairly large percentages of internet-using adults are willing to admit that they don't know these marketplace facts of life.

Going down the table from most correct to least correct responses, three themes seem clear:

- **Most internet-using U.S. adults are aware that companies can follow their behavior online.** Fully 80% know marketers "have the ability" to track them across the web, and 62% know that a company "can tell" if they have opened its email without getting their response.
- **Large majorities of internet-using U.S. do not understand key laws and practices relating to profiling, behavioral targeting and price discrimination.** About half of the population does know some basics. About 50% recognize that

most online merchants are allowed to share information with “affiliates” without the consumers’ permission; that magazines can sell information about them without permission; and that merchants do not (and need not) allow consumers the opportunity to see or erase the information they gather about them. Moreover, about half seem to have caught the description of “phishing” and so answer it is false that banks “often send their customers emails that ask them to click on a link wanting them to verify their account.”

Yet saying one out of two internet-using adults is aware of these realities means that the other 50% do not understand them. In this connection, the inability of half the respondents to discern phishing is particularly alarming because of the activity’s growth. The Gartner consulting firm concluded from April 2004 research that direct losses from identity theft fraud against phishing attack victims — including new-account, checking account and credit card account fraud — cost U.S. banks and credit card issuers about \$1.2 billion in 2003.³⁴

It is also troubling that around 50% of internet-using U.S. adults are unaware that information about them can move between magazines and amid affiliated websites without their approval. A similar percentage thinks they have more control over the information that online firms hold about them than they actually do. A far higher percentage—75%—doesn’t realize that the mere presence of a privacy policy is no indication that a site will refrain from sharing visitors’ information. This pattern of unawareness online and offline may well lead them to be less careful about providing certain sorts of information to merchants than they would be if they knew what actually takes place.

Table 2 also shows a lack of knowledge about the legal right of supermarkets, video stores and charities to sell personal information; of banks to share customer information with affiliates; and of retailers’ to discriminate on price. When it comes to these topics, from 63% to 72% of respondents are wrong. Considering the popularity of online travel sites, one must suspect that many people don’t get the best deals when 68% of internet-using adults believe incorrectly that “a site such as Expedia or Orbitz that compares prices on different airlines must include the lowest airline prices.”

It might seem odd that higher proportions of respondents are incorrect about the legality of information-sharing by banks, charities, supermarkets and video stores than by magazines and non-specific “websites.” Although we have no data to explain the differences, it seems reasonable that those interviewed used their belief about the sensitivity of the material that the merchants gather as a guide for answering. People may believe that banks and supermarkets hold data about their activities that are more personally revealing than what generic websites and magazines store about them. People may also believe that disclosing the charities that receive their money means divulging particularly sensitive information about lifestyles. Respondents therefore may have concluded that it is illegal for banks, charities and supermarkets but not generic “websites” and magazines to exchange information.

Note that the statement on video rentals has the highest “don’t know” percentage in Table 3. Perhaps that is because respondents are unsure whether the personal data reflected in video rental titles pass a personal-sensitivity threshold that would make sharing them illegal. As it happens, video tapes represent an unusual case—where there actually is a law to stop stores from revealing personal data. Only 29% of respondents answered that statement correctly, though.

- **Large majorities of internet-using U.S. adults do not know basic places to turn for help if their marketplace information is used illegally.** The lack of understanding regarding marketplace laws and practices carries over to their understanding of where they can go for recourse if things do go wrong. Fully 76% agree incorrectly that “The Federal Trade Commission will correct errors in credit reports if it is shown proof of the errors.” The FTC suggests that consumers contact one of the three national credit reporting agencies, Equifax, Experian, or TransUnion. Yet when asked “Can you give me the name of national Credit Reporting Agencies that can give you a copy of your credit report?” 66% of the respondents could not name any of them.

Table 3: Responses to statements about rules of profiling, behavioral targeting, price discrimination and recourse in the marketplace (N=1,500)*

	%T	%F	DK
1. Companies today have the ability to follow my activity across many sites on the web. <i>20% wrong</i>	80	8	12
2. A company can tell that I have opened its email even if I don't respond <i>28% wrong</i>	62	14	24
3. Most online merchants give me the opportunity to see the information they gather about me. <i>47% wrong</i>	23	53	25
4. Banks often send their customers emails that ask them to click on a link wanting them to verify their account <i>49% wrong</i>	26	51	23
5. Most online merchants allow me the opportunity to erase information they have gathered about me <i>50% wrong</i>	19	50	30
6. A website is allowed to share information about me with affiliates without telling me the names of the affiliates. <i>49% wrong</i>	51	29	20
7. When I subscribe to a magazine, by law that magazine cannot sell my name to another company unless I give it permission. <i>52% wrong</i>	36	48	16
8. It is legal for an online store to charge different people different prices at the same time of day. <i>62% wrong</i>	38	29	33
9. My supermarket is allowed to sell other companies information about what I buy. <i>64% wrong</i>	36	36	28
10. Correctly knows the name of a credit reporting agency <i>66% wrong</i>	34	66	--
11. By law, a site such as Expedia or Orbitz that compares prices on different airlines must include the lowest airline prices <i>68% wrong</i>	37	32	31
12. A video store is not allowed to sell information about the titles I have rented. <i>71% wrong</i>	35	29	36
13. It is legal for an offline store to charge different people different prices at the same time of day. <i>71% wrong</i>	29	42	29
14. When I give money to charity, by law that charity cannot sell my name to another charity unless I give it permission <i>72% wrong</i>	47	28	25
15. When I give personal information to a bank, privacy laws say the bank has no right to share that information, even with companies the bank owns. <i>73% wrong</i>	55	27	18
16. When a website has a privacy policy, it means the site will not share my information with other websites or companies. <i>75% wrong</i>	59	25	16
17. The Federal Trade Commission will correct errors in credit reports if it is shown proof of the errors. <i>76% wrong</i>	52	24	24
Bold numbers indicate the correct answer.			
The statements were rotated to eliminate position bias.			
For more explanation, see text.			

*When the numbers don't add up to 100% it is because of a rounding error.

T=true; F=false; DK=don't know

Notes explaining the basis for the correct answers can be found at the Annenberg Public Policy website:

<http://www.annenbergpublicpolicycenter.org/>

CONCERNS AND OBJECTIONS

Part 4 of the interview involves three short scenarios describing different types of behavioral targeting and soliciting the person's opinions about their ethical acceptability.

Scenario 1 centers on a “website [that] changes the ads that you see based on what you are reading on the site. The site does not ask you for any personal information. It just looks at what you are reading now and places ads related to that topic next to the article. One result is that people get different ads based on their interest.”

In Scenario 2, an “online store you like decides to buy personal information about you from a database company that lets it know your job, how many children you have, whether or not you have a car, and what vacations you take.” It then changes the products seen based on that lifestyle information.

Scenario 3 shifts to “a supermarket [you shop at] near your home.” We asked the person interviewed to picture that “The supermarket places a device on the shopping cart you use. The supermarket asks you to swipe your frequent shopper card into the device on the shopping cart.” (We asked those interviewed to imagine using a frequent shopper card if they don’t have one.) “As you walk down the aisle,” we continued, “the device checks the records of your past shopping in the store’s computer and gives you personalized offers, including offers others do not get. It also gives other people using the cart personalized offers that you do not get.”

After presenting each of the first two scenarios, we asked the respondents whether they thought the activities we wanted them to imagine “actually do” take place. The affirmatives were overwhelming. 85% believe that some websites analyze what people are reading on their sites; 84% accept that sites change the ads that people see based on what they are reading on their sites; 84% believe that sites buy personal information about “you” from database companies; and 75% agree that sites change the products “people” see based on the personal information that the sites have bought from database companies. These responses parallel our earlier-noted finding that 80% of the respondents know “Companies today have the ability to follow my activity across many sites on the web.” In addition to believing that this sort of behavioral profiling takes place online, a substantial portion of the population is explicitly aware that at least some type of personal identification takes place in the supermarket: Almost all (89%) of the 1,079 respondents of our sample who say their supermarkets offer frequent shopper cards received one. In the course of filling out material for it, they knowingly gave the stores personally identifiable information about themselves.

This wide awareness of behavioral tracking online and personal identification in offline supermarkets by no means translated into acceptance of the price discrimination that might flow from firms having these data. As Table 4 shows, most internet-using adults dislike a range of activities that retailers carry out daily based on customer information they collect.

Table 4: Attitudes about retailer activities online and offline (N=1,500)

	% A	% D	% N	% DK
It's OK if the supermarket I use charges different people different prices for the same products during the same hour.	8	91	1	--
It's OK if a store charges me a price based on what it knows about me.	8	91	--	1
If I trust an online store, I don't mind if it buys information about me from database companies without asking me.	9	90	--	1
It's OK if an online store I use charges different people different prices for the same products during the same hour	11	87	1	1
Websites should be required to let customers know if they charge different people different prices for the same products during the same hour.	84	14	1	1
It would bother me to learn that other people pay less than I do for the same products.	76	22	1	1
If a store I shop at frequently charges me lower prices than it charges other people because it wants to keep me as a customer more than it wants to keep them, that's OK.	26	72	2	--
The information I give online stores about myself will often determine the prices they will charge me.	21	67	2	10
It's OK with me if the supermarket I shop at keeps detailed records of my buying behavior	32	66	2	--
It would bother me to learn that other people get better discount coupons than I do for the same products.	64	33	2	--
It would bother me if websites I shop at keep detailed records of my buying behavior.	57	41	2	1
It's OK if a store I shop at frequently uses information it has about me to create a picture of me that improves the services they provide for me.	50	47	2	1
If I trust an online store, I don't mind giving it information about what I have bought in the last month.	49	49	1	1

*When the numbers don't add up to 100% it is because of a rounding error.

A=agree or agree strongly; D=disagree or disagree strongly; N=neither agree nor disagree;

DK=don't know

The smallest (though still-high) numbers of people object to situations that involve volunteering information to retail websites and accepting online behavioral targeting when the retailer is trustworthy. 49% of internet using adults disagree (and 49% agree) that “If I trust an online store, I don’t mind giving it information about what I have bought in the last month.” 47% disagree (and 50% agree) that “It’s OK if a store I shop at frequently uses information it has about me to create a picture of me that improves the services they provide for me.”

Take trust and improved service out, and more object. 57% agree that “It would bother me if websites I shop at keep detailed records of my buying behavior. Similarly, 66% disagree with the statement that “It’s OK with me if the supermarket I shop at keeps detailed records of my buying behavior.” Higher still is the negative response to a statement that people seem to have understood as a violation of trust: 90% of the respondents disagree that “If I trust an online store, I don’t mind if it buys information about me from database companies without asking me.”

The most consistent objections are to various presentations of price discrimination online and offline. Evidence suggests that people don’t expect that it is happening to them on a continual basis. Even though people know that they are tracked on the internet, only 21% agree that “The information I give online stores about myself will often determine the prices they will charge me.” Table 4 suggests that large percentages would object to it happening, though. When presented with various concatenations of price discrimination, between 64% and 91% of respondents registered aversion to the activity. Interestingly, a smaller percentage (64%) disagrees with discount coupons as mechanisms for price discrimination compared to simply asking for less money (76%). The largest percentages are riled about the idea of different people paying different prices for the same products during the same hour. 87% disagree with the implementation of such a practice by an “online store” and 91% disagree with its taking place in the supermarket.

The responses the internet-using adults gave to questions about the three scenarios indicated that their objections to rather general statements about price discrimination carry over to more concrete situations. All five circumstances are plausible. Websites often present different ads and products to their online customers as a result of database or tracking information. Similarly, supermarkets regularly present customers with discounts based on what they know about them through their frequent shopper cards, including whether they have children at home. Differential pricing in favor of people over 45 years old is probably not common, although price discrimination for “senior citizens” and AARP members (who are 50+) has become a well-publicized part of the retail landscape and receives little public condemnation. An important difference in this case compared to standard senior and AARP discounts is that in the scenario the favorable treatment is not announced publicly. Rather, the consumer is treated to the age discount based on the supermarket’s behavioral and other database information. We used the “people over 45” designation to see if people would accept the idea of price discrimination in an unusual age bracket and to note if people outside that age bracket would object more than those inside it.

We asked the people we interviewed what they thought of the three supermarket situations on a continuum from very good to very bad, with “neither a good nor bad idea” in the middle. As Table 5 indicates, 68% believe it is a “bad” or “very bad” idea if the store charges them different “higher or lower” prices than other people based on database information about their previous purchases. That response is not at the level of the 91% who in the non-scenario part of the interview thought it is wrong if “if the supermarket I use charges different people different prices for the same products during the same hour.” But it does fall in line with the reaction to statements such as “It’s OK with me if the supermarket I shop at keeps detailed records of my buying behavior” (66% disagree) and “It would bother me to learn that other people pay less than I do for the same products” (64%).³⁵

When it comes to the specific examples of supermarket discrimination around children and age, the proportions of people objecting—68% for children and 79% for age—are as large as or even larger than the proportion of internet-using adults who object to the pricing statement that does not mention a demographic category. Moreover, people voice little support for self-serving price-discrimination. When confronted with privileged pricing for children under age 18, people with children under age 18 are as likely to object to the activity as parents with kids age 18 and older. We do find a statistically significant relationship between being over age 45 and accepting the age-based price discrimination in the scenario as a “good” or “very good” idea. That relationship is quite weak, however. Fully 79% of internet using adults of all ages do not like behavior-driven price discrimination around age.

The first two scenarios center on popular forms of behavioral tracking that don’t involve price discrimination. Rather, they entail following people’s web movements or using purchased data about them for the purpose of deciding what content to serve them. The first scenario involves sending custom-chosen ads based on noticing the person’s “reading on the site.” The second involves showing the respondent different products on the site based on “personal information it bought about you from a database company.”

Table 5 reveals an interesting switch in responses between these two types of profile-driven customization. 45% of the respondents say that changing the ads based on what the site “sees you reading on the site” is a good or very good idea; 22% think it is a bad or very bad idea, while 33% say it is neither good nor bad. By contrast, 46% of the respondents believe that from a consumer’s standpoint it is a bad or very bad idea to change the products they see based on purchased personal information. 23% say it is a good or very good idea, and 29% say it is neither good nor bad.

Because different aspects of the two scenarios might explain the flip, we asked the respondents to tell us in an open-ended way why they answered “a good idea,” “a bad idea,” or “neither good nor bad” to each case. It turns out that with respect to each scenario the great majority of people who discuss it favorably when noting it is “a good idea” or “neither a good nor bad idea” say the behavioral customization would allow them to learn about products specifically for them. As might be expected, the proportion of those interviewed who note this benefit declines across the two scenarios—from 42%

who mention it in the case of custom-presented ads based on a person's reading to 25% who mention the benefit when presented with the idea of custom-presented products based on purchased personal data. Instead of answers stressing that advantage, reasons for the second case being "a bad idea" increased.

Table 5: Attitudes toward scenario activities (N=1,500)

	%G	%B	%N
Case 1: ... From a consumer's viewpoint, please tell me what you think of a company changing the ads on its website for you based on what it sees you reading on the site.	45	22	33
Case 2: ...From a consumer's viewpoint, please tell me what you would think if a store changes the products you see [on its website] based on the personal information it bought about you from a database company.	23	46	29
[In the supermarket] During the same time you are shopping, the store charges you different higher or lower prices than other people for the same products based on the store's knowledge of what you and the others had bought in the past.	16	68	15
[In the supermarket] The price for a product specifically targeting shoppers with children at home is lower for them than for other shoppers who don't have children at home.	18	68	13
[In the supermarket] The price on the same product is different between you and other shoppers based on what the supermarket knows about your age, with people over 45 paying less than people 45 or younger paying less than people 45 or younger.	9	79	11

*When the numbers don't add up to 100% it is because of a rounding error.

G=good or very good idea; B=bad or very bad idea; N= neither good nor bad

Two major criticisms came up in responses to both the first and second scenarios. One was that tracking or profiling people is an invasion of privacy. The other was that not showing people ads or products that others could see is an unfair limitation of people's views of the world. While 29% of the 1,500 internet-using adults volunteered privacy concerns and/or 25% noted world-view concerns in the data-buying case, substantially smaller numbers (11% and 14%, respectively) responded this way in the situation where ads are changed based on what people are reading at that time. Clearly the data-buying scenario bothers people who aren't concerned that serving different ads based on what people are reading would inhibit their privacy or view of what was available for sale. For them, the second scenario is a situation where the desire for privacy and the autonomy to view all options exceed the benefits of personalization.

Underlying the concerns and objections our respondents raised is a general feeling of vulnerability in the retail environment. Table 6 shows that only 17% agree with the statement that "what companies know about me won't hurt me" (81% disagree), 70% disagree that "privacy policies are easy to understand," and 79% agree that "I am nervous about websites having information about me." People seem to expect enforced

transparency in retail activities. 84% agree that “Websites should be required to let customers know if they charge different people different prices for the same products during the same hour.” Sadly, though, only about one out of three (35%) says he or she “trust(s) the U.S. government to protect consumers from marketers who misuse their information.”

Table 6: Attitudes towards privacy and personal information (N=1,500)

	% A	% D	% N	% DK
Websites should be required to let customers know if they charge different people different prices for the same products during the same hour.	84	14	1	--
What companies' know about me won't hurt me.	17	81	1	1
I am nervous about websites having information about me	79	18	2	--
I like to give information to websites because I get offers for products and services I personally like.	20	78	2	1
If a store I shop at frequently charges me lower prices than it charges other people because it wants to keep me as a customer more than it wants to keep them, that's OK.	26	72	2	1
Web site privacy policies are easy to understand.	28	70	2	2
I am more concerned about giving away sensitive information online than about giving away sensitive information any other way.	65	32	2	--
I know what I have to do to protect myself from being taken advantage of by sellers on the web.	65	33	1	1
I trust the U.S. government to protect consumers from marketers who misuse their information	35	65	--	1
I trust websites not to share information with other companies or advertisers when they say they won't.	43	55	--	1
When I go to a web site it can collect information about me even if I don't register.	47	45	1	7

*When the numbers don't add up to 100% it is because of a rounding error.

A= agree or agree strongly; D=disagree or disagree strongly; N=neither agree nor disagree;
DK=don't know

LINKING ATTITUDES AND BACKGROUNDS TO KNOWLEDGE

In the face of all the nervousness and seeming confusion around the laws and practices of behavioral targeting and price discrimination, it is startling that 65% of internet-using adult Americans nevertheless say they “know what I have to do to protect myself from being taken advantage of by sellers on the web.” One way to judge whether to accept this self-assessment is to examine their scores on the 17 true-false questions about laws and practices of price discrimination and behavioral targeting and about where they can turn for help if their marketplace information is used illegally. What shows up is a misplaced sense of confidence. People who say they know how to protect themselves score just as poorly on the true-false questions—and even the ones specifically regarding the online marketplace—as the people who don’t think they know how to protect themselves.

To get a sense of whether any of the attitude statements we presented to our respondents relate to higher or lower knowledge scores, we conducted a multiple regression where the score on the true-false test was regressed on the twenty-four attitudinal variables measured in the survey. Eight attitudes emerged as statistically significant predictors of knowledge; these are listed in Table 7, along with their corresponding regression coefficients. Together, these eight attitudes account for nearly 20% of the variance in knowledge ($R^2=0.197$). A positive coefficient indicates that as agreement with the statement increases, so does one’s score on the true-false test; a negative coefficient suggests that the more one *disagrees* with the statement, the greater one’s true-false knowledge.³⁶

Table 7: Predicting True/False Knowledge Score From Attitudes (N=1,087)

	Unstandardized Regression Coefficients <i>B</i>	Standardized Regression Coefficients <i>Beta</i>
A website can collect information about me even if I don’t register	0.470***	0.221
It’s OK if a store I shop at uses information about me to create a picture of me	0.432***	0.180
I get a better price shopping online than at the mall	0.217**	0.083
I am more concerned about giving away sensitive information online	-0.132*	-0.061
I am nervous about websites having information about me	-0.180*	-0.066
What companies know about me won’t hurt me	-0.232**	-0.081
I trust the U.S. government to protect consumers from marketers misusing their information	-0.333***	-0.143
Web site privacy policies are easy to understand	-0.408***	-0.158
CONSTANT	6.416	
<i>R</i> ²	0.197	

The attitudes were measured on a 5-point scale, where 1=strongly disagree and 5=strongly agree. N=1,087 and not 1,500 because people who answered “don’t know” were excluded. *=<.05 level significance; **=<.01 level; ***<.001 level

The findings suggest that people with relatively more knowledge consider themselves realists. They recognize that websites use information about them, and they accept it, perhaps because of the benefits doing business on the web affords them. People with more knowledge are more likely to agree, for example, that “I get a better price shopping online than at the mall.” They are less likely to say they are nervous about websites having information about them.

Curiously, this lower tendency to report emotional distress about website issues is connected to a greater tendency to admit intellectual concerns. People with more knowledge are more likely than those with less knowledgeable to agree that website privacy policies are difficult to understand. They are more likely to believe that what companies know about them *will* hurt them. And they are more likely than people with lower scores not to trust the federal government to protect consumers from marketers misusing their information.

Conversely, of course, internet-users who are less knowledgeable have a greater tendency to say they are more nervous. At the same time, they have a lesser tendency to believe that what companies know about them will hurt them and a greater chance of saying they trust the government to protect consumers. Their greater nervousness reflects uneasiness with the new marketing world. Despite this nervousness, though, they evidence a greater sense of corporate and government trust. We might suspect that for people whose knowledge about the online/offline marketing environment is low, the mix of nervousness and trust could cause them to vacillate between participating in online shopping and fearing it. In fact, we found a significant correlation between online shopping frequency and knowledge—people with lower knowledge scores shop less online—even when controlling for self-perceived ability to navigate the web.³⁷

It is important to point out that because these data are cross-sectional, we cannot draw conclusions about the direction of causality—that is, whether attitudes predict knowledge, or knowledge predicts attitudes. It is unclear, for example, whether knowing that the law does not protect people from price discrimination leads to distrust in the government, or if distrust in the government leads one to think—albeit correctly—that there are few laws that prohibit price discrimination. While the nature of multiple regression requires certain variables to be designated as either predictors (the attitudes) or outcome measure (knowledge), in this case these relationships should be not be assumed as causal but rather associative.

Causal direction becomes much less ambiguous, however, when we consider the relationships between demographic variables and knowledge. That is, we know with certainty that knowledge of price discrimination cannot cause categories such as gender and household income; logically, the direction is the other way. To determine which demographic characteristics of internet-using adults are the strongest predictors of knowledge, we again used multiple regression. The score on the true-false test was regressed on education, income, gender, race, and self-perceived ability to navigate the internet.³⁸ The results reported in Table 8 suggest that each of these variables is a significant predictor of a higher knowledge score, even when controlling for the influence

of the others. Specifically, people with more years of education, higher incomes, and greater online expertise score better on the test. Men and people who designated themselves as white are also more likely to do better on the test.

Understanding the larger significance and dynamics of these relationships remains open to future research. What does seem quite clear from the findings, though, is the relatively important role education plays in predicting people's knowledge about the laws and practices surrounding price discrimination and behavioral targeting. As judged by the magnitude of the standardized regression coefficients reported in Table 8, of all characteristics in people's backgrounds, having more years of education is the best determinant of understanding basic realities about power to control information about individuals and the prices they pay in the online/offline marketplace.

Table 8: Predicting True/False Knowledge Score From Demographics (N=1180)

	Unstandardized Regression Coefficients <i>B</i>	Standardized Regression Coefficients <i>Beta</i>
Education	0.630***	0.200
Income	0.383***	0.150
Self-perceived ability to navigate internet	0.616***	0.149
Race (white)	0.936***	0.100
Gender (male)	0.517**	0.073
CONSTANT	2.687	
R ²	0.148	

N=1,087 and not 1,500 because people who answered "don't know" were excluded.

significance<.01 level; *significance<.001 level

Interestingly, those with a higher education tend to be more modest about knowing how to protect themselves "from being taken advantage of by sellers on the web."³⁹ Their modesty is perceptive, and appropriate. In all of the relationships noted here, a "higher" knowledge score is not necessarily an impressive performance. Even having more general schooling doesn't necessarily mean really being well-informed about the laws and practices surrounding behavioral targeting and price discrimination. People whose formal education ended with a high school diploma know correct answers to an average of 6.1 items out of a possible 17. People with a college degree do better—8.1—but that still means they get only 45% right. Even people with graduate school or more average 8.9—just 51% correct.

CONCLUDING REMARKS

The most hopeful way to see our survey is as a benchmark for the new era that is unfolding. As U.S. society moves further into the twenty-first century, prices that vary based on firms' information about us could become an increasing feature of the marketplace. Trade magazine articles and discussions with industry experts suggest strongly that database-driven price distinctions will spread. Growing numbers of retailers will use information consumers never knew they revealed to draw conclusions about their buying patterns that they would not have wanted.

The findings suggest that most internet-using adult Americans will fall prey to marketplace manipulations even while many believe (incorrectly) that they know how to handle themselves. Already we find that 68% of American adults who have used the internet in the past month believe incorrectly that "a site such as Expedia or Orbitz that compares prices on different airlines must include the lowest airline prices." 64% of American adults who have used the internet recently do not know it is legal for "an online store to charge different people different prices at the same time of day." 71% don't know it is legal for an *offline* store to do that. Consumers who are not aware of how price discrimination and behavioral targeting work, of what rights they hold when it comes to companies' using knowledge about them, and of how to respond to these circumstances may find themselves consistently paying more than others for the same products.

Our data indicate that overwhelming portions of internet-using adult Americans object to price discrimination that is guided by behavioral targeting. Our data also suggest they would be quite angry if they found out it is happening to them. Americans who suspect themselves disadvantaged as a result of these often-hidden activities (but don't know what to do about them) may well turn against the corporate and government institutions who they believe are encouraging the practices. That could ignite new marketplace tensions—and possibly even broader frictions—with U.S. society.

We suggest three policy initiatives:

- **The Federal Trade Commission should require websites to drop the label *Privacy Policy* and replace it with *Using Your Information*.** We found that 75% of internet-using adults do not know the correct response—false—to the statement, "When a website has a privacy policy, it means the site will not share my information with other websites and companies." For many people, then, the label is deceptive; they assume it indicates protection for them. A *Using Your Information* designation will likely go far toward reversing the broad public misconception that the mere presence of a privacy policy automatically means the firm will not share the person's information with other websites and companies.
- **U.S. school systems—from elementary through high school—must develop curricula that tightly integrate consumer education and media literacy.** We found that though education related positively to a better score on the true-false test, having a high level of general schooling doesn't necessarily mean being

well-informed about the laws and practices surrounding behavioral targeting and price discrimination or about where people can turn for help if marketplace information is used illegally. We conclude that specific consumer education linked to media literacy is needed in addition to general schooling to improve the public's understanding of market practices.

Consumer education (which is often considered part of the larger umbrella of economic or financial education) varies dramatically state-to-state. Several non-profit organizations such as the Jump\$tart Coalition for Personal Financial Literacy and the National Council on Economic Education have as their goal the financial competency of America's young people. According to Jump\$tart, in early 2004 only 15% of high school graduates nationally had taken a course covering the basics of personal finance.⁴⁰

There is, however, growing awareness of the need to make financial education a priority both at the federal and state levels. The 2002 education bill commonly called the No Child Left Behind Act includes an Excellence in Economic Education (EEE) program to promote economic, financial, and consumer education in grades K through 12. In July 2004, the Department of Education granted its first EEE award of \$1.48 million to the National Council on Economic Education.⁴¹ Though advocates of financial education for youngsters applaud the grant, they also point out that the amount awarded is small for the work that needs to be carried out.

If consumer education has little visibility in elementary through high school, media literacy is virtually nonexistent. Educators typically justify the lack of attention by saying that they have a hard enough time covering the standard curriculum; they consider media education a luxury, a kind of icing on the educational cake.

But the developments that motivated our survey should underscore one reason that media literacy is a necessity rather than a luxury. More and more, cutting-edge media vehicles are becoming integral to the selling environment. Computers with commercials and interactive messages are showing up on supermarket shopping carts. Checkout areas in all sorts of retailers are places where discount coupons are selectively printed based on database information that the stores accumulated during previous visits or bought from data brokers. Websites use a myriad of data-collection approaches that have consequences for the ads people see, the products they encounter, and the prices they pay.

These techniques and more are redefining the shopping and media landscapes. Educators must integrate an understanding of media and marketing into the curriculum so that contemporary elementary and high school students do not repeat the ignorance, fear, and distrust that we noted with today's adults when it comes to central trends in the marketplace.

- **The government should require retailers to disclose specifically what data they have collected about individual customers as well as when and how they use those data to influence interactions with them.** In one of the saddest findings of our survey, 81% of respondents *disagreed* that "What companies

know about me won't hurt me." This basic, widespread concern that businesses' collection of information about individuals can cause them harm ramified through the interviews. It showed up most prominently in our several attempts to tap into people's attitudes toward different forms of price discrimination. Perhaps sometimes to the point of naïveté, this nationally representative sample of internet-using adults insisted on fairness in pricing. Fully 91% thought it wrong if their supermarket charges people differently for the same products during the same hour. 87% said the same thing about online stores, and 84% said that websites should be required to let customers know if they vary charges for the same items during the same period.

Clearly, people are begging for transparency in their relationships with marketers. In our general questions and through our scenarios, we found that they object to behavioral tracking and to companies buying information about them without their knowledge. It may well be that if informed about now-surreptitious price discrimination activities that affect them, internet-using adult Americans would still view the practices as unfair. But they believe it is their right to know. Perhaps in an environment of greater trust and openness certain kinds of preferential dealings would be acceptable—just as publicly announced price preferences for senior-citizens are acceptable in U.S. society today.

Government actions are critical to establishing an atmosphere of marketplace transparency and trust. The broad disagreement we found with the statement that the U.S. government will protect consumers from marketers who misuse their information indicates there is much that public officials must do to regain the public's trust. It also suggests the connection between people's attitudes as consumers and their roles as citizens. A well-developed, critically informed understanding of how the new worlds of media and commerce work together can have favorable consequences for the ways people view key institutions of society as well as the environments in which they shop.

References

- ¹ See, for example, D. Zwick, and N. Dholakia, (2004, June), "Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing," *Journal of Macromarketing*. 24(1) 31; and Carol Krol, DM budgets heading upward. *B to B*, May 3, 2004, p. 14.
- ² See, for example, K. Carroll and D. Cates (1999), "Teaching Price Discrimination: Some Clarification," *Southern Economic Journal* 66(2), 466-480; J.V. Koch and R.J. Cebula, (2002), "Price, Quality, and Service On The Internet: Sense and Nonsense," *Contemporary Economic Policy* 20(1), 25-37; and S. K. Clerides (2004), "Price Discrimination With Differentiated Products: Definition and Identification," *Economic Inquiry* 42(3), 402-413.
- ³ E. Garbarino and O.F. Lee (2003), "Dynamic pricing in internet retail: Effects on consumer trust," *Psychology & Marketing* 20(6), 495-513.
- ⁴ See, for example, [No author], "Sight Lines: RFID, labor, and Wal-Mart aren't going away, but this year will bring in a new crop of industry challenges. Here's a look at what lies ahead," *Progressive Grocer*, January 1, 2005, <http://www.progressivegrocer.com>; Tom Weir, "Scanning the Future," *Supermarket Business Magazine*, October 15, 2000, p.34.
- ⁵ As an example, see the Bloomingdales site registration area:
<https://www.bloomingdales.com/myinfo/register/index.ognc>
- ⁶ See, for example, T. Zeller Jr., "Release of Consumers' Data Spurs Choicepoint Inquiries," *New York Times*, March 5, 2005, Sec C, p. 2.
- ⁷ See T. Zeller Jr., "Another Data Broker Reports a Breach," *New York Times*, March 10, 2005, Sec C, p. 1.
- ⁸ The regulations relate to the Health Insurance Portability and Accountability Act of 1996 (HIPPA); the Financial Modernization Act (Graham-Leach-Bliley Act), and The Children's Online Privacy Act (COPA).
- ⁹ Epiphany, "Case Study: American Airlines,"
http://epiphany.com/products/downloads/Amer_Airlines_CS.pdf, p. 3.
- ¹⁰ Epiphany, "Case Study: American Airlines,"
http://epiphany.com/products/downloads/Amer_Airlines_CS.pdf, p. 4.
- ¹¹ Epiphany, "Case Study: American Airlines,"
http://epiphany.com/products/downloads/Amer_Airlines_CS.pdf, p. 4.
- ¹² Epiphany, "Case Study: American Airlines,"
http://epiphany.com/products/downloads/Amer_Airlines_CS.pdf, p. 5.
- ¹³ Lorraine Calvacca, "Data on Demand," *Direct*, July 1, 2004, p.9.
- ¹⁴ See, for example, Carrie A. Johnson, "The US Consumer 2004: Multichannel and In-Sore Technology," Forrester Data Overview, September 20, 2004, p. 2.
- ¹⁵ "Customer Recognition Solutions," Acxiom website, January 5, 2005.
http://acxiom.com/default.aspx?ID=1841&Country_Code=USA
- ¹⁶ See, for example, C. S. Overby, "Maximizing Grocery Loyalty Data," Forrester Research *Trends*, February 24, 2005; and C. A. Johnson, "Getting Multichannel Retailing Right," Forrester Research *Best Practices*, December 10, 2004.
- ¹⁷ Segmentation Analysis: "P\$cycle," Claritas website, accessed March 23, 2005.
<http://www.clusterbigip1.claritas.com/claritas/Default.jsp?main=3&submenu=seg&subcat=segpsycle#groupl1>
- ¹⁸ R. H. Levey, "Bloomingdale's Goes for the Best," *Direct*, January 1, 2004, p. 1.
- ¹⁹ S. Klein, CEO of Information Resources Inc. quoted in Jack Neff, "Why Some Marketers Turn Away Customers," *Advertising Age*, February 14, 2005, p. 1
- ²⁰ R. Shulman, "Picking Your MVPs," *Progressive Grocer*, March 1, 2005, via Nexis.
- ²¹ R. H. Levey, "Bloomingdale's Goes for the Best," *Direct*, January 1, 2004, p. 1.
- ²² Press reports have identified Filene's and Best Buy in this regard. See, for example, B. Mohl, "Facing Their Demons Firms Intentionally Use Poor Service, Other Direct Methods To Weed Out Profit-Zapping Customers," *Boston Globe*, July 27, 2003, p. F1; and R. Shulman, "Picking Your MVPs," *Progressive Grocer*, March 1, 2005, via Nexis.
- ²³ Telephone discussion with Michelle Bauer of Catalina Marketing, March 2005.
- ²⁴ W. Baker, W., M. Marn, M., & C. Zawada, (2001). "Price smarter on the net." *Harvard Business Review* 79(2), 122-127.

-
- ²⁵ M. Kung, M., K.B. Monroe, and J.L. Cox (2002). "Pricing on the internet," *The Journal of Product and Brand Management* 11(4/5), 274-287.
- ²⁶ See J. Adamy, "E-tailer price tailoring may be wave of future," *Chicago Tribune*, September 25, 2000.
- ²⁷ William McGee, "Major Travel Sites Face Credibility Crunch," March 1, 2005. <http://www.consumerwebwatch.org/dynamic/travel-report-first-class-airfare-abstract.cfm>
- ²⁸ Personal communication to the author, May 2, 2005.
- ²⁹ R.M. Weiss and A.K. Mehrotra (2001), "Online dynamic pricing: Efficiency, equity and the future of e-commerce," *Virginia Journal of Law and Technology* 6(2), p. 28. Retrieved January 31, 2005 from <http://www.vjolt.net/vol6/issue2/v6i2-a11-Weiss.html>
- ³⁰ J. D. Gertz, "The Purloined Personality: Consumer Profiling in Financial Services," *San Diego Law Review*, Summer 2002, p. 943.
- ³¹ C. Hoofnagle, "Privacy Self Regulation: A Decade of Disappointment," January 19, 2005, at <http://ssrn.com/abstract=650804>
- ³² E. Garbarino and O.F. Lee (2003), "Dynamic pricing in internet retail: Effects on consumer trust," *Psychology & Marketing* 20(6), 495-513; and D. Grewal, D. Hardesty and G. Iyer (2004). The effects of buyer identification and purchase timing on consumers' perceptions of trust, price fairness, and repurchase intentions. *Journal of Interactive Marketing* 18(4), 87-100.
- ³³ According to ICR, during the fourth quarter of 2004, Centris surveyed 12,422 people. The percent of adults who "used the internet in the past 30 days at home, work or anywhere else" was 56.4%. The percentage of households in which an adult accessed the internet in the past 30 days was 53.6%.
- ³⁴ A. Litan, "Phishing Attack Victims Likely Targets for Identity Theft," Gartner research document ID Number FT-22-8873, May 5, 2005. See also Kevin Coughlin, "Hackers Keep Up With Every High-Tech Development," Newhouse News Service, May 4, 2005, via Nexis: "According to Gartner, two million Americans have taken the bait and supplied Social Security and credit-card numbers, as well as other sensitive data to phishers, often in far-flung crime rings. At least 2,625 active phishing sites were reported in February by the Anti-Phishing Working Group."
- ³⁵ Older people and women, in particular, were most likely to object to the price discrimination and behavioral targeting scenarios, according to the results of a multiple regression that examined the influence of demographic variables on individuals' responses to the scenarios. This is also consistent with findings related to individuals' more generalized attitudes toward price discrimination and the use of personally identifiable information in the marketplace; gender (i.e., female) and age were almost always found to be correlated with disagreement with such practices. While the present data do not allow us to explain why these relationships exist, this presents a tantalizing question for future research.
- ³⁶ The magnitude of each coefficient represents the gain in knowledge that will occur as a result of a 1-unit increase in the attitude. Thus, given a 1-unit increase—for example, a change from "agree" to "strongly agree"—in the first attitude listed in the table, "A website can collect information about me even if I don't register," an individual's score on the true-false test would rise by 0.470. The standardized coefficients have been transformed so that all coefficients are measured on the same scale, with a mean of zero and a standard deviation of 1; this allows them to be directly comparable to one another, with the largest coefficient indicating which attitude relates most strongly to the knowledge score.
- ³⁷ The partial correlation between online shopping and knowledge, controlling for ability to navigate the web, is .155 ($p<.001$).
- ³⁸ Because a full 73% of the sample identified as non-Hispanic white, race was entered into the regression as a dichotomous variable (white versus non-white). Respondents' age was not included in the regression because it was found that it was not linearly related to knowledge. Instead, there is a curvilinear relationship between the two variables, such that the youngest (18-29) and oldest (65+) internet users have less knowledge than those who are of intermediate age (30-64).
- ³⁹ A correlation between education and believing that one is capable of protecting oneself was significant and negative ($r=-.118$, $p<.001$), suggesting that individuals with greater education are actually more likely to admit being vulnerable to exploitation by web merchants.
- ⁴⁰ "Jump\$tart sees surge in Legislation Promoting Financial Literacy," Jump\$tart press release, March 5, 2004, <http://www.jumpstart.org/fileuptemp/ACF17B5.doc>
- ⁴¹ See Educational Testing Service, "The No Child Left Behind Act: A Special Report," ETS, June 2002, <http://ftp.ets.org/pub/corp/nclb.pdf>; and [No author], "Today's Events in Washington," July 21, 2004, The Frontrunner, via Nexis.

NOTES

NOTES

Cookie:TShram@google.com/mobile

Cookie:TShram@tvguide.com/PartnerGrid

Cookie:TShram@www.dell.com/phpvm2

Cookie:TShram@voip.fabphone.co.uk/voip/promo

Cookie:TShram@www.toadhammer.com/publication

Cookie:TShram@www.comcastsupport.com/sccuser/rnn

Cookie:TShram@www.ebay.com/rtm/main

Cookie:TShram@stat.upc.com/sb/

Cookie:TShram@www.comcastrupport.com/sdCookie:TShram@user

Cookie:TShram@bing.com/search

Cookie:TShram@www.google.com/mobile

Cookie:TShram@onlinestores.metaservices.microsoft.com/services/watching

Cookie:TShram@www.librarything.com/tag

Cookie:TShram@www.google.com/talk

Cookie:TShram@ytsa.net/tase

Cookie:TShram@community.adobe.com/help/api/v1/thumbs

Cookie:TShram@google.com/verify

Cookie:TShram@google.ca/verify

Cookie:TShram@www.windowsmobile.com/windows/mobile

SNID

27=1JR2BZwybn9ozsGG7nzQprKfpqOX_Ai6QDcxTmOf4Q=SSDIBYXE3on3iWwc

google.com/verify

9728

2320728704

30067751

406026352

30030938

*

ach-search

UjiezX7sFgNwJhrie19zsC69Vu8=

community.adobe.com/help/api/v1/thumbs/

1536

2784647552

30759988

3564042032

30025733

*

sik_client_guid

47aeeb428-73bc-ada9-bb60-728dc6367a7

www.comcastsupport.com/bsnuser/rnn

Joseph Turow
Annenberg School for Communication, University of Pennsylvania

Jennifer King

University of California, Berkeley, School of Law, Berkeley Center for Law & Technology

1088

284664448

30089887

2560430544

30016461

*

SynZCSI

K_25_503=10036:80001

tvguide.com/PartnerGrid

Chris Jay Hoofnagle

University of California, Berkeley, School of Law, Berkeley Center for Law & Technology

Amy Bleakley

Annenberg Public Policy Center, University of Pennsylvania

Michael Hennessy

Annenberg Public Policy Center, University of Pennsylvania

Contrary to what marketers say,

AMERICANS REJECT TAILORED ADVERTISING

AND THREE ACTIVITIES THAT ENABLE IT

Joseph Turow, Ph.D., is Robert Lewis Shayon Professor of Communication at the Annenberg School for Communication, University of Pennsylvania. Among his several books are *Niche Envy: Marketing Discrimination in the Digital Age* (MIT Press, 2006) and *Breaking Up America: Advertisers and the New Media World* (U of Chicago Press, 1997). Since 1999 he has conducted national telephone surveys that have moved forward public discourse on digital media, marketing, and privacy. Several can be found at the Annenberg Public Policy Center website, APPCPenn.org.

Jennifer King, MIMS, is a Ph.D. student at the UC Berkeley School of Information. Most recently she was a researcher at the Samuelson Law, Technology, and Public Policy Clinic at UC Berkeley's School of Law. Her research areas include information privacy and security, usability and human-computer interaction, video surveillance and other sensor networks. With Chris Hoofnagle, King has published three reports exploring Californians' privacy attitudes; these are available at ssrn.com.

Chris Jay Hoofnagle, J.D., is director of the Berkeley Center for Law & Technology's information privacy programs and senior fellow to the Samuelson Law, Technology & Public Policy Clinic. He is an expert in information privacy law. Hoofnagle co-chairs the annual Privacy Law Scholars Conference. He is licensed to practice law in California and Washington, DC.

Amy Bleakley, Ph.D., MPH, is a Research Scientist in the Health Communication Group of the Annenberg Public Policy Center at the University of Pennsylvania. Dr. Bleakley studies adolescent sexual behavior, sexual and reproductive health policies, health behavior theory, and contextual influences on health behavior. Her current research focuses investigating the effect of sexual content in the media on adolescent sexual development.

Michael Hennessy, Ph.D., is Project Manager and Statistician in the Health Communication Group of the Annenberg Public Policy Center. His major interest is the integration of structural equation modeling and intervention program/behavioral theory, growth curve analysis of longitudinal data, and using factorial surveys to design both behavioral intervention programs and community-based clinical trials for experimental vaccines. He has published over 90 articles in *Evaluation Review*, *Structural Equation Modeling*, *AIDS and Behavior*, *Psychology Health & Medicine*, *The American Journal of Evaluation*, and *Evaluation and the Health Profession* among other journals.

September, 2009

This survey was supported by the Rose Foundation for Communities and the Environment, Tim Little, Executive Director, under grant 025629-003, Chris Jay Hoofnagle, Principal Investigator; and by The Annenberg School for Communication—Michael Delli Carpini, Dean.

Overview

Contrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests. Moreover, when Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages—between 73% and 86%—say they would not want such advertising.

These are two findings from the first nationally representative telephone (wireline and cell phone) survey to explore Americans' opinions about behavioral targeting by marketers, a controversial issue currently before government policymakers. Behavioral targeting involves two types of activities: following users' actions and then tailoring advertisements for the users based on those actions. While privacy advocates have lambasted behavioral targeting for tracking and labeling people in ways they do not know or understand, marketers have defended the practice by insisting it gives Americans what they want: advertisements and other forms of content that are as relevant to their lives as possible.

We conducted this survey to determine which view Americans hold. In high percentages, they stand on the side of privacy advocates. That is the case even among young adults whom advertisers often portray as caring little about information privacy. Our survey did find that younger American adults are less likely to say no to tailored advertising than are older ones. Still, more than half (55%) of 18-24 year-olds do not want tailored advertising. And contrary to consistent assertions of marketers, young adults have as strong an aversion to being followed across websites and offline (for example, in stores) as do older adults. 86% of young adults say they don't want tailored advertising if it is the result of following their behavior on websites other than one they are visiting, and 90% of them reject it if it is the result of following what they do offline. The survey uncovered other attitudes by Americans toward tailored content and the collection of information about them. For example:

- Even when they are told that the act of following them on websites will take place anonymously, Americans' aversion to it remains: 68% "definitely" would not allow it, and 19% would "probably" not allow it.
- A majority of Americans also does not want discounts or news fashioned specifically for them, though the percentages are smaller than the proportion rejecting ads.
- 69% of American adults feel there should be a law that gives people the right to know everything that a website knows about them.
- 92% agree there should be a law that requires "websites and advertising companies to delete all stored information about an individual, if requested to do so."
- 63% believe advertisers should be required by law to immediately delete information about their internet activity.

- Americans mistakenly believe that current government laws restrict companies from selling wide-ranging data about them. When asked true-false questions about companies' rights to share and sell information about their activities online and off, respondents on average answer only 1.5 of 5 online laws and 1.7 of the 4 offline laws correctly because they falsely assume government regulations prohibit the sale of data.
- Signaling frustration over privacy issues, Americans are inclined toward strict punishment of information offenders. 70% suggest that a company should be fined more than the maximum amount suggested (\$2,500) "if a company purchases or uses someone's information illegally."
- When asked to choose what, if anything should be a company's single punishment beyond fines if it "uses a person's information illegally," 38% of Americans answer that the company should "fund efforts to help people protect privacy." But over half of Americans adults are far tougher: 18% choose that the company should "be put out of business" and 35% select that "executives who are responsible should face jail time."

It is hard to escape the conclusion that our survey is tapping into a deep concern by Americans that marketers' tailoring of ads for them and various forms of tracking that informs those personalizations are wrong. Exactly why they reject behavioral targeting is hard to determine. There may well be several reasons. One may be a general antagonism to being followed without knowing exactly how or with what effects. Americans may not want their behavior on one site to somehow affect the interaction with subsequent sites. Consumers may intend to divide their web browsing into different subjective contexts (e.g. shopping, work, play, education), and they may worry that tracking across those contexts may subject them to embarrassment (e.g. while using the computer in the work context, ads may be displayed that are relevant to play). Another reason might be a fear that selective presentation of advertisements, discount offers, or news will put them at a monetary or social disadvantage: some people might get more useful or interesting tailored content than others depending on the conclusions marketers draw about them. The rejection of even anonymous behavioral targeting by large proportions of Americans may mean that they do not believe that data about them will remain disconnected from their personally identifiable information. It may also mean that anonymity is not the only worry they have about the process. Being labeled in ways they consider unfair by marketers online and off may be just as important a concern.

Whatever the reasons, our findings suggest that if Americans could vote on behavioral targeting today, they would shut it down. The findings also suggest that marketers and government policymakers may be faced with a backlash if Americans were to organize around complaints that the laws they think protect them from the sale of their data actually don't exist. It is also important to note that this rejection of tailoring and behavioral tracking by marketers and media firms does not mean Americans reject the idea of customizing ads, discounts, and news themselves. To the contrary, evidence from around the digital world shows that they want to control and shape what

content they receive. The problem for marketers is that Americans are worried about others' use of data about them in ways they do not know or understand, and might not like.

In fact, our survey found that Americans want openness with marketers. If marketers want to continue to use various forms of behavioral targeting in their interactions with Americans, they must work with policymakers to open up the process so that individuals can learn exactly how their information is being collected and used, and then exercise control over their data. At the end of this report, we offer specific proposals in this direction. An overarching one is for marketers to implement a regime of *information respect* toward the public rather than to treat them as objects from which they can take information in order to optimally persuade them.

Background

Behavioral targeting (BT) has quickly become one of the central, yet most controversial, vehicles for reaching consumers in the digital age. Critics' calls for its restriction run parallel to marketers' statements about its crucial nature as a lifeline for the new media age. Yet the arguments about the process, which include claims about public attitudes, discuss it as if it is a single act, when it is really made up of many parts that can and should be evaluated separately from a public interest standpoint. To help with that evaluation, policymakers, social advocates, and marketers need public-opinion benchmarks about the distinct yet related activities that make up the process.

With that goal in mind, this study for the first time disentangles Americans' attitudes toward tailored content from their opinions about three common behavioral tracking methods. Behavioral tracking involves following an individual's activities over time and the using the information to select which advertisements to display to that individual. Advertisers believe the practice helps them deliver their persuasive messages to audiences who are most likely to be interested. Tailoring of content involves the creation or alteration of media material to suit marketers' perceived interests of an individual or individuals.

This study concerns three types of companies—websites, advertising networks, and offline retailers—that carry out contemporary behavioral targeting. Websites closely follow the movements of visitors—for example, what articles they read, what ads they clicked, what products they started to buy but didn't purchase. The site can serve up ads to the person based on the topic selected—for example, a movie ad if the person is viewing movie reviews. The sites can also save the records of these actions and link them to the visitor by placing identifying text files called *persistent cookies* on the visitor's computer. When a user of that computer returns, the site can serve relevant advertisements based on the visitor's previous activity patterns. For example, if the past visits indicate particular attention to newspaper site's travel section, the website can serve ads from its travel advertisers to that visitor.

Advertising networks also track visitors and store their peregrinations, but across thousands, even tens of thousands, of websites that accept ads from those firms and share in the revenues. This approach means that ads served to site visitors by networks owned by Google, Yahoo, AOL,

ValueClick and many other firms may reflect a history of movements through the online world. In the most basic sense, a person who visited an auto site to search for used Mini Coopers might find himself shown a Mini Cooper ad on a newspaper site he visits the next day if the newspaper is part of the same advertising network.

Offline retailers also track visitors, most often through frequent shopper cards. As in the online world, supermarkets and drug stores may use the data to selectively send advertisements to different cardholders based on the different shopping experiences. The stores may also present special prices and shopping experiences to individuals whom they identify while they are in the stores. The Stop-and-Shop supermarket chain, for example, has experimented with giving people carts with devices activated by their frequent-shopper cards to which they can email shopping lists and which present them with offers based on past and present shopping behavior. Beyond bringing digital technology to the physical store, merchants are also merging the data they have about their customers from the web, the phone, and the store floor in an attempt to get a unified view of individual customers' behavior.

Websites, advertising networks, and offline retailers often rely on database technology companies to help them carry out behavioral targeting in the most sophisticated ways possible. One such firm, Audience Science, states that its work involves “recording billions of behavioral events daily and reaching over 385 million unique Internet users” who then make the data available to its clients: “Web publishers, marketers, networks, exchanges, and agencies to create intelligent audience segments to connect people with relevant advertising driving the transition to data-driven audience marketing online.”¹ To further enhance their knowledge of individual customers, offline stores and individual websites often go beyond tracking behavior to explore the backgrounds of members of their audience who seem to be particularly good prospects for sales or to present to advertisers. Over the past few decades, the sale and purchase of information on individuals has become big business. American privacy law is sectoral, meaning that certain businesses are restricted from selling information without consumer consent, but those rules apply in limited circumstances. Generally, companies have virtually free rein to use data in the U.S. for business purposes without their customers’ knowledge or consent. Websites and stores can therefore easily buy and sell information on valued visitors with the intention of merging behavioral with demographic and geographic data in ways that will create social categories that advertisers covet and target with ads tailored to them or people like them.

Unlike individual websites and offline retailers, however, advertising networks today typically don’t know the names or postal addresses of the people they track across the web. The networks consequently can’t buy personally identifiable data about them. They have, however, parlayed the desire to know consumers’ personalities and demographics into major enterprises to connect the millions of information dots they have about their users in ways that will appeal to advertisers. Complex dot-connecting formulas are used by ad networks of Google, Yahoo, AOL, Value Click and other firms to label millions of people according to categories that reflect inferences about gender—whether a person’s search habits are feminine or masculine—as well as lifestyle and

personality—for example, whether a person is a soccer mom and/or world traveler. Ad networks still hold rather few geographic, demographic, and psychographic and lifestyles categories about individual web users. Nevertheless, the knowledge in these networks is growing and the tracking is spreading beyond the web to mobile handsets and television set-top boxes.

The reason websites, advertising networks and offline retailers are so intent on keeping track of their visitors has to do with the desire to tailor the messages that they deliver. Many advertisers believe that learning customers' present and past browsing and shopping habits can suggest what products would appeal to them and what advertising messages will catch their attention. Just as the process of making inferences about consumers is proceeding apace, so the technology to tailor commercial messages to them is becoming increasingly efficient across a variety of digital media, including television. Coupons are already tailored for individuals in physical stores, websites, and mobile handsets based on data-driven shopping, traveling and demographic patterns. And although advertisers' contemporary focus is on ads and coupons, it is also possible to present people with different offerings of entertainment and news based on analyses of their interests or their marketing profiles—starting with the kinds of recommendation engines characterized by Amazon.com and going far beyond them. News and entertainment distributors may increasingly explore the proposition that tailoring material—even just headlines and promotional materials—based on what they have learned from tracking audiences will encourage return visitors who will provide yet more information to use for targeting ads to them. Technology companies such as Visible World already offer technology that can insert products into television entertainment programs in real time based on information about the family that their cable company has placed into their set boxes based on their viewing behaviors and additional information the firm has learned about them.

Critics and Defenders

Critics of behavioral targeting complain that it is wrong to gather so much data about individual Americans, create dossiers about them without their awareness, and use the data to surround them with ads based on social and consumer categories that the citizens have not validated and might not agree with. While deleting one's browser cookies is often recommended as a quick fix for preventing tracking, it's a practice users must repeat often because websites place new cookies at each new visit. In addition, an increasing number of websites are installing *Flash cookies*, which also allow site visits to be tracked. More than half of the internet's top websites use them, according to a recent UC Berkeley study led by Ashkan Soltani and Chris Hoofnagle.² Also known as local shared objects (LSOs), Flash cookies are stored in connection with the Adobe Flash player and cannot be erased through the cookie privacy controls in a browser. In order to delete Flash cookies on a user's computer, a user must visit Adobe's website and use an online settings manager tool.³ The consequence, noted a *Wired* magazine article, is that "even if a user thinks they have cleared their computer of tracking objects, they most likely have not." Moreover, sites have even begun to use the Flash cookies as backups to reinstate traditional cookies that a user deleted, a process that is called *re-spawning*.

Calls for an opt-in approach whereby individuals would have to consent to being tracked, are often dismissed by the advertising industry as unrealistic. Demands to let users opt out have met with half-hearted assent. Companies that allow opt out possibilities often make it hard for consumers to learn how to do it. Regardless, when a consumer clears his or her browser cookies, any opt out cookies are erased along with regular cookies, putting consumers in an impossible bind between refusing to allow cookies (causing most websites to be completely unusable), or deleting unwanted cookies manually, one by one. The difficulty even applies to sites belonging to the National Advertising Initiative's Opt-Out Program: Note 11 of its FAQ points out that "If you ever delete the 'opt-out cookie' from your browser, buy a new computer, or change Web browsers, you'll need to perform the opt-out task again."⁴ Note, too, that in some cases opting out of advertising does not prevent websites from tracking. Instead, it stops them from sending tailored ads. If one conceives of the privacy objection to online advertising as related to tracking, opting out does nothing to quell that concern.

TRUSTe, a company that promotes privacy practices and a related approval seal to websites as a way to gain consumer confidence, noted in March 2009 that "Behavioral advertising still represents uncharted territory, without clearly applicable laws or regulations." In February 2009, the Federal Trade Commission (FTC) published guidelines for companies collecting behavioral data of web users with the aim of presenting tailored advertising to them. The principles encourage transparency and customer control, security of customer data and the retention of customer information for a limited period.⁵ Seemingly in response to such pressure, Google now allows visitors to its site to learn the categories it identifies with their browser's cookie, and to opt out of such cookie-linking if they wish. Google's "permanent opt-out" process takes several steps, however, and neither Google nor any other major company explains where it received such information, how it arrived at its conclusions, or gives people the right to challenge what they consider misperceptions.⁶ In fact, as *Wired* magazine noted in August 2009, the attempts at self-regulation by the online tracking and advertising industry "have conspicuously failed to make the industry transparent about when, how and why it collects data about internet users."⁷

A key reason advertising executives have held back allowing transparency and offering consumers choices regarding behavioral tracking might be the activity's immense value—it is "the future in digital advertising," in the words of a TRUSTe executive⁸—together a parallel concern that consumers would opt out if they learned about it. *New York Times* reporter Louise Story put their dilemma concisely:

Underscoring all the debates about online privacy, behavioral targeting and Internet advertising is a hard, cold reality: content costs money. . . .

As mass advertising dies, there is more pressure for media companies to develop audiences with more specific interests and characteristics. From an economic standpoint, the drop in the total number of eyeballs means the eyeballs that remain must become more lucrative.

Media companies are also using targeting, often called behavioral targeting, to provide more valuable eyeballs. . . .⁹

Marketing executives typically justify behavioral targeting by making two claims related to tailoring and tracking. The first is that Americans want advertisements tailored to their interests; implicitly this requires learning about them through tracking their behavior. The other assertion is that only older consumers worry about the privacy issues related to behavioral tracking.

The notion that the younger generations really don't care about tracking was repeated recently by Disney CEO Robert Iger who told a July 2009 Fortune Brainstorm Tech conference that media companies should use individual tracking data to target ads and that younger people "don't care" about the privacy aspects around this. "Kids don't care," Iger said, adding that his own adult children "can't figure out what I'm talking about" when he asks them about their online privacy concerns.¹⁰

Iger went on to herald the value for Disney of using tracked data to tailor ads: "If we know that you've gone online and looked at five different autos online, you are a great consumer for us to serve up a 30-second ad for a car," he said. To marketers, it is self-evident that consumers want customized commercial messages. Typical of this claim for tailoring is the perspective of an executive at customer-relationship-management firm Dunnhumby USA. He notes that "Something amazing happens when marketing efforts are actually relevant to people. We see this step as initiating that crucial dialogue. And shoppers, for their part, are replying; essentially giving their permission to marketers to learn their habits and respond accordingly."¹¹ Reflecting that assumption, AudienceScience states that its "sophisticated behavioral targeting technology enables the company to improve its user experience by making the ads shown more relevant to each viewer, as well as offer its advertisers a higher level of engagement and return."¹² Similarly, Google's light description for the public of its AdSense contextual and behavioral advertising program states that "It's our goal to make these ads as relevant as possible for you. While we often show you ads based on the content of the page you are viewing, we also developed new technology that shows some ads based on interest categories that you might find useful."¹³ And the National Advertising Initiative, in its web page that allows opting out of member advertising networks, informs visitors thinking about the decision in bold type that "Opting out of a network does not mean you will no longer receive online advertising. It does mean that the network from which you opted out will no longer deliver ads tailored to your Web preferences and usage patterns."¹⁴

The Right Questions of the Right Samples

The advertising industry's stress on the utility of behavioral targeting for Americans because they enjoy relevant advertising raises a number of basic questions: First, do Americans in fact want advertisers to tailor advertising to their interests? Second, if they say they want tailored advertising, would they continue to want it when told that it results from following their activities—for example,

on individual websites, across websites, and in physical stores? And is it indeed the case that younger American adults tend not to be concerned about tracking and tailoring?

Prior to the research reported here, we did not have straightforward answers to these separate questions. Several studies do show strong concern for internet privacy among Americans and a desire for firms not to collect information about them online. It seems clear, too, that Americans value the right to opt out from this sort of collection. For example, in a 2008 national telephone survey, Consumers Union found that 72% of Americans 18 years and older “want the right to opt out when companies track their online behavior.” But regarding Americans’ response to behavioral targeting and tailoring, the findings are less clear. As far as we can tell the only publicly available studies on the subject are from a 2008 survey by TRUSTe that was repeated in 2009 and a 2009 survey from the Privacy Consulting Group, led by Alan Westin. Both suffer from a number of conceptual and methodological problems which we had to consider when developing our own questions and methods.

TRUSTe’s questionnaire, fielded two years in a row by TNS, asked about behavioral targeting and tailoring in a way that asked respondents whether they agreed or disagreed with a statement about both activities that also added the promise of anonymity: “I am comfortable with advertisers using my browsing history to serve me relevant ads, as long as that information cannot be tied to my name or any other personal information.” In response, about 57% said they either strongly agreed (18%) or agreed (39%). The Westin study, conducted by Harris Interactive online, also posed a standalone question about how “comfortable” people felt with behavioral targeting and tailoring: “As you may know, websites like Google, Yahoo! And Microsoft (MSN) are able to provide free search engines or free e-mail accounts because of the income they receive from advertisers trying to reach users on their websites. How comfortable are you when those websites use information about your online activity to tailor advertisements or content to your hobbies or interests?” Westin found that 59% said they were uncomfortable, with younger people (18-24 and 25-29) having lower percentages than older people—though still over 50%. Westin then asked people to assume that “websites” adopted four stringent privacy and security policies (explaining how the tailoring process would work, offering choices of tailoring, safeguarding information, and promising not to share any user’s name or address) and found that now most people apart from those 63+ were “comfortable” with behavioral targeting and tailoring. Still, the percentages “not comfortable” despite these stringent standards were substantial—38% for 18-31 year olds, 44% for 32-43 year olds, 48% for 44-62 year olds and 54% for those 63+.

Both surveys have the major limitation of being online investigations in which people responded to ads to partake in the companies’ research. The survey firms acknowledge that the sample is not representative and no confidence levels can be presented. The particular nature of the topic of this survey makes the findings particularly suspect. One might worry that people who volunteer to participate would feel less concerned about companies using their data online than would a representative sample of adults who use the internet but would not volunteer for an online survey. Another drawback to emphasize is that both these surveys combined two ideas into one question:

the issue of whether sites should serve tailored content and whether the tailoring should be based on a certain kind of tracking. A further problem is that both surveys say nothing about the particular nature of the targeted behavior. Westin's explanation of tracking said "those websites use information about your online activity," while TRUSTe described it as "using my browsing history." Neither is specific about whether the tracking takes place on a particular website or across websites, and neither suggests the possibility that data collected offline might be used to serve tailored ads.

The latter is an increasing activity that is beginning to receive attention from policymakers.

It is also important to know whether Americans consider the very idea of tailored advertising a good idea, irrespective of how data are collected. To justify behavioral targeting, marketers in recent months been insisting that Americans do in fact want tailored ads. Westin's report suggests that people would want tailored advertising if the four FTC self-regulatory policies were observed. The TRUSTe study uses responses to a statement having nothing to do with tailoring—"If given the option, I would choose to only see online ads from online stores and brands that I know and trust"—to conclude that "individuals want their advertising to be more relevant."

Marketing executives who speak to the trade press tend to take for granted that Americans want tailored ads because they are relevant ads. So, for example, a Facebook executive recently noted that "there is nothing controversial" about using member profiles and wall postings to create tailored ads for them. "The controversy," he added "comes in when a user's behavior without their knowledge is tracked across the internet, which is not something we do."¹⁵ The contention underscores the point that tailoring can take place through a variety of methods other than behavioral targeting. It also raises key questions: Do Americans consider tailoring of advertising, discounts or news suited their interests to be a service they appreciate? Separately, do Americans accept behavioral tracking as the means for providing that tailored content?

The Study and the Population

We explored these questions as part of a larger survey of Americans' opinions about and understanding of a variety of online and offline privacy issues. We cast our population net broadly. We included people in our study if they were 18 years or older said yes to one of the following questions: "Do you go on online or use the internet, at least occasionally?" and "Do you send or receive email, at least occasionally?"

The survey questions we included in this report focus on four areas. One explores Americans opinions about tailored content and three different forms of behavioral tracking. A second investigates people's knowledge of rules of the marketplace when it comes to sharing information in the online and the offline world. A third area of questions asks Americans their opinions about laws that might associate with the tracking their information as well as misusing their information. And a fourth area inquires into people's beliefs about their control over their personal information, whether businesses "handle the personal information they collect about consumers in a proper and

confidential way” and whether they believe “existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.”

The survey was conducted from June 18 to July 2, 2009 by Princeton Survey Research Associates International. PSRA conducted telephone interviews with a nationally representative, English-speaking sample of 1,000 adult internet users living in the continental United States. A combination of landline ($n=725$) and wireless ($n=275$) random digit dial (RDD) samples was used to represent all adults in the continental United States who have access to either a landline or cellular telephone. The interviews averaged 20 minutes. Based on a 7-callback procedure and using the American Association of Public Opinion research (AAPOR) RR3 method, a standard for this type of survey, the overall response rates were a rather typical 18 percent for the landline sample and 22 percent for the cellular sample. Statistical results are weighted to correct known demographic discrepancies.* The margin of sampling error for the complete set of weighted data is ± 3.6 percent at the 95% confidence level. The margin of error is higher for smaller subgroups within the sample.

Table 1 provides an introductory snapshot of the population we interviewed. As Table 1 indicates, women slightly outnumber men; 78% designate themselves as White; 9% identify themselves as blacks or African American; Asian Americans make up 4%; and Native Americans comprise about 1%. Hispanics (white and black) comprise about 11% of the sample. About 56% are under age 45 and 53% are married. Most have at least some higher education, and 33% report over \$75,000 household income while 21% list it as below \$30,000; 10% refused to reveal their household income.

Rejecting Tailored Content and Behavioral Tracking

The telephone interviewer asked all these people the following questions in a randomly rotated manner:

- Please tell me whether or not you want the websites you visit to show you ads that are tailored to your interests

* A two-stage procedure was used to weight this dual-frame sample. A first-stage weight was applied to account for the overlapping sample frames. The first stage weight balanced the phone use distribution of the entire sample to match population parameters. The phone use parameter was derived from an analysis of the most recently available National Health Interview Survey (NHIS) data along with data from recent dual-frame surveys. (See Blumberg SJ, Luke JV, “Wireless substitution: Early release of estimates from the National Health Interview Survey, July–December, 2008.” National Center for Health Statistics. May 2009.) This adjustment ensures that the dual- users are appropriately divided between the landline and cell sample frames.

The second stage of weighting balanced total sample demographics to population parameters. The total sample was balanced to match national population parameters for sex, age, education, race, Hispanic origin, region (U.S. Census definitions), population density, and telephone usage. The basic weighting parameters came from a special analysis of the Census Bureau’s 2008 Annual Social and Economic Supplement (ASEC) that included all households in the continental United States. The population density parameter was derived from Census 2000 data. The telephone usage parameter came from the analysis of NHIS data.

Table 1: Characteristics of U.S. Adults in Sample (N=1,000)*

	%
Sex	
Male	48
Female	52
Age	
18-24	14
25-34	21
35-49	30
50-64	26
65-89	9
Race	
White	78
Black or African American	9
Asian or Pacific Islander	4
American Indian or Alaskan Native	1
Mixed Race	2
Other/Don't Know/Refused	6
Hispanic or Latino Background?	
Yes	11
No	88
Don't Know/Refused	1
Household Income	
Under \$30,000	21
\$30,000 to under \$50,000	19
\$50,000 to under \$75,000	17
\$75,000 and Over	33
Don't Know/Refused	10
Region of the Country	
Northeast	19
Midwest	22
South	33
West	26

*When the numbers don't add to 100% it is because of a rounding error.

- Please tell me whether or not you want the websites you visit to give you discounts that are tailored to your interests.
- Please tell me whether or not you want the websites you visit to show you news that is tailored to your interests.

If a subject answered “yes” to any of the above questions about ads, discounts, and news, its corresponding question below was then asked:

- Would it be OK or not OK if these ads [discounts/news] were tailored for you based on following what you do on the website you are visiting?
- Would it be OK or not OK if these ads [discounts/news] were tailored for you based on following what you do on OTHER websites you have visited?
- Would it be OK or not OK if these ads [discounts/news] were tailored for you based on following what you do OFFLINE—for example, in stores?

The interviewer also asked a general question about the acceptability of behavioral tracking for the purpose of tailored ads if the tracking is anonymous. The lead-up to the question noted that marketers “often use technologies to follow the websites you visit and the content you look at in order to better customize ads.” The interviewer then asked whether the respondent would “definitely allow, probably allow, probably NOT allow, or definitely not allow advertisers” to “follow you online in an anonymous way in exchange for free content.”

Tables 2 and 3 present the findings. Table 2 shows that fully 66% of the respondents do not want advertisements tailored for them. The proportions saying no are lower when it comes to tailored discounts and news, but they still represent around half the population—49% and 57% respectively.

Table 3 shows whether people who said yes to tailored ads, discounts or news continued to say they wanted the tailored content when the interviewers told them the three ways that the information to facilitate tailoring would be gathered. Two interesting patterns show up. One is that for each topic—ads, discounts, and news—the increase in the proportion of people saying no was substantially lower when told that the tracking would take place “on the website you are visiting” compared to tracking based on “other websites you have visited” and on “what you do offline—for example, in stores.” Another notable pattern is for advertisements, discounts, and news, around 80% of the respondents reject tailoring either outright or when they learn they will be followed at other websites or offline.

So, for example, 66% of the 1,000 respondents said no to tailored ads before being told about the forms of tracking. When told the tailored advertising would be based on following them on other websites they have visited, 18% *more* of those 1,000 respondents said no to tailored advertising. That means that 84% of the respondents rejected tailored ads outright or when they found out it would

Table 2: Please Tell Me Whether Or Not You Want Websites You Visit to . . . (N=1,000)*

	No, Would Not (%)	Yes, Would (%)	Maybe, DK (%)
Show you <i>ads</i> that are tailored to your interests.	66	32	2
Give you <i>discounts</i> that are tailored to your interests.	49	47	4
Show you <i>news</i> that is tailored to your interests.	57	40	3

*See text for explanation. DK=Don't Know

Table 3: Would It be OK or not OK if . . . (N=1,000)*

	OK (%)	Not OK (%)	Maybe/ DK (%)	Didn't Want Tailoring (%)	Not OK + Didn't Want Tailoring (%)
<i>these ads were tailored for you based on following</i>					
what you do on the website you are visiting.	24	7	3	66	73
what you did on <i>other</i> websites you have visited.	13	18	3	66	84
what you do <i>offline</i> —for example, in stores.	11	20	3	66	86
<i>these discounts were tailored for you based on following</i>					
what you do on the website you are visiting.	34	13	4	49	62
what you did on <i>other</i> websites you have visited.	18	29	4	49	78
what you do <i>offline</i> —for example, in stores.	18	29	4	49	78
<i>this news was tailored for you base on following</i>					
what you do on the website you are visiting.	25	14	4	57	71
what you did on <i>other</i> websites you have visited.	14	26	3	57	83
what you do <i>offline</i> —for example, in stores.	12	28	3	57	85

happen through tracking them on other sites. The corresponding numbers for discounts and news are 78% and 83%, respectively.

Assurance of anonymous tracking doesn't seem to lower Americans' concerns about behavioral targeting. They are quite negative when it comes to the general scenario of free content supported by tailored advertising that results from "following the websites you visit and the content you look at" in a manner that keeps them anonymous. 68% definitely would not allow it, and 19% would probably not allow it. 10% would probably allow, and only 2% would definitely do it; 1% say they don't know what they would do.

Differences by Age

Americans' negative response to tailored ads, discounts, and news goes up with age in a statistically significant manner ($\text{Rho} = -.24, -.22$, and $-.12$ respectively). When we divide age into traditional marketing categories, however, we find that only the differences in ads and discounts emerge as statistically significant. Through cruder than the statistically significant correlations, the categorical approach allows us to see sharp variations between familiar social groupings. The spread is most pronounced between young adults and seniors. Specific comparison of these two groups revealed their differences are significant statistically across all three forms of content. As Table 4 shows, 55% of Americans 18 and 24 years old say no to tailored advertising, 37% say no to tailored discounts, and 54% reject tailored news. By contrast, among Americans over 65 the numbers are 82%, 70%, and 68% for ads, discounts, and news.

Note that while younger Americans are more welcoming of tailored content than are older ones, well over half of young adults nevertheless do say no to tailored advertising and news. Moreover, the percentage of young adults saying no to the three forms of tailored content becomes substantially higher when we include those who said yes to tailoring alone but then balked when told that their actions would be tracked in order for tailoring to be implemented. Tables 5-7 display the age breakdowns regarding the respondents who said *Not OK* or *OK* to tailoring and tracking. (We left out the 3% or 4% that answered *maybe*, *it depends*, or *don't know*). As Table 5 indicates, 67% of the 18-24 year old Americans say they do not want tailored advertising when we include those saying it is not OK to tailor for them based on what they do on the website they are visiting. 86% of 18-24 year olds say they don't want tailored ads when we include those saying it is not OK to tailor for them based on tracking on "other websites" they have visited. The rejection of tailored content goes up to 90% when what they do "offline—for example, in stores"—is the behavioral-tracking method.

Tables 6 and 7 show that the percentages of young adults saying no to tailored discounts and news are also quite high when we take into account those who say no to the types of behavioral-tracking. Looking across all the age groups, we see that not all the differences between them are significant statistically. Nevertheless, three broad patterns do emerge:

Table 4: Please Tell Me Whether Or Not You Want Websites You Visit to Show You Ads/Discounts/News That Are Tailored To Your Interests.*

	Age 18-24	Age 25-34	Age 35-49	Age 50-64	Age 65-89	Total
Tailored Ads*						
No	55	59	67	77	82	66
Yes	45	41	33	23	18	34
Tailored Discounts*						
No	37	44	50	58	70	51
Yes	64	56	50	42	30	49
Tailored News						
No	54	52	57	62	68	58
Yes	46	48	43	38	32	42

* Using the Chi² statistic, the differences are significant at the .05 level. The table excludes the small percentages that said *Don't Know* or *Maybe*. See text for further explanation.

Table 5: Saying *Not OK* or *OK* to Ads Tailored Based on Age and Three Tracking Activities[§]

.. based on	Age 18-24	Age 25-34	Age 35-49	Age 50-64	Age 65-89	Total
“the website you are visiting”**						
Not OK	67	70	72	82	87	75
OK	33	30	27	18	13	25
“other websites you have visited”						
Not OK	86	82	86	91	95	87
OK	14	18	14	9	5	13
“what you do offline—for example, in stores.”						
Not OK	90	88	86	92	95	89
Not OK	10	12	14	8	5	11

[§]Not OK includes those who said no to tailored advertising at the outset. The table excludes the small percentages that said *Don't Know* or *Maybe*. See text for further explanation. *Using the Chi² statistic, the differences are significant at the .05 level.

Table 6: Saying *OK* or *Not OK* to Discounts Tailored Based on Age and Three Tracking Activities[§]

..based on -	Age 18-24	Age 25-34	Age 35-49	Age 50-64	Age 65-89	Total
“the website you are visiting”*						
Not OK	61	58	62	74	81	66
OK	39	42	38	26	19	34
“other websites you have visited”*						
Not OK	77	76	80	86	90	81
OK	23	24	20	14	10	19
“what you do <i>offline</i> — for example, in stores.”*						
Not OK	74	80	80	86	91	82
OK	26	20	20	14	9	18

Table 7: Saying *OK* or *Not OK* to News Tailored Based on Age and Certain Tracking Activities[§]

..based on -	Age 18-24	Age 25-34	Age 35-49	Age 50-64	Age 65-89	Total
“the website you are visiting”						
Not OK	68	73	72	77	85	74
“what you do <i>offline</i> — for example, in stores.”						
Not OK	79	82	85	90	94	85
OK	21	18	15	10	6	15
Not OK	84	85	85	91	96	87
OK	16	15	15	9	4	13

[§] In Tables 6 and 7, *Not OK* includes those who said no to tailored advertising at the outset. The table excludes the small percentages that said *Don't Know* or *Maybe*. See text for further explanation. *Using the Chi² statistic, the differences are significant at the .05 level.

- In the tables where the comparisons are statistically significant, older groups of Americans reject tailoring and the forms of behavioral tracking in higher percentages than do groups of younger Americans.
- All age groups have somewhat more tolerance for tailoring and behavioral tracking when carried out for discounts than when carried out for advertisements and news.
- Every age group has somewhat more tolerance for behavioral tracking when carried out on the website they are visiting compared to when carried out on other websites or offline, as in stores.

These interesting distinctions should not let us lose sight of the overarching finding: *When we combine Americans who reject tailored content outright with those who said they would want it but changed their minds when told of one or another form of tracking that would yield the tailored content, we find that substantially over 60% of all groups—and often over 80%—say no to the activity.* That includes the younger Americans who marketing executives have asserted don’t care about being tracked as long as they can get relevant content.

Attitudes Toward Tailored Ads By Privacy Experience, Institutional Confidence, And Privacy Knowledge

Because of current policy interests in advertising-related behavioral targeting, we sought to understand whether Americans’ acceptance or rejection of toward tailored advertising related to three aspects of their lives—bad experiences they might have had with information theft, their confidence in the way businesses and the law handle their information, and their knowledge of laws that relate to whether or not firms can sell their information in the online and offline worlds. We defined “bad privacy experiences” as ever having had one or more of the following happen: someone “used or revealed personal information about you without your permission” (it happened to 39%), someone “made a purchase on your credit card or opened a new credit card in your name without your permission” (that happed to 28%), and you “receive a notice in your postal mail that your personal information has been lost or stolen—for example, in a security breach” (it happened to 31%). We defined confidence in business and law through three statements noted in Table 8 that are borrowed from privacy researcher Alan Westin.¹⁶ And we defined online and offline knowledge via the true-false questions in Table 8.

Each of these areas in itself provides an important insight into Americans’ relation to their personal information. Further analysis of the answers revealed that 38% of Americans have never had one of the bad privacy experiences noted, 32% have had one experience, 21% have had two, and 9% have had all three. We also found that 47% of our respondents agree and 20% agree strongly that “consumers have lost all control over how personal information is collected and used by consumers.” Despite these bad experiences and a belief that they have no control over their personal information, Americans have confidence that businesses and laws do protect them: 53% of our respondents agreed and 5% agreed strongly that “most businesses handle the personal

information they collect about consumers in a proper or confidential way.” Most also express confidence in “laws and organizational practices,” with 50% agreeing and 4% agreeing strongly that they “provide a reasonable level of protection for consumer privacy today.”

Part of the reason that majorities believe that businesses or laws protect them may well be because Americans mistakenly assume that laws do not allow businesses to sell personal information . Table 9 shows that, in fact, a substantial majority does not know the correct answers to most true-false statements about companies’ rights to share and sell information about them online and off. Further analysis revealed that individual respondents on average answered only 1.5 of the 5 online statements and 1.7 of the 4 offline statements correctly.

The score on the online or offline privacy indexes—that is, knowledge a person has about privacy law—has no statistical relationship with whether or not a person will agree to tailored ads. Likewise, having one or more bad privacy experiences does not associate with being for or against receiving tailored ads. By contrast, beliefs about personal control and social protection do make a difference, as Table 10 indicates: Agreeing that consumers have lost all control over personal information is significantly associated with not wanting tailored advertising. And having confidence that companies and existing laws protect people increases the statistical likelihood that that a person will want tailored advertising.

Asserting Rights Around Behavioral Tracking

Shifting attention from tailored content to behavioral tracking of people online and off, Table 11 presents the responses to five questions about an individual’s opinions about laws that ought to apply to firms’ behavioral tracking. Large majorities share the same views:

- 69% feel there should be a law that gives people the right to know everything that a website knows about them.
- 92% believe there should be a law that requires “websites and advertising companies to delete all stored information about an individual, if requested to do so.”
- 63% believe advertisers should be required by law to immediately delete information about their internet activity.
- 70% stated that a company should be fined more than the maximum amount suggested (\$2,500) “if a company purchases or uses someone’s information illegally.”

The responses about the maximum fine suggested a level of indignation, even anger, by the public when it comes to misusing information. More evidence of this reaction can be seen in the belief by 18% that a company that uses a person’s information illegally should “be put out of business” and the additional 35% who agree that “executives who are responsible should face jail time.” (See Table 12.)

Table 8: Americans' confidence in the way businesses and the law handle their information
(N=1,000)

	Strongly Agree (%)	Agree (%)	Disagree (%)	Strongly Disagree (%)	DK (%)
Consumers have lost all control over how personal information is collected and used by companies.	20	47	27	4	2
Most businesses handle the personal information they collect about consumers in a proper and confidential way.	5	53	32	6	4
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	4	50	34	8	4

DK=Don't Know

Table 9: Americans' Knowledge of Laws Online and Offline* (N=1,000)

Online:	False* (%)	True (%)	DK (%)
If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission.	22	62	16
If a website has a privacy policy, it means that the site cannot give your address and purchase history to the government.	46	26	28
If a website has a privacy policy, it means that the website must delete information it has about you, such as name and address, if you request them to do so.	20	54	26
If a website violates its privacy policy, it means that you have the right to sue the website for violating it.	19	46	35
If a company wants to follow your internet use across multiple sites on the internet, it must first obtain your permission.	48	33	19
Offline:			
When you subscribe to a newspaper or magazine by mail or phone, the publisher is not allowed to sell your address and phone number to other companies without your permission.	49	36	15
When you order a pizza by phone for home delivery, the pizza company is not allowed to sell your address and phone number to other companies without your permission.	31	44	25
When you enter a sweepstakes contest, the sweepstakes company is not allowed to sell your address or phone number to other companies without your permission.	57	28	15
When you give your phone number to a store cashier, the store is not allowed to sell your address or phone number to other companies without your permission.	33	49	18

*For each statement, *false* is the correct answer.

Table 10: Americans' Desire For Tailored Ads Based on Confidence In The Way Businesses And The Law Handle Their Information

Please tell me whether or not you want websites you visit to show you ads tailored to your interests. ▶	No, would Not (%)	Yes, Would (%)
<hr/>		
Consumers have lost all control over how personal information is collected and used by companies.*		
Agree	71	29
Disagree	60	40
<hr/>		
Most businesses handle the personal information they collect about consumers in a proper and confidential way. *		
Agree	61	39
Disagree	77	23
<hr/>		
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.*		
Agree	61	39
Disagree	76	24

* Using the Chi² statistic, the differences are significant at the .05 level.

Table 11: Asserting Rights Around Behavior Tracking

	N=1,000 (%)
<i>Do you think there should be a law that gives people the right to know everything that a website knows about them, or do you feel such a law is not necessary?</i>	
No, a law is not necessary	29
DK	2
<i>Do you think there should be a law that requires websites and advertising companies to delete all stored information about an individual, if requested to do so?</i>	
Yes, there should be a law	92
No, a law is not necessary	7
DK	1
<i>Advertisers would like to keep and store information about your internet activity. How long should they be able to keep it? Do you think--</i>	
They should have to delete it immediately, OR	63
They should be allowed to keep it for a few months, OR	25
They should be allowed to keep it for a year, OR	6
They should be allowed to keep it for as long as they want	4
DK	2
<i>If a company purchases or uses someone's information illegally, about how much—if anything—do you think that company should be fined?</i>	
\$100	2
\$500	4
\$1,000	9
\$2,500	7
More than \$2,500	70
It depends	4
DK	4
<i>Beyond a fine, companies that use a person's information illegally might be punished in other ways. Which one of the following ways to punish companies do you think is most important?</i>	
The company should fund efforts to help people protect privacy	38
Executives who are responsible should face jail time	35
The company should be put out of business	18
The company should not be published in any of these ways	3
It depends	2
DK	4

DK=Don't Know

Table 12: “Beyond a fine, companies that use a person’s information illegally might be punished in other ways. Which *one* of the following ways to punish companies do you think is most important?”

	N=1,000 (%)
The company should fund efforts to help people protect privacy.	38
Executives who are responsible should face jail time.	35
The company should be put out of business	18
The company should not be punished in any of these ways	3
It depends; don’t know	6

Conclusion

It is noteworthy that 38% of Americans told us that companies that use a person’s information illegally should “fund efforts to help people protect privacy.” While the choice doesn’t suggest the anger of “the company should be put out of business” or “executives who are responsible should face jail time,” it does reflect concern about the state of information privacy that is demonstrated in the answers about tailored content and behavioral tracking. Americans’ widespread rejection of relevant tailored advertising is particularly startling because it flies in the face of marketers’ consistent contention that Americans desire for relevant commercial messages justifies a variety of tracking activities. When three contemporary forms of behavioral tracking are highlighted, rejection of tailored ads is even more widespread. The finding applies across all age groups, including young adults, a cohort that media executives have insisted cares little about information privacy.

The desire by a majority of Americans not to be followed for the purpose of tailored content comes at a time when behavioral targeting is a fast-growing advertising practice upon which many content providers have staked their businesses. A mini-industry is growing up around the process, with companies such as DoubleClick, Audience Science, and Akamai following the activities of individuals in ways that yield detailed suggestions about what kinds of people they are, what that means for their perspectives on life, how that has translated into what they bought recently, and how that might transfer into the products and services they might buy in the near future. At this point the sketches are often not connected to a person’s “offline” or real name and postal address. However, a political consensus is emerging that this point hardly matters when the person’s digital trail is a treasure trove of data that marketers can use to de facto identify the individual across the internet, drawing inferences about personality, gender, location, interests, purchasing power, and more.

Our research did not inquire into why Americans do not want companies to tailor relevant advertising, discounts, or news for them. We can suggest, however, that many of them understand that behavioral targeting can lead to hidden forms of social discrimination. Many may be

uncomfortable with the realization that tailored content and tracking go hand-in-hand. They may know that these activities can lead marketers to retail policies that place them at a disadvantage compared to other consumers. They may fear receiving tailored ads for products that are not as upscale and tailored discounts that are not as generous as the ones their neighbors get. They may worry, too, that news served to them based on criteria they don't understand may separate them from views of the world received by others whom marketers judge differently.

Whatever the reasons explaining Americans' dislike of behavioral targeting, our findings indicate that they expect companies to take privacy rules extremely seriously. Our results show that Americans consumers believe (albeit mistakenly) that an array of strong laws prohibit companies from sharing or selling of data about them. Recall, too, that 70% went beyond the highest option we provided for fines resulting from illegal use of people's data, and that a substantial proportion wanted significant non-monetary sanctions, including liquidation of companies and jail time for employees. Moreover, when asked whether or not they want regulations demanding control and transparency, they say "Yes" in large proportions. 63% prefer immediate deletion of data marketers hold about them, and 25% choose the next most restrictive option—"a few months." 92% percent want a law requiring websites and advertising companies to delete all stored information upon request. While data-intensive companies have resisted calls to reduce data retention and have grudgingly accepted shorter retention times, Americans want them to go farther.

Such a strong preference for a right to delete means that consumers want a way to meaningfully object and withdraw from certain practices around the collection and use of their data. This response is not possible today short of engaging in some very disciplined internet browsing habits or refusing to use the internet at all. And even if they do opt out, their actions are still tracked, and data about their internet use can still be collected. Moving forward, policymakers must be savvy to similar self-regulatory proposals that create illusory protections. There is a real risk that future industry proposals will use technical means to ensure continued website ("first party") and cross-website or even cross-media ("third party") tracking while leading the consumer to believe that such tracking has been limited--for example, by masking third-party tracking to imply it is carried out by the first party.

This survey's findings support the proposition that consumers should have a substantive right to reject behavioral targeting and its underlying practices. Rejection could take the form of a reinvigorated opt out right that actually pertains to collection of information. It could also be implemented through a procedure to enforce an option to delete records. In fact, default rules creating opt in and opt out may be less important than time limits for keeping data. While some accommodations may need to be made for keeping data for security reasons, firms should not be able to use data for marketing purposes for periods longer than those consumers want.

In recent months, a variety of suggestions have been made in this direction by industry and advocacy groups.¹⁷ Our survey findings indicate that the most persuasive of these approaches

encourage transparency and retention limits in marketers' actions and consumers' ability to exercise control over the data companies collect about them. To these important suggestions, we would like to add a broad operating value: Companies need to *respect* their publics rather than to treat them as objects from which they can take information in order to optimally persuade them with no clear option not to participate. Traditionally the potential for harm and unwanted intrusion have been cited as justifications for protecting the privacy of people's information. Respect ought to be encouraged as a positive, trust-building reason for protecting information privacy. Respect as a value requires marketers to promote information reciprocity. That is, in return for collecting and using consumers' data, marketers should allow those consumers to learn exactly where the information came from and how it is being used. Marketers should also allow consumers to decide which of the collected data should be used and for what purposes, and which should be deleted.

Joseph Turow has suggested that marketers create a privacy dashboard that would allow consumers to interact with data the firms have collected about them.¹⁸ Beyond informing people about the information circulating about them, their interaction with data through these dashboards will do more to make the public savvy about their information and how to protect it than will wordy paragraphs and lengthy privacy policies on websites. Implementing a regime of respect around the collection and use of consumer information will not be easy. Our findings in this survey suggest, however, that such activities are imperative for a public that broadly dislikes the emerging contemporary data-gathering regime.

REFERENCES

¹ Audience Science Press Release, "AudienceScience Behaviorally Targets Video Advertising With Hulu," *Marketwire*, July 14, 2009, via Lexis Nexis.

² Ashkan Soltani et al., "Flash Cookies and Privacy," University of California School of Information, 2009, http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1446862

³ See http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html

⁴ NAI, "FAQs," http://www.networkadvertising.org/managing/faqs.asp#question_11, accessed August 31, 2007.

⁵ Federal Trade Commission, "Self-Regulatory Principles for Online Behavioral Advertising," February 2009.

⁶ See Holly Sanders Ware, "Google Is Faulted On Privacy," *New York Post*, July 10, 2009, p. 37.

⁷ Ryan Singel, "You Deleted Your Cookies? Think Again," *Wired*, August 10, 2009.

⁸ Collin O'Malley, VP of Strategic Business at TRUSTe, in TRUSTe press release, "Behavioral Targeting: Not that Bad?!" *Marketwire*, March 4, 2009, via Lexis Nexis.

⁹ Louise Story, "Bits" New York Times, November 5, 2007, p. C-6.

¹⁰ Noelle McElhatton, Noelle McElhatton, Marketing Direct, July 27, 2009,
<http://www.marketingdirectmag.co.uk/channel/directmarketing/article/922859/Disney-CEO-says-young-consumers-dont-care-behavioural-targeting-privacy/>, accessed September 3, 2009.

¹¹ Mark Wilmot, "The Welcome Mat," *Marketing Daily*, July 28, 2009,
http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=110489

¹² Audience Science Press Release, "AudienceScience Behaviorally Targets Video Advertising With Hulu," *Marketwire*, July 14, 2009, via Lexis Nexis.

¹³ Google, "Make the Ads You See More Interesting," accessed on August 31, 2009.

¹⁴ National Advertising Initiative, "Opt Out of Behavioral Advertising,"
http://www.networkadvertising.org/managing/opt_out.asp accessed August 31, 2009. Emphasis in original.

¹⁵ Mediapost, August 14, 2009

¹⁶ See Ponnurangam Kumaraguru and Lorrie Faith Cantor, "Privacy Indexes: A Survey of Westin's Studies," Carnegie Mellon University (CMU-ISRI-5-138), December 2005.

¹⁷ See, for example, "Online Behavioral Tracking and Targeting, Legislative Primer," produced by the Center for Digital Democracy, Consumer Federation of America, Consumers Union, Consumer Watchdog, Electronic Frontier Foundation, Privacy Lives, Privacy Rights Clearinghouse, Privacy Times, U.S. Public Interest Research Group, and World Privacy Forum, September 2009; and Arnold and Porter, LLP, "The Great Behavioral Advertising (BA) Debate Continues," *Consumer Advertising Law Blog*, Sept 17, 2009, <http://www.consumeradvertisinglawblog.com/2009/09/the-great-ba-debate-continues.html>

¹⁸ See Saul Hansell, "An Icon That Says They're Watching You," New York Times, March 19, 2009,
<http://bits.blogs.nytimes.com/2009/03/19/an-icon-that-says-theyre-watching-you/>

HOW DIFFERENT ARE YOUNG ADULTS FROM OLDER ADULTS WHEN IT COMES TO INFORMATION PRIVACY ATTITUDES & POLICIES?

APRIL 14, 2010

"WE SUGGEST...THAT YOUNG-ADULT AMERICANS HAVE AN ASPIRATION FOR INCREASED PRIVACY EVEN WHILE THEY PARTICIPATE IN AN ONLINE REALITY THAT IS OPTIMIZED TO INCREASE THEIR REVELATION OF PERSONAL DATA." (SEE PAGE 20)

Chris Hoofnagle

UC Berkeley School of Law, Berkeley Center for Law and Technology

Jennifer King

UC Berkeley School of Information

Su Li

UC Berkeley School of Law, Center for the Study of Law and Society

Joseph Turow

Annenberg School for Communication, University of Pennsylvania

Chris Jay Hoofnagle, J.D., is director of the Berkeley Center for Law & Technology's information privacy programs and senior fellow to the Samuelson Law, Technology & Public Policy Clinic. He is an expert in information privacy law. Hoofnagle co-chairs the annual Privacy Law Scholars Conference. He is licensed to practice law in California and Washington, DC.

Jennifer King, MIMS, is a Ph.D. candidate at the UC Berkeley School of Information. Most recently she was a researcher at the Samuelson Law, Technology, and Public Policy Clinic at UC Berkeley's School of Law. Her research areas include information privacy and security, usability and human-computer interaction, video surveillance and other sensor networks. With Chris Hoofnagle, King has published three reports exploring Californians' privacy attitudes, available at SSRN.com.

Su Li, Ph.D., recently joined Berkeley Law as its new Statistician in Empirical Legal Studies. Her research interests include gender and social inequality, economic sociology, social network analysis, and the sociology of education. Li received her Ph.D. in Sociology and a Master's in Mathematical Models for Social Science at Northwestern University. An expert in quantitative methodology, Li was Assistant Professor of Sociology at Wichita State University before joining Berkeley Law.

Joseph Turow, Ph.D., is Robert Lewis Shayon Professor of Communication at the Annenberg School for Communication, University of Pennsylvania. Among his several books are *Niche Envy: Marketing Discrimination in the Digital Age* (MIT Press, 2006) and *Breaking Up America: Advertisers and the New Media World* (U of Chicago Press, 1997). Since 1999 he has conducted national telephone surveys that have moved forward public discourse on digital media, marketing, and privacy. Several can be found at the Annenberg Public Policy Center website, APPCPenn.org.

This survey was supported by the Rose Foundation for Communities and the Environment, Tim Little, Executive Director, under grant 025629-003, Chris Jay Hoofnagle, Principal Investigator; and by The Annenberg School for Communication—Michael Delli Carpini, Dean.

Overview

Media reports teem with stories of young people posting salacious photos online, writing about alcohol-fueled misdeeds on social networking sites, and publicizing other ill-considered escapades that may haunt them in the future. These anecdotes are interpreted as representing a generation-wide shift in attitude toward information privacy. Many commentators therefore claim that young people “are less concerned with maintaining privacy than older people are.”¹ Surprisingly, though, few empirical investigations have explored the privacy attitudes of young adults.² This report is among the first quantitative studies evaluating young adults’ attitudes. It demonstrates that the picture is more nuanced than portrayed in the popular media.

In July 2009, we commissioned a nationally representative telephone survey (landline and cellular) of Americans in order to understand the public’s views of both online and offline privacy issues. Our first report from this effort, *Americans Reject Tailored Advertising and Three Activities that Enable It*,³ released in October 2009, investigated Americans’ comprehension of online tailored advertising and related privacy concerns. In this report, we compare young adults and older adults with respect to attitudes toward online privacy protection, whether they carry out certain privacy-protecting behaviors, their public policy preferences regarding privacy, and their knowledge of information privacy law that might affect them in their everyday lives. We found that expressed attitudes towards privacy by American young adults (aged 18-24) are not nearly as different from those of older adults as many suggest. With important exceptions, large percentages of young adults are in harmony with older Americans when it comes to sensitivity about online privacy and policy suggestions. For example, a large majority of young adults:

¹ Ariel Maislos, chief executive of Pudding Media, quoted in Louise Story, *Company Will Monitor Phone Calls to Tailor Ads*, New York Times, Sept. 24, 2007, available at: <http://www.nytimes.com/2007/09/24/business/media/24adcol.html>.

² Marwick, A., Murgia-Díaz, D., and Palfrey, J. (2010). Youth, Privacy and Reputation Literature Review. Berkman Center for Internet and Society, Harvard University.

³ Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It*, SSRN ELIBRARY (2009), <http://ssrn.com/paper=1478214>.

- Has refused to give information to a business in cases where they felt it was too personal or not necessary;
- Believes anyone who uploads a photo of them to the internet should get their permission first, even if taken in public;
- Believes there should be a law that gives people the right to know all the information websites know about them; and
- Believes there should be a law that requires websites to delete all stored information about an individual.

In view of these findings, why would so many young adults act in social networks and elsewhere online in ways that would seem to offer quite private information to all comers? A number of answers present themselves, including suggestions that people 24 years and younger approach cost-benefit analyses related to risk differently than do individuals older than 24. An important part of the picture, though, must surely be our finding that higher proportions of 18-24 year olds believe incorrectly that the law protects their privacy online and offline more than it actually does. This lack of knowledge in a tempting environment, rather than a cavalier lack of concern regarding privacy, may be an important reason large numbers of them engage with the digital world in a seemingly unconcerned manner.

Background

Popular writings and comments suggest that America's youngest adults do not care about information privacy, particularly online. As evidence, many point to younger internet users' adoption and prolific use of blogs, social network sites, posting of photos, and general documenting and (over)sharing of their life's details online, from the mundane to the intimate, for all the world to consume. "Young adults," exhorted one newspaper article to that segment of its readers, "you might regret that scandalous Facebook posting as you get older."⁴ More broadly, Robert Iger, CEO of Disney, recently commented categorically that "kids don't care" about privacy issues, contending that complaints generally came from much older consumers. Indeed, he said that when

⁴ Roger [no surname], "There is No Privacy," *Virginia Pilot*, April 4, 2009, p. B9.

he talked to his adult children about their online privacy concerns “they can’t figure out what I’m talking about.”⁵

Iger is not alone in making claims about differences between young people—even college students—and older members of the population when it comes to giving out personal information online. Anecdotes abound detailing how college-age students post photos of themselves unclothed and/or drunken, for the entire world—including potential employers—to see. It is not a leap to argue that these actions are hard-wired into young people. One psychological study found that adolescents (aged 13-16) and what they termed “youths” (those aged 18-22) are “more inclined toward risky behavior and risky decision making than are ‘adults’ (those older than 24 years) and that peer influence plays an important role in explaining risky behavior during adolescence.” Their finding was more pronounced among adolescents than among the youths, but differences between youths and adults were striking in willingness to take risks—particularly when group behavior was involved.⁶ Although the authors do not mention social media, the findings are clearly relevant to these situations. There the benefits of looking cool to peers may outweigh concerns about negative consequences, especially if those potential consequences are not likely to happen immediately. A related explanation for risky privacy behavior on social-networking sites is that they encourage users to disclose more and more information over time.

Young people’s use of social media does not in itself mean that they find privacy irrelevant.⁷ Indeed, the Pew Internet & American Life Project found in 2007 that teenagers used a variety of techniques to obscure their real location or personal details on social networking sites.⁸ That study fits with the findings of other researchers, who have

⁵ Gina Keating, “Disney CEO Bullish on Direct Marketing to Consumers,” Reuters, July 23, 2009, <http://www.reuters.com/article/idUSTRE56M0ZY20090723?pageNumber=2&virtualBrandChannel=0>

⁶ Margo Gardner and Laurence Steinberg, “Peer Influence on Risk Taking, Risk Preference, and Risky Decision Making in Adolescence and Adulthood: An Experimental Study,” *Developmental Psychology* 41:4, 625-635. No one 23 or 24 years of age was in the sample.

⁷ Raynes-Goldie, Kate. “Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook” *First Monday* [Online], Volume 15 Number 1 (2 January 2010); Lenhart, Amanda and Madden, Mary. “Teens, Privacy, and Online Social Networks.” Pew Internet & American Life Project, April 18, 2007. Available at: <http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx>; and more generally danah boyd’s excellent bibliography of Social Networking Studies at: <http://www.danah.org/researchBibs/sns.html>.

⁸ Lenhart and Madden, *Id.*

urged the importance of reframing the issue to ask *what dimensions* of privacy younger adults care about.⁹ While differences between young adults and those older than they may be important, other more subtle commonalities may be ignored. In recent years older age groups have rushed to social networking in large numbers with discussions of personal issues and details. A common anecdotal observation is that young adults and adolescents are more likely than their elders to post racy photos or document episodes of untoward behavior. If research shows this distinction is accurate, the question nevertheless remains whether the same, higher, or lower percentages of Americans over 24 years old reveal more subtle but important private information about themselves that might lead to embarrassing and unfortunate incidents, such as identity theft.

In spite of vigorous social concerns and discussions, there does not appear to be research that shows definitively that young adults are fundamentally different from older Americans when it comes to privacy attitudes. Moreover, comparisons of what people of different ages do online must be placed within a context of how they understand the norms and laws of privacy in their society. What, if anything, have they done to protect their privacy? What do they believe about privacy norms when presented with the opportunity to think rationally about them? And what protections do they believe laws afford them when they do present themselves in various online environments? The extent to which Americans of different ages have similar or different answers to these questions will suggest whether they converge on similar policy approaches despite seemingly different decisions in the heat of online activities. That is the topic we chose for this study.

In our earlier report on tailored advertising we compared age groups' responses to three questions that asked, "Please tell me whether or not you want websites you visit to show you *ads* [another question substituted *discounts* and a third *news*] that are tailored to your interests." We found that while young adults' concerns were lower compared to other age categories, substantial proportions nevertheless said they did not want tailoring of ads, discounts, and news (55%, 37%, and 54% respectively). Moreover, the percentages saying no rose to very high levels when the young adults were told that the information required to tailor advertisements would come from following them on the

⁹ See Raynes-Goldie (2010).

website they were visiting (67% said no), on other websites they have visited (86% said no) and what they do offline—for example, in stores (90% said no).¹⁰ The findings led us to believe that these tendencies might apply to young adults’ approaches to privacy in general. We hypothesized a dual dynamic: A smaller percentage of young adults than older adults would evidence privacy concerns, but that percentage would still be large, typically exceeding 50% of young adults. We did find this dynamic at work. But we also noted that differences in privacy attitudes and practices between young adults and older ones were at times so small as to not be statistically significant.

Methods

In 2009, we commissioned a survey on behalf of the Berkeley Center for Law and Technology at the University of California, Berkeley School of Law in order to gauge the American public’s attitudes towards and knowledge of the rules and practices surrounding the collection and use of personal information. In this report, we present a summary of our findings for a subset of our survey questions.¹¹ These questions were part of a survey of Americans’ opinions about and understanding of a variety of online and offline privacy issues. We cast our population net broadly. We included people in our study if they were 18 years or older said yes to one of the following questions: “Do you go on online or use the internet, at least occasionally?” and “Do you send or receive email, at least occasionally?”

The survey was conducted from June 18 to July 2, 2009 by Princeton Survey Research Associates International. PSRA conducted telephone interviews with a nationally representative, English-speaking sample of 1,000 American adults living in the continental United States. A combination of landline (n=725) and wireless (n=275) random digit dial (RDD) samples was used to represent all adults in the continental United States who have access to either a landline or cellular telephone. The interviews averaged 20 minutes. Based on a seven callback procedure and using the American Association of Public Opinion research (AAPOR) RR3 method, a standard for this type of survey, the overall response rates were a typical 18 percent for the landline sample and

¹⁰ *Id.* at Fn. 3.

¹¹ *Id.*

22 percent for the cellular sample. Statistical results are weighted to correct known demographic discrepancies.¹² The margin of sampling error for the complete set of weighted data is ± 3.6 percent at the 95 percent confidence level. The margin of error is higher for smaller subgroups within the sample.

Table 1 presents the characteristics of the sample. For this report, we created cross-tabulations of a subset of our survey questions to compare responses across typical age categories (18-24, 25-34, 35-44, 45-54, 55-64, and 65+). Because some people didn't reveal their age, the total for this study's sample is 975 individuals. We considered chi-square values for each table significant at the level of $p < .05$. When the chi-square tests were significant, we used two sample t-tests to discover whether there are statistically significant differences between the 18-24 year olds and all the older adults (i.e. 18-24 compared to 25-65+). We also used Scheffe post-hoc tests to examine if any two age groups are significantly different from each other (e.g. 18-24 vs. 25-34 or 18-24 vs. 35-44) on each possible answer to the question being asked in the tables. For both t-tests and Scheffe tests¹³ we considered significance to be at the level of $p < .05$.

All tables presented in this paper are based on the weighted sample of the data,

¹² A two-stage procedure was used to weight this dual-frame sample. A first-stage weight was applied to account for the overlapping sample frames. The first stage weight balanced the phone use distribution of the entire sample to match population parameters. The phone use parameter was derived from an analysis of the most recently available National Health Interview Survey (NHIS) data along with data from recent dual-frame surveys. (See Blumberg SJ, Luke JV, "Wireless substitution: Early release of estimates from the National Health Interview Survey, July-December, 2008." National Center for Health Statistics. May 2009.) This adjustment ensures that the dual-users are appropriately divided between the landline and cell sample frames.

The second stage of weighting balanced the total sample demographics to population parameters. The total sample was balanced to match national population parameters for sex, age, education, race, Hispanic origin, region (U.S. Census definitions), population density, and telephone usage. The basic weighting parameters came from a special analysis of the Census Bureau's 2008 Annual Social and Economic Supplement (ASEC) that included all households in the continental United States. The population density parameter was derived from Census 2000 data. The telephone usage parameter came from the analysis of NHIS data.

We conducted all analyses in this report using SPSS on a weighted random sample. Due to the unique way that SPSS handles weight, we applied the standardized weight in all analyses so that the sample was corrected by population proportion but not by population size. That is, the sample size was not inflated to the original population size in our analysis. Using the standardized weight prevents the risk of unduly reducing standard errors in significance tests and thereby prevents the risk of having type I errors in the analysis.

¹³ Since Tables 15 and 16 involve indexed variables, on top of the tests on the comparisons of percentages we conducted additional t-tests and Scheffe tests to compare the means of the created indexed variables. See text for details.

with a valid sample size of 975. However, applying weights causes rounding errors in cross-tabulations, which is the reason that the Ns in all tables, except for Table 11, appear as a number other than 975.

Table 1: Characteristics of U.S. Adults in Sample (N=1,000)*

	%
Sex	
Male	48
Female	52
Age	
18-24	14
25-34	21
35-44	20
45-54	19
55-64	15
65+	8
Refused	3
Race	
White	78
Black or African American	9
Asian or Pacific Islander	4
American Indian or Alaskan Native	1
Mixed Race	2
Other/Don't Know/Refused	6
Hispanic or Latino Background?	
Yes	11
No	88
Don't Know/Refused	1
Household Income	
Under \$30,000	21
\$30,000 to under \$50,000	19
\$50,000 to under \$75,000	17
\$75,000 and Over	33
Don't Know/Refused	10
Region of the Country	
Northeast	19
Midwest	22
South	33
West	26

*When the numbers don't add to 100% it is because of a rounding error.

Findings

The following tables will elaborate on a basic theme: Large percentages of young adults (those 18-24 years) are in harmony with older Americans regarding concerns about online privacy, norms, and policy suggestions. In several cases, there are no statistically significant differences between young adults and older age categories on these topics. For most of the questions we asked, there is a statistically significant difference between the youngest adults and older age categories. However, even in these cases over half of the young adult-respondents did answer in the direction of older adults. There clearly is *social significance* in that large numbers of young adults—in some cases, 80-90 percent—agree with older Americans on issues of information privacy.

Table 2 – Refused to Provide Information

Have you ever refused to give information to a business or a company because you thought it was not really necessary or was too personal?	Total	18-24	25-34	35-44	45-54	55-64	65 +
Yes, have	88%	82%	84%	91%	93%	92%	85%
No, have not	11%	18%	13%	9%	7%	7%	14%
Don't know/refused	1%	0%	3%	0%	0%	1%	1%
Total	974	139	206	197	195	151	86

$\chi^2 = 34.158$, df = 10, $p < .001$

Table 3 – Uploading Where I am Recognizable

Generally speaking, anyone who uploads a photo or video of me to the internet where I am clearly recognizable should first get my permission.	Overall	18-24	25-34	35-44	45-54	55-64	65 +
Strongly agree or Agree	86%	84%	81%	86%	90%	91%	88%
Strongly disagree or Disagree	13%	16%	18%	13%	9%	9%	8%
Don't know/refused	1%	0%	2%	1%	1%	0%	3%
Total	973	140	206	197	195	150	85

$\chi^2 = 22.8$, df = 10, $p < .05$; Differences are significant but not related to young adults vs. older adults. See text.

Table 4 – Right To Know

Do you think there should be a law that gives people the right to know everything that a website knows about them, or do you feel such a law is not necessary?	Overall	18-24	25-34	35-44	45-54	55-64	65 +
<i>Yes, should be a law</i>	68%	62%	68%	73%	71%	64%	69%
<i>No, law is not necessary</i>	30%	35%	31%	24%	28%	31%	30%
<i>Don't know/refused</i>	2%	3%	2%	3%	1%	5%	1%
<i>Total</i>	976	141	206	197	196	150	86

$\chi^2 = 12.3$, df = 10, $p = .27$: Differences not significant

Table 5 – Right To Delete

Do you think there should be a law that requires websites and advertising companies to delete all stored information about an individual, or do you feel such a law is not necessary?	Overall	18-24	25-34	35-44	45-54	55-64	65 +
<i>Yes, should be a law</i>	92%	88%	91%	90%	94%	94%	90%
<i>No, law is not necessary</i>	8%	11%	7%	10%	5%	5%	9%
<i>Don't know/refused</i>	1%	1%	1%	0%	1%	1%	1%
<i>Total</i>	975	139	207	197	195	150	87

$\chi^2 = 10.6$, df = 10, $p = .39$: Differences not significant

These dynamics are visible quite clearly in Tables Two through Five, which report on Americans' sensitivity regarding privacy issues. Large proportions of all age groups have refused to provide information to a business for privacy reasons. They agree or agree strongly with the norm that a person should get permission before posting a photo of someone who is clearly recognizable to the internet, even if that photo was taken in public. They agree that there should be a law that gives people the right to know "everything that a website knows about them." And they agree that there should be a law that requires websites and advertising companies to delete "all stored information" about an individual. In the case of the first issue (see Table Two), a statistically significant lower proportion of 18-24 year olds agrees with these positions, but this proportion of young adults agreeing or agreeing strongly was nevertheless over 80%.¹⁴ With respect to

¹⁴ In Table 2, when comparing the 18-24 year olds to the rest of the sample, the differences in the percentages between the two groups are statistically significant at .05 level according to a two-sample t-test. Interestingly, the Scheffe tests of differences between 18-24 year olds and each of the other groups show no significance at .05 level. With respect to Table 3, although answers to this question are

the other three issues (see Tables Three through Five), the differences between the 18-24 year olds and the other adults are not statistically significant: both young and old alike are in agreement.

Privacy Practices

We also sought to determine whether young adults were different from other adult categories when it came to common privacy-related practices—whether they read privacy policies, how frequently they erase their browser cookies, whether or not they had ever changed their mind about an online purchase because of a privacy or security concern, and how frequently they check their credit report. In the case of reading privacy policies, there are no statistical differences among age groups. As Table 6 shows, about half the adult population, including young adults, says it reads policies often or sometimes. When it comes to erasing cookies (Table 7), 58% of young adults say they erase cookies often or sometimes. Statistical tests beyond the chi-square also indicate that age differences are essentially not statistically significant. The t-test tells us that the only statistically significant finding involves the higher proportion of 18-24 year olds answering “hardly ever” compared to the rest of adults. The Scheffe test finds no significance at all between the answers of young adults and the other age groups when it comes to erasing cookies.

About half of young adults have changed their mind about a purchase because of some privacy concern. Post hoc comparisons of the data in Table 8 show no significant difference between young adults and the rest of the population.

We did find a difference regarding checking credit reports. A substantially lower percentage of 18-24 year olds does that, with statistically significant differences from the other age groups centering on their answers of “about once a year,” and “less often than once a year.” Young adults have a significantly higher proportion of people who answered “never” than the other age groups.¹⁵ This distinction between young adults and the others is understandable because credit reports become relevant to older adults, as they buy homes and use credit cards that are not cosigned by their parents.

significantly related to age, neither Scheffe tests nor t-tests show clear patterns of significance between young adults and the rest of the sample or between the youngest adults and each of the older groups.

¹⁵ The comparison between the 18-24 year olds and the rest of the sample was statistically significant at .05 level according a two sample t-test.

Table 6 – Reading Privacy Policies

Do you read the privacy policies of websites ...	Overall	18-24	25-34	35-44	45-54	55-64	65 +
<i>Often</i>	14%	14%	12%	16%	15%	14%	15%
<i>Sometimes</i>	36%	37%	32%	40%	34%	39%	36%
<i>Hardly ever</i>	32%	31%	32%	28%	37%	32%	27%
<i>Never</i>	18%	16%	24%	16%	13%	14%	22%
<i>Don't know/refused</i>	1%	1%	0%	1%	0%	1%	0%
<i>Total</i>	974	141	207	196	195	149	86

$\chi^2 = 21.9$, df = 20, $p = .349$: Differences not significant

Table 7 – Erasing Cookies

When using the internet, do you erase your cookies ...	Overall	18-24	25-34	35-44	45-54	55-64	65 +
<i>Often</i>	39%	33%	36%	51%	40%	39%	33%
<i>Sometimes</i>	24%	25%	31%	19%	20%	28%	16%
<i>Hardly ever</i>	17%	25%	12%	18%	20%	13%	13%
<i>Never</i>	12%	14%	14%	7%	12%	13%	17%
<i>Not familiar with cookies</i>	6%	4%	3%	3%	5%	7%	17%
<i>Don't know/refused</i>	3%	0%	4%	3%	4%	1%	5%
<i>Total</i>	974	139	206	196	195	150	88

$\chi^2 = 73.7$, df = 25, $p < .001$

Table 8 – Changing Mind About Purchase

Have you ever changed your mind about buying something online because of a privacy or security concern?	Overall	18-24	25-34	35-44	45-54	55-64	65 +
<i>Yes, have</i>	56%	49%	55%	66%	58%	56%	41%
<i>No, have not</i>	38%	44%	39%	29%	38%	39%	47%
<i>Does not shop online</i>	6%	7%	6%	5%	4%	5%	12%
<i>Don't know/refused</i>	0%	0%	0%	1%	1%	1%	0%
<i>Total</i>	974	140	207	196	196	150	85

$\chi^2 = 27.7$, df = 15, $p < .05$

Table 9 – Checked Credit Report

In general, how often do you check your credit report?	Overall	18-24	25-34	35-44	45-54	55-64	65 +
<i>At least once a month</i>	10%	14%	9%	12%	5%	9%	9%
<i>Every few months (quarterly)</i>	18%	13%	19%	17%	17%	22%	17%
<i>About once a year</i>	34%	16%	40%	39%	40%	33%	31%
<i>Less often than once a year</i>	18%	5%	17%	24%	21%	21%	20%
<i>Never</i>	19%	48%	14%	8%	17%	15%	21%
<i>Don't know/refused</i>	1%	4%	1%	1%	1%	1%	1%
<i>Total</i>	972	139	206	197	194	150	86

$\chi^2 = 144.4$, df = 25, $p < .001$

Levels of Concern

The tendencies noted above carry over to levels of privacy concern. We fielded a two-prong question. The first asked the individual whether his or her privacy concern was greater, the same, or less than five years ago; the responses are in Table 10. Answers are significantly associated with age, but the 18-24 group was not significantly different than all older respondents, or any single group. Contributing to the significance in this table is the 65+ group, which is more concerned than the 25-34 year olds ($p < .05$).

The obvious problem with Table 10 is that there is no baseline—we don't know the level of concern at which the person began five years ago. But we pursued the question so we could ask people whose privacy concerns increased to note “the most important reason” for the rise. The responses, in Table 11, reveal no statistically significant association with age or differences between the 18-24 year olds and the other age groups.

Table 10 – Concern About Privacy Issues

Compared to five years ago, would you say you are more concerned about privacy issues on the internet, less concerned, or that you have the same level of concern?	Overall	18-24	25-34	35-44	45-54	55-64	65 +
<i>More concerned</i>	55%	54%	44%	59%	55%	60%	67%
<i>Less concerned</i>	6%	9%	8%	5%	6%	5%	4%
<i>Same level</i>	38%	36%	47%	36%	39%	35%	29%
<i>Don't know/refused</i>	1%	1%	2%	1%	1%	0%	0%
<i>Total</i>	974	140	206	196	196	150	86

$\chi^2 = 26.7$, df = 15, $p < .05$

Table 11 – Concern About Privacy Issues – Most Important Reason

Please tell me which one of the following is the most important reason you are more concerned about privacy issues on the internet than you were five years ago.	Overall	18-24	25-34	35-44	45-54	55-64	65 +
<i>You know more about privacy risks online</i>	48%	42%	59%	41%	51%	47%	46%
<i>You have more to lose if your privacy were violated</i>	30%	32%	23%	29%	29%	32%	39%
<i>You have had an experience that has changed your mind about privacy</i>	17%	22%	13%	23%	15%	17%	12%
<i>Some other reason?</i>	3%	0%	4%	6%	3%	2%	4%
<i>Don't know/refused</i>	2%	4%	0%	2%	2%	2%	0%
<i>Total</i>	532 ¹⁶	74	90	115	107	89	57

$\chi^2 = 23.0$, df = 20, $p = .29$: Differences not significant

Penalties for Information Misuse

One way to judge a person's concern about privacy laws is to ask about the penalties that companies or individuals should pay for breaching them. We asked respondents one question related to the monetary penalties a firm should pay and another regarding what should happen to executives involved in illegal privacy breaches. As seen in Tables 12 and 13, the two tendencies we have seen throughout can be found here. Table 12 shows a clear majority of 18-24 year olds selecting the highest dollar amount of punishment offered (more than \$2,500), though a t-test demonstrates that they were

¹⁶ N is small because only people who answered "more concerned" in the previous question were asked this question.

significantly less likely to choose that amount than the rest of the population ($p < .001$), and more likely to select \$1,000 ($p < .05$).

In Table 13, around half of the sample chose the harshest penalties for the companies or individuals—being put out of business and facing jail time, while a third or more thought the company should fund efforts to protect privacy. Though answers to this question are associated with age, 18-24 year olds differed¹⁷ significantly from all other age groups only in selecting “The company should not be punished in any of those ways” ($p < .01$).

Table 12 – Illegal Use of Personal Information

If a company purchases or uses someone's personal information illegally, about how much—if anything—do you think that company should be fined?	Overall	18-24	25-34	35-44	45-54	55-64	65 +
\$100	2%	3%	3%	1%	1%	1%	2%
\$500	4%	5%	5%	5%	5%	1%	3%
\$1,000	9%	14%	10%	10%	8%	7%	6%
\$2,500	7%	11%	9%	6%	7%	3%	5%
More than \$2,500	69%	54%	63%	68%	76%	79%	77%
<i>It depends</i>	4%	10%	1%	5%	3%	5%	2%
<i>Don't know/refused</i>	4%	3%	8%	5%	1%	5%	5%
<i>Total</i>	979 ¹⁸	141	207	196	196	152	87

$\chi^2 = 70.8$, df = 35, $p < .001$

Table 13 – Punishing Companies for Illegal Uses of Information

Beyond a fine, companies that use a person's information illegally might be punished in other ways. Which ONE of the following ways to punish companies do you think is most important?	Overall	18-24	25-34	35-44	45-54	55-64	65 +
<i>The company should be put out of business</i>	18%	16%	19%	18%	14%	20%	22%
<i>The company should fund efforts to help people protect privacy</i>	38%	33%	46%	33%	43%	36%	31%
<i>Executives who are responsible should face jail time</i>	35%	40%	29%	40%	33%	34%	40%
<i>The company should not be punished in any of those ways</i>	3%	7%	2%	5%	2%	2%	2%
<i>It depends</i>	2%	0%	2%	2%	2%	3%	2%
<i>Don't know/refused</i>	4%	4%	3%	3%	7%	5%	2%
<i>Total</i>	973	139	206	197	195	151	85

$\chi^2 = 39.0$, df = 25, $p < .05$

¹⁷ 18-24 year olds have a higher percentage choosing the no penalty option.

¹⁸ The slightly inconsistent N is caused by rounding errors as explained in the methods section.

Privacy Knowledge

Do the similarities between young adults and other age groups carry over to knowledge of existing privacy laws? In order to explore this question, we gave the respondents a set of true/false statements to evaluate and answer. (See Table 14.) All of the answers are false. Consistently answering *true* reflects a belief that the law protects an individual's online and offline privacy more than it does in these common circumstances. We read the statements in separate clusters relating to online and offline privacy; within these clusters, we read the statements in random order. To simplify presentation of the findings, we created a composite index tallying the number correct for each age group.

Table 14 – Online and Offline Privacy Questions

Online Questions	Answer
If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission.	False
If a website has a privacy policy, it means that the site cannot give your address and purchase history to the government.	False
If a website has a privacy policy, it means that the website must delete information it has about you, such as name and address, if you request them to do so.	False
If a website violates its privacy policy, it means that you have the right to sue the website for violating it.	False
If a company wants to follow your internet use across multiple sites on the internet, it must first obtain your permission.	False
Offline Questions	Answer
When you subscribe to a newspaper or magazine by mail or phone, the publisher is not allowed to sell your address and phone number to other companies without your permission.	False
When you order a pizza by phone for home delivery, the pizza company is not allowed to sell your address and phone number to other companies without your permission.	False
When you enter a sweepstakes contest, the sweepstakes company is not allowed to sell your address or phone number to other companies without your permission.	False
When you give your phone number to a store cashier, the store is not allowed to sell your address or phone number to other companies without your permission.	False

As Table 15 indicates, the savvy that many attribute to younger individuals about the online environment doesn't appear to translate to privacy knowledge. The entire population of adult Americans exhibits a high level of online-privacy illiteracy; 75 percent answered only two or fewer questions correctly, with 30 percent getting none right. But the youngest adults perform the worst on these measures: 88 percent answered

only two or fewer correctly, and 42 percent could answer none correctly. A t-test shows that the difference between the average number correct for 18-24 year olds and the other adults—1.12 correct compared to 1.61 for the others—is statistically significant ($p < .001$). When focusing particularly on how these differences play out between young adults and the particular groups, a Scheffe test reveals that the 18-24 year olds were more likely to get none correct than the 25-34 and 35-44 year olds ($p < .05$ in both cases). Young adults were also less likely to get 3-4 correct than the 35-44 and 55-64 groups ($p < .05$ in both cases). In all of these statistically significant cases, a substantially larger percentage of young adults know less about online privacy regulations.

When it came to our offline privacy knowledge questions, the differences between young adults and the other age groups were even more pronounced. Eighty-eight percent of 18-24 year olds answered two or fewer of our offline questions correctly, compared to 74 percent overall. A t-test showed that 18-24 year olds only answered 0.9 correctly compared to 1.8 for the other groups ($p < .001$). Moreover, Scheffe tests note statistical significance compared to each of the other groups. Young adults were more likely to answer no questions correctly than any other age group; conversely, they were less likely to answer 3-4 questions correctly than any other age group.

Getting these questions right is important because it indicates whether the respondents know that privacy laws protect them in common commercial transactions. We found that while young adults tend to be similar to older adults in attitudes, practices, and policy preferences regarding information privacy, they are quite more likely than older adults to be wrong in judging whether the legal environment protects them.

Table 15 - Online Privacy Knowledge Questions (5 total)

Age Range	0 Correct	1-2 Correct	3-4 Correct	5 Correct
18-24 (N=139)	42%	46%	11%	1%
25-34 (N=206)	25%	58%	16%	2%
35-44 (N=197)	24%	38%	30%	8%
45-54 (N=196)	26%	48%	24%	3%
55-64 (N=150)	39%	32%	28%	1%
65 and Older (N=86)	31%	43%	24%	1%
Overall (N=974)	30%	45%	22%	3%

$\chi^2 = 73.1$, df = 15, $p < .001$

Table 16 - Offline Privacy Knowledge Questions (4 total)

Age Range	0 Correct	1-2 Correct	3-4 Correct
18-24 (N=139)	50%	38%	12%
25-34 (N=206)	34%	37%	29%
35-44 (N=197)	24%	33%	43%
45-54 (N=196)	26%	41%	34%
55-64 (N=150)	26%	32%	42%
65 and Older (N=86)	27%	37%	36%
Overall (N=974)	27%	35%	38%

$\chi^2 = 69.9$, df = 20, $p < .001$

Conclusion

In policy circles, it has become almost a cliché to claim that young people do not care about privacy. Certainly there are many troubling anecdotes surrounding young individuals' use of the internet, and of social networking sites in particular. Nevertheless, we found that in large proportions young adults do care about privacy. The data show that they and older adults are more alike on many privacy topics than they are different. We suggest, then, that young-adult Americans have an aspiration for increased privacy even while they participate in an online reality that is optimized to increase their revelation of personal data.

Public policy agendas should therefore not start with the proposition that young adults do not care about privacy and thus do not need regulations and other safeguards. Rather, policy discussions should acknowledge that the current business environment along with other factors sometimes encourages young adults to release personal data in order to enjoy social inclusion even while in their most rational moments they may espouse more conservative norms. Education may be useful. Although many young adults are exposed to educational programs about the internet, the focus of these programs is on personal safety from online predators and cyberbullying with little emphasis on information security and privacy.¹⁹ Young adults certainly are different from older adults when it comes to knowledge of privacy law. They are more likely to believe that the law protects them both online and off. This lack of knowledge in a tempting environment, rather than a cavalier lack of concern regarding privacy, may be an important reason large numbers of them engage with the digital world in a seemingly unconcerned manner.

But education alone is probably not enough for young adults to reach aspirational levels of privacy. They likely need multiple forms of help from various quarters of society, including perhaps the regulatory arena, to cope with the complex online currents that aim to contradict their best privacy instincts.

¹⁹ "Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force." The Berkman Center for Internet & Society, December 31, 2008. Available at: <http://cyber.law.harvard.edu/pubrelease/isttf/>

Americans Roundly Reject Tailored Political Advertising

**AT A TIME WHEN POLITICAL CAMPAIGNS
ARE EMBRACING IT**

Joseph Turow
Michael X. Delli Carpini
Nora Draper
Rowan Howard-Williams

Joseph Turow, Ph.D., is Robert Lewis Shayon Professor of Communication at the Annenberg School for Communication, University of Pennsylvania. Among his several books are *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth* (Yale University Press, 2011), *Niche Envy: Marketing Discrimination in the Digital Age* (MIT Press, 2006) and *Breaking Up America: Advertisers and the New Media World* (University of Chicago Press, 1997). Since 1999 he has conducted national telephone surveys that have moved forward public discourse on digital media, marketing, and privacy.

Michael X. Delli Carpini, Ph.D., is the Walter H. Annenberg Dean of the Annenberg School for Communication, University of Pennsylvania. His research explores the role of the citizen in American politics, with particular emphasis on the impact of the mass media on public opinion, political knowledge and political participation. He is author of *After Broadcast News: Media Regimes, Democracy, and the New Information Environment* (Cambridge University Press, 2011), *Talking Together: Public Deliberation and Political Participation in America* (University of Chicago Press, 2009), *A New Engagement? Political Participation, Civic Life and the Changing American Citizen* (Oxford University Press, 2006), *What Americans Know about Politics and Why It Matters* (Yale University Press, 1996), and *Stability and Change in American Politics: The Coming of Age of the Generation of the 1960s* (New York University Press, 1986).

Nora Draper is a doctoral student at the Annenberg School for Communication, University of Pennsylvania. Her research interests include the struggle over information control in the digital era with a particular focus on digitally-mediated consumer surveillance.

Rowan Howard-Williams is a doctoral student at the Annenberg School for Communication, University of Pennsylvania. His research interests include how digital media are influencing campaigning and advocacy, particularly as related to environmental issues.

July, 2012

Overview

The 2012 election marks a watershed moment for online advertising. In unprecedented ways, and to an unprecedented extent, campaign organizations across the American political spectrum are using hundreds of pieces of information about individuals' online and offline lives to ensure the "right" people are being targeted with the "right" advertising. Yet, contrary to what marketers claim, the vast majority of adult Americans—86%—do not want political campaigns to tailor advertisements to their interests. Moreover, large majorities of Americans say that if they learn a candidate they support carries out one or another real-life example of tailored political advertising, it will decrease their likelihood of voting for the candidate.

These are two findings from the first nationally representative telephone (wireline and cell phone) survey to explore Americans' opinions about targeting and tailored advertising by political campaigns. *Targeting* refers to the analysis of data about a population to determine who should receive a persuasive message, how, when and for what reasons. *Tailored* advertising refers to shaping a persuasive message for a particular individual based on conclusions the targeting process generated about that person's interests and values. Critics of the new advertising regime have lambasted it for threatening privacy and undermining democratic values. Marketers have defended the practice by insisting it gives Americans what they want: political advertisements and other forms of content that are relevant to their concerns.

We conducted this survey to determine what Americans say. We found that the percentage who do not want "political advertising tailored to your interests" (86%) is far higher than the still-quite-high proportions of the population who reject "ads for products and services that are tailored to your interests" (61%), "news that is tailored to your interests" (56%), and "discounts that are tailored to your interests" (46%). Moreover, we found that the rejection of targeted political ads is unrelated to political-party affiliation or political orientation. It also cuts across gender and age, and it while does vary with race and ethnicity the numbers opposing tailored political advertising are high across the board. The survey uncovered other noteworthy attitudes by Americans toward the targeting and tailoring of political advertising. For example:

- 64% of Americans say their likelihood of voting for a candidate they support would decrease (37% say *decrease a lot*, 27% say *decrease somewhat*) if they learn a candidate's campaign organization buys information about their online activities and their neighbor's online activities—and then sends them different political messages it thinks will appeal to them. [This activity is common during the 2012 election.]
- 70% of adult Americans say their likelihood of voting for a candidate they support would decrease (50% say *decrease a lot*, 22% say *decrease somewhat*) if they learn a candidate's campaign organization uses Facebook to send ads to the friends of a person (Sally in the example) who "likes" the candidate's Facebook page. The ads contain Sally's photo and proclaim her support of the candidate. [This activity, too, is taking place during the 2012 election.]
- 77% of Americans agree (including 35% who agree strongly) that "If I knew a website I visit was sharing information about me with political advertisers, I would not return to the site." [Many sites, independently or through third parties, do share such data.]

- 85% agree (including 47% who agree strongly) that “If I found out that Facebook was sending me ads for political candidates based on my profile information that I had set to private, I would be angry.” [Facebook does do this.]

These findings and others in the following pages represent a national statement of concern. What we have is a major attitudinal tug of war: the public’s emphatic and broad rejection of tailored political ads pulling against political campaigns’ growing adoption of tailored political advertising without disclosing when they are using individuals’ information and how. Our survey shows that in the face of these activities, Americans themselves want information.

- A majority wants to know what political campaigns know about them that lead to a tailored ad, and how they learned it. When asked “If a political campaign sends you an online ad that’s relevant to you, would you want to know what the campaign knows about you that led to the ad, or do you not care?,” 65% say they would want to know. Further, when asked if they “would want to know where the campaign got the information to make it relevant, or do you not care?” 76% say they would want to know.
- A majority also wants political candidates’ websites to ask permission when using their information. 91% of Americans say no when asked if it’s OK for a political candidate’s website to sell information they provide to the site. 63% of them say no even when told that the site’s privacy policy would inform them it was selling the information. But when Americans are given the opportunity to “opt in” every time a candidate’s political website wants to sell information they provided to the site, the percentage who then say no drops to 38% of the entire sample.

It’s hard to escape the conclusion that our survey is tapping into a deep discomfort over behavioral targeting and tailored advertising when it comes to politics. Political campaigning is moving in a direction starkly at odds with what the public believes should take place. At the end of this report we suggest how this divide may in coming decades erode citizens’ beliefs in the authority of elections. We also suggest steps toward lifting the hood on the new world of political marketing in the interest of public discussion regarding Americans’ understanding of their evolving political system and where they would like to see it go.

Background

Political advertisers have long had an interest in targeted advertising and tailored messages. As early as 1892 Republican National Committee chairman James Clarkson boasted that he had “with two years of hard work, secured a list of the names of all the voters in all the important States of the North, in 20 or more states, and lists with the age, occupation, nativity, residence and all other facts of each voters’ life, and had them arranged alphabetically, so that literature could be sent constantly to each voter directly, dealing with every public question and issue from the standpoint of his personal interest.”¹

The rise of mass media dampened enthusiasm for individual targeting during the first half of the twentieth century. By the early 1960s, though, the introduction of market segmentation to the field of commercial advertising was influencing political marketing. In his 1960 primary campaign, John F. Kennedy collected large amounts of data about the opinions and values of voters, using it to hone his message for different audiences and transform himself from a relative unknown to his party’s eventual nominee.² Political campaigners increasingly turned to pollsters to help identify messages that would resonate with various voter segments. These initiatives drew on the development of psychographic marketing, which relied on a combination of demographic and psychological information to create homogeneous market segments. In the early 2000s, campaigns began to adopt techniques from commercial advertising where individual voter behavior could be predicted through analyzing masses of consumer data. Among the first to use the technique was Mitt Romney in his successful 2002 run for Governor of Massachusetts. Romney’s consultant Alexander Gage deployed a tactic known as *microtargeting*.³ It involved finding and combining information about individuals’ political preferences and consumer habits. These were then added to the Republican Party’s comprehensive database of information on voters. These individuals could then be targeted – usually by the traditional avenues of phone and direct mail – with messages designed to appeal to them.

Tailoring and Targeting in the Digital Era

Far from inventing targeted and tailored advertising techniques, then, organizations involved in political advertising via digital media build on strategies used by political campaigners for decades. The spread of the web and mobile phones during the 2000s has, however, transformed those practices in three key ways. One is a campaign’s unprecedented ability to gather enormous amounts of information about individuals by getting them to register on websites, purchasing information about them, following their activities on the web, and noting the geographical locations of their digital devices—their desktop computers, laptops, tablets, mobile phones, and even gaming consoles. Another game-changer is the ability to create sophisticated computer models that use enormous amounts of data to identify the most and least desirable individuals and groups from the standpoint of a particular political campaign strategy. The third is the ability to reach those people via a variety of digital platforms—advertising on websites, ads on Google and Bing search engines, email, social media such as Facebook and Twitter, and more—at the particular moment a campaign believes such pinpointing is useful.⁴

These three sets of practices occur without letting the American public—the citizens who are the targets as well as the source of the information for targeting—know the details. Campaign organizations and political data-management firms buy and trade individuals’ information

regularly. These practices are entirely legal in the United States. In fact, beyond certain areas of health and financial information, few regulations govern the gathering, exchange and use of data about people in the digital realm. The Federal Trade Commission encourages companies that use people's data toward a self-regulatory regime around the principles of notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress.⁵ Political marketers may claim to be exempt from even these weak rules under First Amendment rights, though this has not been tested. Though their work is largely hidden from public view, it has grown in detail and texture even over the last four election cycles. In addition to selecting people by demographic and psychographic characteristics, political campaigns increasingly rely on behavioral targeting—that is, the buying and selling of data about users' online, and offline, activities.⁶ Put simply, advertisers, often in partnership with ad networks, drop data packets called cookies into a user's browser when they enter a website. When that user enters another website that is monitored by the ad network, the network reads its cookie in the user's browser and decides if it wants to serve an ad. This method can be used for market segmentation—to target pregnant women wherever they appear, for example. But campaigns can also use it to go beyond market segmentation to target any *individual* with the "right" product or message at the "right" time – a message that may be different from the one served to her neighbor or friend. Borrowing heavily from the practices of commercial marketers, this strategy allows for the creation of customized campaigns that help create a personalized online experience for each user regardless of where that person travels online.

How Campaigns are using these Techniques

As early as 2008, political organizations used "web behavior" including news articles read, blogs visited or search terms entered to target people likely to be sympathetic to their political messages.⁷ The trade magazine *Campaigns & Elections* outlined how a group of online marketing and analytics companies used a series of targeting techniques to help Senator Harry Reid beat Sharron Angle in 2010.⁸ Reid's campaign organization targeted voters based on what the campaign knew about their demographics and online behavior. It then tailored the message: each voter received an advertisement about Reid's health care plan that was most relevant to that individual. In the 2012 election cycle political-marketing organizations are innovating by combining online and offline data – particularly information found in the voter file – to try to ensure that the "right" people are being targeted with advertising that suits them.

In addition to tracking people's behaviors on and off the web in the interest of tailored communication, campaigns show growing sophistication in their use of social networking sites. For example, Facebook has introduced ZIP-code specific advertising, which may be useful for politicians looking to target advertisers in specific districts.⁹ Microtargeting techniques are used by political campaigns to gather information about individuals from social networking sites – including interests, employment, ethnicity, language and age – and send highly targeted ads to those deemed beneficial by the campaign.¹⁰ Harry Reid's election organization used Facebook to target young people as well as individuals identified as lesbian, gay, bisexual, or transgender through profile information like age and relationship status.¹¹ Campaigns are even able to tap into friendship networks to help build their list of targets.¹²

In addition, many candidates have Facebook pages where they invite voters to "like" them. These pages will send campaign information to those subscribed to the page.¹³ It may not be

clear to those who sign up that they may become stars in targeted, tailored ads. If a candidate pays Facebook, the social networking site will send advertisements called *sponsored stories* to the Facebook friends of people who are fans of the candidate. These tailored ads often include the fan's Facebook photo. They tell those receiving the message that their friend supports the candidate.¹⁴

The 2012 campaign is also seeing an unprecedented role for mobile advertising. Campaigns have for several years encouraged people to sign-up with their mobile phone number to receive text-message updates about the campaign or candidate. Now politicians are able to target advertisements to mobile phones and tablets based on location. Campaigns are reportedly using hyper-local targeted advertisements—those that reach neighborhoods or areas within neighborhoods—to send particular messages to certain types of voters, even certain individual voters, in swing states who might be swayed in the campaigns' direction.¹⁵ New ways of tracking individuals' phones and tablets without cookies (using the devices' electronic identification signals, for example) portend a future ability to identify and follow individuals across devices, space, and time, often without the person's full understanding of what is happening.

Critics Worry Tailored Political Advertising Undermines Privacy and Threatens Democracy

These developments have stirred concern among advocates of a transparent and fair political process. In a February 2012 *Stanford Law Review Online* article Daniel Kreiss, a Journalism professor at the University of North Carolina, Chapel Hill, concisely summarized critics' views about why "the proliferation of political data undermines political privacy and threatens democratic practice." First, there is the risk of data breaches and the unauthorized dissemination of sensitive citizen information. Another concern is that citizens in future years will hesitate to discuss politics in digital venues if they believe their comments are being collected for analysis by and even sale to political marketers. A third concern is that the high cost of political data and related political consulting activities add yet another bar to political races for all but the well-heeled or their good friends. And a fourth issue is the use of data to routinely "redline the electorate, ignoring individuals they model as unlikely to vote, such as unregistered, uneducated, and poor voters."¹⁶ A corollary of this concern is what might be called *rhetorical redlining*: the likelihood that individuals will receive ads from candidates based on what the campaign's statisticians believe they want to hear—shutting them off from messages that the statisticians determined might make them waver in their support.

Responding directly to Kreiss, three Campaign Grid executives argued generally that "relevant online ads support democracy." They contended that "A positive aspect of relevant campaign ads is that the ads are more relevant to the voter receiving them: voters receive ads about issues they are most likely to care about, with easily accessed links to click-through to learn more."¹⁷

Despite growing press discussion in recent months regarding the rise of tailored political advertising, no one has asked the citizens themselves whether they think it's a good idea. A study that comes closest to this topic is a national landline-and-cell-phone survey of 1,000 Americans that one of us (Joseph Turow) conducted in 2009 with researchers at the University of Pennsylvania and Berkeley Law School with the help of Princeton Survey Research Associates

International.¹⁸ The central finding was that contrary to what many marketers claimed: most adult Americans (66%) do not want to receive advertisements “tailored to their interests.” Moreover, when Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages—between 73% and 86%—say they would not want such advertising.

Our central question for this study was whether Americans would express the same disinclination toward tailored *political* advertising. Related questions tumbled out. Would people who oppose political advertising be against it because they dislike online advertising generally or because they dislike tailored political advertising? Are there certain circumstances where Americans support tailored advertising more than other circumstances? Do they believe that such activities are actually occurring (they are)? If they knew a candidate they support uses their information to send them political ads tailored to their interests, would it increase or decrease their likelihood for voting for that candidate? How do these answers vary by Americans’ age, gender, education, and party affiliation?

The Study and Its Population

We explored these questions as part of a larger survey of Americans’ opinions about and understanding of a variety of online privacy issues. We cast our population net broadly. We included people in our study if they were 18 years or older said yes to one of the following questions: “Do you go on online or use the internet, at least occasionally?” and “Do you send or receive email, at least occasionally?”

The survey was conducted from April 23 - May 6, 2012 by Princeton Survey Research Associates International. PSRAI conducted telephone interviews with a nationally representative, English and Spanish speaking sample of 1,503 adult internet users living in the continental United States. The interviews averaged 20 minutes. A combination of landline (N=901) and cellular (N=602, including 279 without a landline phone) random digit dial (RDD) samples was used to represent all adults in the continental United States who have access to either a landline or cellular telephone.

For the landline sample, interviewers asked to speak with the youngest adult male or female currently at home based on a random rotation. If no male/female was available, interviewers asked to speak with the youngest adult of the other gender. This systematic respondent selection technique has been shown to produce samples that closely mirror the population in terms of age and gender when combined with cell interviewing. For the cellular sample, interviews were conducted with the person who answered the phone. Interviewers verified that the person was an adult and in a safe place before administering the survey. Cellular respondents were offered a post-paid cash reimbursement for their participation.

Table 1: Characteristics of U.S. Adults in Sample (N=1,503)*

Sex	
Male	49
Female	51
Age	
18-24	15
25-34	19
35-49	27
50-64	25
65-97	10
Don't Know/Refused	3
Race	
White	75
Black or African American	11
Asian or Pacific Islander	4
American Indian or Alaskan Native	1
Mixed Race	2
Other/Don't Know/Refused	7
Hispanic or Latino Background?	
No	88
Yes, born in US	7
Yes, born outside US	4
Other/Don't Know/Refused	3
Household Income	
Under \$30,00	25
\$30,000 to under \$50,000	17
\$50,000 to under \$75,000	14
\$75,000 to under \$100,000	10
\$100,000 to under \$150,000	10
\$150,000 or more	8
Don't Know/Refused	16
Region of the Country	
Northeast	19
Midwest	22
South	35
West	24
Education	
Less than high school graduate	5
High school graduate	29
Some college/associate degree	29
College graduate	37

*When the numbers don't add to 100%, it is because of rounding error.

Based on a 7-callback procedure and using the American Association of Public Opinion research (AAPOR) method, a standard for this type of survey, the overall response rates were a typical 12 percent for the landline sample and 12 percent for the cellular sample. We note that the cooperation rate for both the landline and cellular samples was 20% and that 92% of the landline and 95% of the cellular respondents completed the interviews once they started.

Statistical results are weighted to correct known demographic discrepancies. The margin of sampling error for the complete set of weighted data is ± 2.8 percent at the 95% confidence level. The margin of error is higher for smaller subgroups within the sample.

Table 1 provides an introductory snapshot of our internet-using population. As the table indicates, women slightly outnumber men; 75% designate themselves as White; 11% identify themselves as blacks or African American; Asian Americans make up 4%; and Native Americans comprise about 1%. Hispanics (white and black) comprise about 11% of the sample. About 61% are under age 49. Most have at least some higher education, and 28% report over \$75,000 household income while 25% list it as below \$30,000; 16% did not want to reveal their household income.

The Findings

Americans Reject Tailored Political Content and Behavioral Tracking

The telephone interviewer asked all these people the following questions:

- Please tell me whether or not you want the websites you visit to show you ads for products and services that are tailored to your interests.
- Please tell me whether or not you want the websites you visit to give you discounts that are tailored to your interests.
- Please tell me whether or not you want the websites you visit to show you news that is tailored to your interests.
- Please tell me whether or not you want the websites you visit to show you political ads that are tailored to your interests.

We had asked the questions about ads, discounts, and news in the 2009 study; the question about political ads is new with this survey. So that the respondent would note the distinction between ads and political ads, we asked the query about “ads for products and services that are tailored to your interest” first. We asked the other questions in a randomly rotated manner.

If a respondent answered “yes” to any of the above questions, we then asked its corresponding question below:

- Would it be OK or not OK if these ads [discounts/news/political ads] were tailored for you based on following what you do on the website you are visiting?

- Would it be OK or not OK if these ads [discounts/news/political ads] were tailored for you based on following what you do on OTHER websites you have visited?
- Would it be OK or not OK if these ads [discounts/news/political ads] were tailored for you based on following what you do OFFLINE—for example, in stores or your magazine subscriptions?

If the person answered yes to wanting “political ads tailored to your interest,” we added two additional questions:

- Would it be OK or not OK if these political ads were tailored for you based on the political party you belong to?
- Would it be OK or not OK if these political ads were tailored for you based on whether you voted in the past two elections?

Tables 2 and 3 present the findings. Table 2 shows that fully 86% of adult Americans do not want political advertisements tailored for them. Three other points stand out. First, the 86% saying no to tailored political ads is especially startling in view of substantially lower (yet still high) percentages who reject ads for products and services (61%), news (56%), and discounts (46%). Second, Americans’ reactions to commercial ads, news, and discounts are not one-time flukes. The percentages saying no to tailoring in this survey are quite similar to those numbers in our 2009 survey. Third, the numbers indicate the population clearly considers political ads to be different from the other categories of tailored content: far more people reject political ads at the outset.

Table 2: Please Tell Me Whether Or Not You Want Websites You Visit to... (N=1,503)*

	No, Would Not (%)	Yes, Would (%)	Maybe/ DK (%)	No, Would Not, in 2009 (%)
Show you ads for products and services that are tailored to your interests.	61	37	2	66 **
Give you discounts that are tailored to your interests.	46	53	1	49
Show you news that is tailored to your interests.	56	42	1	57
Show you political ads that are tailored to your interests.	86	13	1	NA

*See text for explanation. When the numbers don’t add to 100%, it is because of rounding error.

DK=Don’t Know; NA=Not Asked

** In the 2009 survey the phrasing was “Show you ads that are tailored to your interests.” We added *for products and services* this time to make clear the distinction between this question and the one about political ads.

Table 3 shows that the percentages of Americans who reject political ads remain higher than those who reject commercial ads, news, and discounts when the interviewers tell them how the information to facilitate tailoring would be gathered. Two interesting patterns arise. One is that for each topic—political ads, commercial ads, discounts, and news—the increase in the proportion of people saying no is lower when told that the tracking would take place “on the website you are visiting” compared to tracking based on “*other* websites you have visited” and on “what you do *offline*—for example, in stores and magazines.” Another notable pattern is for advertisements, discounts, and news, over 75% of the respondents reject tailoring either outright or when they learn they will be followed at other websites or offline.

So, for example, 61% of the 1,503 respondents said no to tailored ads before being told about the forms of tracking. When told the tailored advertising would be based on following them on other websites they have visited, 22% *more* of those 1,503 respondents said no to tailored advertising. That means that 83% of the respondents rejected tailored ads outright or when they found out it would happen through tracking them on other sites. The corresponding numbers for discounts and news are 76% and 80%, respectively.

Despite the huge proportions of the population saying no to tailored commercial ads, discounts, and news when informed how the tailoring takes place, the proportions of people saying no to tailored political advertising is consistently higher. Table 3 shows what happens when the 14% of Americans who accept tailored political ads at the outset are told of five ways campaigns might gather information about them in order to carry out the practice. Many of those who were OK with the activity initially change their minds, and Americans’ rebuff of tailored political advertising rises to between 89% and 93%.

Americans Note Displeasure over Targeting and Tailoring by Even a Favored Candidate

Americans’ broad unhappiness with the use of data about themselves for political advertising is clear in their responses to scenarios we presented to them of activities that political campaigns actually carry out:

- Scenario 1 focused on targeting: *Let’s say that a political campaign buys information about where you go online and what you buy on the web. The campaign uses this information to draw conclusions about your political beliefs and voting preferences.*
- Scenario 2 highlighted distinctively tailored messages: *Now let’s say a candidate’s campaign organization uses information it has bought about you to send you online political ads with messages it thinks will appeal to you. It sends your neighbors different online ads, based on the information that the campaign bought about THEM.*
- Scenario 3 brought social media into the tailoring activity: *Imagine Sally visits the Facebook page of a political candidate and clicks that she “likes” the page. The campaign organization then pays Facebook to send ads to the Facebook pages of Sally’s friends. The ads contain Sally’s name and photo and proclaim that Sally supports the candidate.*

Table 3: Would it be OK or not OK if (N=1,503)*

	OK (%)	Not OK (%)	Maybe/ DK (%)	Didn't Want Tailoring (%)	Not OK + Didn't Want Tailoring (%)
<i>these political ads were tailored for you based on</i>					
following what you do on the website you are visiting.	11	3	**	86	89
following what you did on other websites you have visited.	8	6	**	86	92
following what you do offline—for example, in stores. . .	7	7	**	86	93
the political party you belong to	10	4	**	86	90
whether or not you voted the in the past two elections	9	5	**	86	91
<i>these ads were tailored for you based on</i>					
following what you do on the website you are visiting.	30	7	2	61	68
following what you did on <i>other</i> websites you have visited.	15	22	1	61	83
following what you do offline—for example, in stores. . .	14	23	2	61	84
<i>these discounts were tailored for you based on</i>					
following what you do on the website you are visiting.	46	7	1	46	53
following what you did on <i>other</i> websites you have visited.	23	30	1	46	76
following what you do offline—for example, in stores. . .	22	31	1	46	77
<i>this news was tailored for you based on</i>					
following what you do on the website when you are visiting.	33	9	1	56	64
following what you did on <i>other</i> websites you have visited.	18	24	1	56	80
following what you do offline—for example, in stores . . .	16	27	1	56	83

*See text for explanation. When the numbers don't add to 100%, it is because of rounding error.

DK=Don't Know

We did not tell the people we interviewed that the scenarios are realistic. Instead, for each one we asked them whether knowing that a candidate *that they supported* was using online information in that way would affect how they voted for the candidate. Table 4 presents the findings. It shows that learning of these targeting activities does not sway everyone from the candidate he or she supports; between 25% and 34% of respondents say it would neither increase nor decrease the likelihood of voting for that person. Nevertheless, between 57% and 70% of Americans do say it would decrease the likelihood of voting for their candidate either a lot or somewhat. And very few people say it would increase their desire to vote for someone engaged in these sorts of political targeting.

The targeting activity that the highest percentage of respondents say would decrease their likelihood of voting for a candidate they support is the one that obviously involves tailored advertising in a social media context: a campaign's use of information about a political supporter to tailor a Facebook ad for that supporter's friend. Fully half of our respondents answered *decrease a lot* when told of a candidate who sends Facebook ads to Sally's friends with Sally's photo and a proclamation of Sally's support for the candidate. When asked if they thought "any candidates have used Facebook information in this way," 70% of our respondents said yes (10% said no, and 20% said they were unsure).

Clearly, people's decision to vote for candidates they initially support relates to various factors. We do not see these responses as necessarily predictive of ballot behavior. Rather, we see them as part of a pattern of answers in this survey that reflects the Americans' displeasure regarding the process of political targeting and tailored communication based on the targeting. In addition to the scenarios, we have already seen the pattern in the ways people responded to the questions about political ads tailored to their interests. This displeasure is further reflected in responses to three statements we read to our respondents later in the survey. As Table 5 shows, large majorities indicate annoyance and even anger when confronted with examples of data sharing and targeting for political purposes. Fully 85%, for example, agree or agree strongly that they would be angry if they found out Facebook was sending them ads for political candidate based on profile information they had set to private.

We asked about the particular situations in Tables 4 and 5 because political marketers actually carry them out. Americans, for their part, seem to realize the activities are not hypothetical. Answers to a number of questions we posed suggest many Americans know these activities are taking place. We asked the people in our sample, for example, if they think any candidates have used information in the ways described in the three scenarios. A large majority of our respondents said yes--75% regarding the first scenario (9% said no, 15% unsure), 77% for the second one (8% said no, 15% unsure), and 70% with respect to the third (10% said no, and 20% said they were unsure). Later in the interview we asked "Do you think political marketers have the technical ability to combine facts about what you do online and offline in order to tailor political ads for you?" Similar to the previous answers, 70% believe this rather high level of sophistication is possible; 24% say no, and 6% don't know.

Table 4: The Three Scenarios (N=1,503)*

If you knew a candidate that you supported was using online information in this way, how would it affect your likelihood of voting for the candidate? Would your likelihood of voting for that candidate---	Decrease a lot	Decrease Somewhat	Neither increase decrease	Increase Somewhat	Increase a lot	DK/ Ref
Let's say that a political campaign buys information about where you go online and what you buy on the web. The campaign uses this information to draw conclusions about your political beliefs and voting preferences.	33	24	34	3	3	4
Now let's say a candidate's campaign organization uses information it has bought about you to send you online political ads with messages it thinks will appeal to you. It sends your neighbors different online ads, based on the information that the campaign bought about <i>THEM</i> .	37	27	29	2	2	3
Imagine Sally visits the Facebook page of a political candidate and clicks that she "likes" the page. The campaign organization then pays Facebook to send ads to the Facebook pages of Sally's friends. The ads contain Sally's name and photo and proclaim that Sally supports the candidate.	50	20	25	1	2	2

*When the numbers don't add to 100%, it is because of rounding error.

DK=Don't Know; Ref=refused to answer

Table 5: Responses to Statements about Political Targeting (N=1,503)*

I am going to read some statements about political advertising. After I read each one, please tell me if you agree or disagree.	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly Disagree	DK/ Ref
I do NOT mind if an organization tries to figure out my political opinions based on what I read online.	3	24	11	33	28	1
If I knew a website I visit was sharing information about me with political advertisers, I would not return to the site.	35	42	8	11	3	1
If I found out that Facebook was sending me ads for political candidates based on my profile information that I had set to private, I would be angry.	47	38	4	6	3	2
If I give a political campaign my cell phone number, it is OK if that candidate's organization sends me text messages.	7	44	5	21	21	2
If I register my name on a candidate's site but have not given the candidate my cell phone number, it is OK if that candidate's organization finds out what my cell phone number is and sends me text messages.	1	4	3	33	58	1

*When the numbers don't add to 100%, it is because of rounding error.

DK=Don't Know; Ref=refused to answer

Americans Hold Various Objections to Political Targeting and Tailoring

We note in Tables 4 and 5 that more people objected to certain types of data extraction than to others. Taking data from Facebook that respondents consider private yielded the highest resistance at 85%. The somewhat more general notion of a site “sharing information” about the respondent with political advertisers (Table 5) bothers the second-highest percentage of respondents (77%). The notion (in Table 5) that an organization would learn about the respondent based on what the person reads online or (in Table 4) about where people go and what they buy online yields relatively lower levels of objections—61% and 57%, respectively.

Note, too, that substantially more people accept being contacted through phone text message by a political organization if they gave the organization their phone number (51%) than if the organization acquired it elsewhere (5%)—even if they had registered on the organization’s site. We take this variability in answers to mean respondents were judging each situation presented to them separately and not just dismissing the notion of political behavioral targeting out of hand. Still, even the lowest proportion of objections to such targeting is quite large—about one of every two Americans.

Large Percentages of Americans’ Reject Tailored Political Ads No Matter Their Party Affiliation or Political Orientation

As Table 6 indicates, there are no statistically significant differences in the percentages associating lack of desire to receive politically tailored ads with a person’s political-party affiliation. And although the association of tailored ads with political orientation is statistically significant, even the lowest percentage—of those who call themselves very liberal—still rejects it in huge proportions (76%). Moreover, the percentages do not seem to reflect a meaningful pattern.

We find this lack of meaningful connection to party or affiliation across the three scenarios, as well. Sometimes the differences in party identification are statistically significant at the .05 level, using the Chi² statistic, and sometimes political orientation is significant. Nevertheless, the differences are small, and they don’t come together to suggest meaningful association of party affiliation or political orientation with attitudes toward political behavior targeting or tailoring.

Large Percentages of Americans Reject Tailored Political Ads No Matter Their Gender, Age, Education, Race, or Ethnicity.

We also see the rejection of political ads in large percentages irrespective of social segments when we look at key demographic categories. Unlike with party affiliation and political orientation, we note pattered differences as well. Table 7 presents the association of respondents’ gender, age, education, and race/ethnicity with their answer to the direct question about tailored political ads. Tables 8-10 then present the association of the demographics with answers to the three scenarios, which depict different aspects of tailored political advertising.

Table 6: Do Party Affiliation and Political Orientation Predict Americans' Attitudes Toward Tailored Political Ads?*

	No, Would Not Want Tailored Political Ads (%)	Maybe/ Depends (%)	Yes, Would Want Tailored Political Ads (%)
◆ Thinking about your general approach to politics, do you consider yourself a			
Republican (N=335)	84	1	15
Independent (N=562)	86	0	14
Democrat (N=423)	85	1	15
◆◆ In general, would you describe your political views as			
Very conservative (N=98)	81	0	19
Conservative (N=390)	85	1	14
Moderate (N=559)	89	0	11
Liberal (N=243)	86	1	13
Very liberal (N=82)	76	0	24

* Because the table excludes the small percentages that said *Don't Know* or *Maybe*, the N for party affiliation is 1,320 and the N for political orientation is N=1,372. See text for explanation. When the numbers don't add to 100%, it is because of rounding error. 0=Less than 1%. ◆=Using the Chi² statistic, differences are not significant at the .05 level. ◆◆= Using the Chi² statistic, differences are significant at the .05 level.

The tables indicate that differences in age and gender are sometimes significant, sometimes not. When age is significant (Table 7), younger people are somewhat more likely than older people to be OK with tailored political ads. When gender is significant (Table 9 and 10), men are somewhat more likely than women to be OK with tailoring political ads based on purchased information and identifying Facebook friends. While gender and age show only occasional relationships with attitudes towards different aspects of tailored and targeted political advertising, somewhat more consistent patterns show up with education and race/ethnicity. People with the lowest and highest amounts of education tend to reveal a bit less concern about tailored advertising than do people with a high school degree and some college. And larger percentages of *Black Non-Hispanics* reflect less concern with various aspects of politically tailored ads than do other groups, while *Other Non-Hispanics* are typically most likely to express concern.

The reasons for the differences are not obvious, and they ought to be a topic for future research. Here we emphasize that concern with an aspect of tailored or targeted political advertising never falls below 50% for any of the social groupings and is frequently far above that proportion. In fact, the proportions of demographic segments saying no are typically in the 80-90% range with respect to the central question about the desire for tailored political advertising (Table 7).

Table 7: Do Gender, Age, Education, and Race/Ethnicity Predict Americans' Attitudes Toward Tailored Political Ads?*

	No, Would Not Want Tailored Political Ads	Maybe/ Depends (%)	Yes, Would Want Tailored Political Ads (%)
◆ Gender			
Male (N=733)	84	2	16
Female (N=764)	88	1	12
◆◆ Age			
18-29 (N=394)	81	1	19
30-45 (N=433)	86	1	13
46-64 (N=484)	88	1	11
65 and older (N=148)	92	1	7
◆◆ Education			
Less than high school degree (N=76)	67	0	33
High school degree (N=425)	84	1	16
Some college (N=438)	87	1	13
College degree or more (N=549)	90	2	10
◆◆ Race/Ethnicity			
White Non-Hispanic (N=1050)	87	1	12
Black Non-Hispanic (N=143)	78	0	22
Hispanic (N=162)	81	0	19
Other Non-Hispanic (N=95)	90	0	11

* Because the table excludes the small percentages that said *Don't Know* or *Maybe*, the N for gender is 1,497, the N for age is 1,459, the N for education is 1,488, and the N for race/ethnicity is 1,450. See text for explanation. When the numbers don't add to 100%, it is because of rounding error. **2**= Less than 1%.

◆=Using the Chi² statistic, differences are not significant at the .05 level. ◆◆= Using the Chi² statistic, differences are significant at the .05 level or lower.

Table 8: Do Gender, Age, Education, and Race/Ethnicity Predict Americans' Attitudes Toward Online Tracking For Political Reasons?*

	Decrease Some / a Lot (%)	Neither Decrease Nor Decrease (%)	Increase Some / A Lot (%)
Now let's say a candidate's campaign organization uses information it has bought about you to send you online political ads with messages it thinks will appeal to you. It sends your neighbors different online ads, based on the information that the campaign bought about THEM.			
If you knew a candidate that you supported was carrying out these activities, how would it affect your likelihood of voting for the candidate? Would your likelihood of voting for that candidate...			
♦ Gender			
Male (N=718)	64	32	5
Female (N=742)	69	27	4
♦ Age			
18-29 (N=383)	64	31	6
30-45 (N=424)	67	30	3
46-64 (N=474)	67	28	5
65 and older (N=144)	69	30	1
♦♦ Education			
Less than high school degree (N=69)	68	17	15
High school degree (N=412)	69	24	7
Some college (N=431)	71	27	2
College degree or more (N=539)	61	37	2
♦♦Race/Ethnicity			
White Non-Hispanic (N=1026)	69	29	3
Black Non-Hispanic (N=142)	54	32	14
Hispanic (N=160)	65	28	7
Other Non-Hispanic (N=93)	65	31	4

* Because the table excludes the small percentages that said *Don't Know* or *Maybe*, the N for gender is 1,460, the N for age is 1,425, the N for education is 1,451, and the N for race/ethnicity is 1,421. See text for explanation. When the numbers don't add to 100%, it is because of rounding error. ♦=Less than 1%.

♦=Using the Chi² statistic, differences are not significant at the .05 level. ♦♦= Using the Chi² statistic, differences are significant at the .05 level or lower.

Table 9: Do Gender, Age, Education, and Race/Ethnicity Predict Americans' Attitudes Toward Tailoring Different Political Ads Based on the Purchase of Personal Data? (N=1,503)*

	Decrease Some / a Lot (%)	Neither Decrease Nor Decrease (%)	Increase Some / A Lot (%)
Let's say that a political campaign buys information about where you go online and what you buy on the web. The campaign uses this information to draw conclusions about your political beliefs and voting preferences.			
If you knew a candidate that you supported was using online information in this way, how would it affect your likelihood of voting for the candidate? Would your likelihood of voting for that candidate...			
♦♦ Gender			
Male (N=715)	56	36	8
Female (N=733)	62	34	4
♦Age			
18-29 (N=381)	56	38	6
Less than high school degree (N=67)	57	25	18
High school degree (N=408)	63	28	9
Some college (N=425)	62	35	4
College degree or more (N=542)	54	42	4
♦♦Race/Ethnicity			
White Non-Hispanic (N=1017)	60	37	4
Black Non-Hispanic (N=139)	52	35	14
Hispanic (N=158)	59	27	14
Other Non-Hispanic (N=92)	66	28	5

* Because the table excludes the small percentages that said *Don't Know* or *Maybe*, the N for gender is 1,448, the N for age is 1,412, the N for education is 1,442, and the N for race/ethnicity is 1,406. See text for explanation. When the numbers don't add to 100%, it is because of rounding error. █ = Less than 1%.

♦=Using the Chi² statistic, differences are not significant at the .05 level. ♦♦= Using the Chi² statistic, differences are significant at the .05 level or lower.

Table 10: Do Gender, Age, Education, and Race/Ethnicity Predict Americans' Attitudes Toward Tailoring Political Ads Based on Identifying Facebook Friends?*

	Decrease Some / a Lot (%)	Neither Decrease Nor Decrease (%)	Increase Some / A Lot (%)
Imagine Sally visits the Facebook page of a political candidate and clicks that she "likes" the page. The campaign organization then pays Facebook to send ads to the Facebook pages of Sally's friends. The ads contain Sally's name and photo and proclaim that Sally supports the candidate.			
If you knew a political campaign that you supported was using Facebook information in this way, how would it affect your likelihood of voting for the candidate? Would your likelihood of voting for that candidate...			
♦♦ Gender			
Male (N=720)	68	27	5
Female (N=749)	75	23	2
♦♦ Age			
18-29 (N=391)	62	32	6
30-45 (N=429)	70	26	4
46-64 (N=469)	77	21	3
65 and older (N=147)	82	18	7
♦♦ Education			
High school degree (N=414)	71	22	7
Some college (N=431)	74	24	2
College degree or more (N=543)	70	29	1
♦♦ Race/Ethnicity			
White Non-Hispanic (N=1034)	75	24	2
Black Non-Hispanic (N=140)	53	36	11
Hispanic (N=161)	62	26	12
Other Non-Hispanic (N=94)	76	25	0

* Because the table excludes the small percentages that said *Don't Know* or *Maybe*, the N for gender is 1,469, the N for age is 1,436, the N for education is 1,465, and the N for race/ethnicity is 1,429. See text for explanation. When the numbers don't add to 100%, it is because of rounding error. DK=Don't know; RF=Refused; ♦=Less than 1%. ♦♦=Using the Chi² statistic, differences are not significant at the .05 level.

♦♦= Using the Chi² statistic, differences are significant at the .05 level or lower.

Americans' Rejection of Tailored Political Ads Is Not Simply Based on a General Dislike of Online Ads

The high proportions of Americans inclined to reject political ads tailored to their interests no matter what their backgrounds raises a basic question about their reasoning. Is it possible that people who reject political advertising are against it because they dislike online advertising generally? To explore this topic, we presented our respondents with a positive statement about regular online ads toward the beginning of the interview, before they received questions about tailored advertising. We asked people to agree or disagree that "I don't mind receiving ads on my computer in exchange for free content." 33% said such regular online ads are OK (including 2% who strongly agreed) and 65% said they are not OK. 1% neither agreed nor disagreed, and 3% don't have a computer.

Does the wide dislike of regular ads on computers explain the rejection of tailored political advertising? The answer is no. We did find a statistically significant correlation (Pearson=.19) between respondents' general views about receiving online ads and their views about receiving tailored political ads more specifically. However, as can be seen in Table 11, this relationship is a weak one: those who are OK with online ads are only 12% more likely than those who are not OK with them to oppose tailored political ads, and over three-in-four respondents who were OK with receiving online ads in general still did *not* want to receive tailored political ads. This finding strongly suggests that people's rejection of tailored political ads is based on reasons that go beyond a simple dislike of online ads in general.

Table 11: "I Don't Mind Receiving Ads On My Computer In Exchange for Free Content." (N=1,473)*

	No, Would Not Want Tailored Political Ads (%)	Yes, Would Want Tailored Political Ads (%)
Agree or agree strongly (N=490)	78	22
Neither agree nor disagree (N=20)	100	0
Disagree or disagree strongly (N=963)	90	10

*The table excludes the small percentages that said *Don't Know*, *Maybe*, or don't have a computer (that is, they access the internet in other ways). Using the Chi² statistic, the differences are significant at the .01 level. When the numbers don't add to 100%, it is because of rounding error. See text for further explanation.

Most Americans Want to Know What Campaigns Know About Them and How They Know

Some of Americans' wariness of tailored political ads may come from a concern that they have no control over their information. Table 12 shows that a large majority would like to understand what information about them is used for political ads and how it came to be used. When asked "If a political campaign sends you an online ad that's relevant to you, would you want to know what the campaign knows about you that led to the ad, or do you not care?," 65% say they would want to know. Further, when asked if they "would want to know where the campaign got the information to make it relevant, or do you not care?" 76% say they would want to know.

Table 12: Americans' Desire to Know the Sources of Tailoring (N=1,503)*

	Wants to Know (%)	Does Not Care (%)	DK/RF (%)
If a political campaign sends you an online ad that's relevant to you, would you want to know what the campaign knows about you that led to the ad, or do you not care?	65	33	2
If a political campaign sends you an online ad that's relevant to you, would you want to know where the campaign got the information to make it relevant, or do you not care?	76	23	1

*See text for explanation. When the numbers don't add to 100%, it is because of rounding error.
DK=Don't know; RF=Refused.

Most Americans Want Political Candidates' Websites to Ask Permission When Using Their Information

An even higher percentage of Americans agree that political websites ought to ask permission for their information. Table 13 indicates 91% of Americans say no when asked if it's OK for a political candidate's website to sell information they provide to the site. 69% of them continue to say no when told that the site's privacy policy would inform them it was selling the information. (The 69% continuing to say no represents 63% of the entire sample.) But when Americans are given the opportunity to "opt in" every time a candidate's political website wants to sell information they provided to the site, the percentage who then say no drops to 41%, which equals 38% of the entire sample. The big drop indicates that more than half of the population accepts that political campaigns should be able to use information about people if the people give affirmative permission every time.

Table 13: Americans' Desire to Have Political Candidates' Websites Ask Permission for Their Information*

	Yes, OK (%)	No, Not OK (%)	DK (%)	RF (%)	% of Entire Sample Saying No (N=1,503)
Do you think it is OK for a political candidate's website to sell information you provide to the site? (N=1,503)	8	91	1	❶	91
Do you think it is OK for a political candidate's website to sell information you provide to the site – including your name, address, and email address – if it uses the privacy policy to tell you what it was doing? (N=1,384)**	29	69	2	1	63
Do you think it is OK for a political candidate's website to sell information you provide to the site – including your name, address, and email address –as long as the campaign tells you every time it wants to do it? (N=1,384)**	58	41	1	❶	38

*See text for explanation. When the numbers don't add to 100%, it is because of rounding error.

DK=Don't Know; RF=refused. ❶ = Less than 1%

** Based on internet users who initially say it is not OK for a political candidate's website to sell information that they provide to the site, don't know or refused [N=1,384]

Concluding Remarks

Why wouldn't the other 38% who still say no allow the website to sell their data if they had the right to opt in? We suggest a large number of internet-using American adults—almost two out of five—are so wary of political advertisers' use of people's data that they simply don't want that use to take place under any conditions.

It's a startling perspective, perhaps, but the findings of our study indicate Americans share a special discomfort regarding behavioral targeting and tailored advertising when it comes to politics. Recall that the large 61% of our respondents who say they don't want regular commercial ads tailored to their interests transforms into a huge 86% who say no to tailored *political* ads. Recall, too, that consistently high proportions of the population reject particular aspects of tailored political advertising, including the three scenarios that describe activities taking place today.

These collective responses are a national statement of concern. The concern is unrelated to political-party affiliation or political orientation. It cuts across gender and age, and while it varies some with education, race and ethnicity the numbers opposing tailored political advertising are high across the board.

The fundamental issue growing out of these findings is enormous: The public's emphatic and broad rejection of tailored political advertising bumps directly up against the huge growth of this

very activity in the 2012 presidential election. What we have is a major attitudinal tug of war—a political class pulling for new ways to divide and address the populace versus a public that appears deeply uncomfortable, even angry, about activities pointing in that direction. This stark collision of political and public views raises two obvious questions: How should politicians respond when the public rejects the very activities their marketing advisors insist represent the future of political campaigning? And, how should the public respond to a politician-created environment suffused with behavioral targeting, data-mining, and tailored communication that it finds distasteful and that generally take place without the permission or even knowledge of the citizens?

These issues have hardly been addressed until now. In the wake of our survey, they deserve to be central to public discussions regarding the future of political campaigning in the twenty-first century. That is because the divide we found between the public’s attitudes about what should take place in politics and what actually takes place may in coming decades erode citizens’ beliefs in the authority of elections. To understand how this erosion can take place, it is important to understand that technology already exists to make television sets “addressable” electronically much as the internet is today. Technology also exists to create audiovisual commercials on the fly that reflect the demographic makeup and political orientation of a household.¹⁹ When these developments roll out, political marketers will consider today’s tailored ads primitive forerunners of their new era.

It will be possible for campaigns to virtually envelope households and individuals with candidates created *for them*. A campaign database may predict that one particular household would lean toward a candidate if it learned of three positions but not four others, while another household would vote for the candidate if it learned of those four but not the other three. Targeting and tailoring technologies will allow the candidate to suffuse likely supporters with the “right” messages online, on mobile devices, on TV, and even in print while playing down or eschewing messages that the data predict will cause dissonance. Opposition candidates and even journalists will have a hard time learning what homes get which thousands of messages, and candidates on news programs will learn to speak in ways that are compatible with broadly acceptable versions of what they believe.

Citizens will know (as this survey has found they already know) that political targeting and tailoring takes place, but they won’t know how or exactly when. They may therefore see every political advertisement—and eventually every message from a politician—with wariness about how the politicians have defined their interests and resentment that they cannot easily know the messages their neighbors, relatives, co-workers, friends, and enemies are getting.

In response to such concerns, political campaign managers will likely point out that the targeting and tailoring that Americans say they dislike nevertheless succeeds in efficiently persuading voters and gaining active adherents, and so its utility trumps the public’s qualms. But this thinking is short term. Long-term the effect of campaigns that surround people with messages based on tactics they intuit but don’t understand or approve may well be to erode people’s trust that they are receiving an honest agenda of issues from candidates. They may see data-driven tailored political communication as an anti-democratic way of practicing democracy. Such corrosive attitudes may end up wounding the credibility of politicians before and after their

campaigns. The attitudinal tug of war will grow tougher and tougher, with resulting tensions coursing throughout the political system.

So what should be done? Our survey suggests that at a minimum Americans want to know what political campaigns know about them and how they got this information. We also found that Americans want political candidates' websites to ask permission to use information about them. In addition, lifting the hood publicly on data-driven political-campaign tactics can be an important way to bring citizens into the process and encourage them to participate in the creation of an election environment that they both understand and approve. This can be achieved through a combination of active press coverage of the issue, frequent surveys of public attitudes on the topic, regular inclusion of politicians' database-marketing activities in campaign coverage and discussions of the public sphere more generally, and the rise of advocates who will insist politicians adopt norms and even limits regarding targeting, tailoring, and data mining.

We hope that this report is a first step to opening up all sorts of public discussion regarding Americans' understanding of their evolving political system and where they would like to see it go.

REFERENCES

- ¹ Michael McGerr, *The Decline of Popular Politics: The American North, 1865-1928*. New York: Oxford University Press, 1986, p. 94.
- ² James Verini, "Big Brother, Inc." *Vanity Fair*, December 200,
<http://www.vanityfair.com/politics/features/2007/12/aristotle200712> Accessed June 19, 2012.
- ³ Sasha Issenberg. 'Anatomy of a narrow victory,' *Slate*, January 4, 2012,
http://www.slate.com/articles/news_and_politics/victory_lab/2012/01/romney_s_iowa_win_it_took_a_lot_more_than_money_.html Accessed June 19, 2012.
- ⁴ See Tanzina Vega, "Online Data Helping Campaigns Customize Ads," *New York Times*, February 20, 2012.
http://www.nytimes.com/2012/02/21/us/politics/campaigns-use-microtargeting-to-attract-supporters.html?_r=1&pagewanted=all Accessed June 19, 2012.
- ⁵ Federal Trade Commission, "Fair Information Practices Principles,"
<http://www.ftc.gov/reports/privacy3/fairinfo.shtm#Enforcement/Redress> Accessed June 18, 2012.
- ⁶ Lois Beckett. 'How Microsoft and Yahoo Are Selling Politicians Access to You,' *ProPublica*, June 11, 2012.
<http://www.propublica.org/article/how-microsoft-and-yahoo-are-selling-politicians-access-to-you>. Accessed June 29, 2012.
- ⁷ P. Whoriskey. 'Candidates' Web Sites Get to Know the Voters,' *WashingtonPost.com*, August 30 2008.
http://msl1.mit.edu/furdlog/docs/washpost/2008-08-30_washpost_political_ad_targeting.pdf. Accessed June 5, 2012.

⁸ J.D. Schlough, J. Koster, A. Barr and T. Davis. ‘Persuasion Points Online: Helping Harry Reid, One Click at a Time,’ *Campaigns & Elections*, May 17 2011. <http://www.campaignsandelections.com/case-studies/176152/persuasion-points-online-helping-harry-reid-one-click-at-a-time.thtml>. Accessed October 19, 2011.

⁹ K. Kaye. ‘Facebook Enables Zip Code Targeting for Ads,’ *ClickZ*, August 11 2011. <http://www.clickz.com/clickz/news/2101293/facebook-enables-zip-code-targeting-ads>. Accessed December 10, 2011.

¹⁰ T. Meloche. ‘How hyper-targeted ads boost your Facebook strategy,’ *All Facebook*, December 9 2011. <http://www.allfacebook.com/facebook-ad-targeting-2011-12>. Accessed December 10, 2011.

¹¹ Schlough, et al.

¹² Ed Pilkington and Amanda Michel. ‘Obama, Facebook and the power of friendship: the 2012 data election,’ *The Guardian*, February 17, 2012. <http://www.guardian.co.uk/world/2012/feb/17/obama-digital-data-machine-facebook-election>. Accessed February 17, 2012.

¹³ M.L. Sifry, ‘Election 2012: It’s not Facebook. It’s the data, stupid,’ *TechPresident*. April 20, 2011. <http://techpresident.com/blog-entry/election-2012-its-not-facebook-its-data-stupid>. Accessed June 6, 2012.

¹⁴ Kate Kaye. ‘Tim Pawlenty tests Facebook sponsored stories,’ *ClickZ*, May 27, 2011. <http://www.clickz.com/clickz/news/2074620/tim-pawlenty-tests-facebook-sponsored-stories> Accessed June 19, 2012.

¹⁵ MarketWatch. ‘Political Campaigns Use Hyper-Local Targeted Mobile Signup Ads to Reach Voters in Swing States and Across the Nation,’ *Wall Street Journal*, May 23 2012. <http://www.marketwatch.com/story/political-campaigns-use-hyper-local-targeted-mobile-signup-ads-to-reach-voters-in-swing-states-and-across-the-nation-2012-05-23>. Accessed June 7, 2012.

¹⁶ Daniel Kreiss, “Yes We Can (Profile You): A Brief Primer on Campaigns and Political data,” 64 Stanford Law Review Online 70, <http://www.stanfordlawreview.org/online/privacy-paradox/political-data>. Accessed May 27, 2012.

¹⁷ Jordan Lieberman, Jeff Dittus and Rich Masterson, “Yes, We Can Profile You and Our Political System is Better for It,” *CampaignGrid*, February 7, 2012, http://www.campaigngrid.com/_blog/CampaignGrid_in_the_News/post/Yes_We_Can_%28Profile_You%29_And_Our_Political_System_Is_Stronger_for_I_An_Industry_Response_from_CampaignGrid,_LLC/. Accessed May 27, 2012. Campaign Grid is now called Audience Partners.

¹⁸ Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy, “Americans Reject Tailored Advertising,” Annenberg School for Communication and Berkeley Law School, September 2009. Available online at <http://ssrn.com/abstract=1478214>

¹⁹ See Joseph Turow, *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth* (New Haven, Yale University Press, 2011), pp. 160-170. See also Terry Gross and Joseph Turow, “How Companies Are ‘Defining Your Worth’ Online,” National Public Radio *Fresh Air* interview, February 22, 2012, <http://www.npr.org/2012/02/22/147189154/how-companies-are-defining-your-worth-online> Accessed June 7, 2012.

I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

JOSEPH TUROW,^a CHRIS JAY HOOFNAGLE,^b DEIRDRE K. MULLIGAN,^c
NATHANIEL GOOD,^d & JENS GROSSKLAGS^e

The Federal Trade Commission and Consumer Privacy in the Coming Decade

Abstract:^f The large majority of consumers believe that the term “privacy policy” describes a baseline level of information practices that protect their privacy. In short,

^a Joseph Turow, Ph.D., is the Robert Lewis Shayon Professor of Communication at the University of Pennsylvania’s Annenberg School for Communication, and the director of the Information & Society Program at the University of Pennsylvania’s Annenberg Public Policy Center. He is the author of, among other books, *Niche Envy: Marketing Discrimination in the Digital Age* (Cambridge, MA: MIT Press, 2006).

^b Chris Jay Hoofnagle, J.D., is a senior staff attorney at the Samuelson Law, Technology & Public Policy Clinic, and a senior fellow at the Berkeley Center for Law & Technology of the Boalt Hall School of Law.

^c Deirdre K. Mulligan, J.D., is the director of the Samuelson Law, Technology & Public Policy Clinic and the Clinical Program at the Boalt Hall School of Law. The work of the Samuelson Clinic is generously supported through an endowment from Professor Pamela Samuelson and Robert Glushko, Ph.D. Additional funding is provided by: The Rose Foundation for Communities and the Environment, the California Consumer Protection Foundation, and the National Science Foundation, Team for Research in Ubiquitous Secure Technologies, NSF CCF-0424422.

^d Nathaniel Good is a Ph.D. candidate at the School of Information at the University of California, Berkeley.

^e Jens Grossklags is a Ph.D. candidate at the School of Information at the University of California, Berkeley. His work is supported in part by the National Science Foundation through ITR award ANI-0331659.

^f This article originally appeared as a paper presented under the same title at the Federal Trade Commission Tech-ade Workshop on November 8, 2006. The version published here contains additional information collected during a 2007 survey.

“privacy,” like “free” before it, has taken on a normative meaning in the marketplace. When consumers see the term “privacy policy,” they believe that their personal information will be protected in specific ways; in particular, they assume that a website that advertises a privacy policy will not share their personal information. Of course, this is not the case. Privacy policies today come in all different flavors. Some companies make affirmative commitments not to share the personal information of their consumers. In other cases, however, privacy policies simply inform consumers that unless they “opt out” of sharing certain information, the company will communicate their personal information to other commercial entities.¹

Given that consumers today associate the term “privacy policy” with specific practices that afford a normative level of privacy protection, the use of the term by a website that does not adhere to these baseline practices can mislead consumers to expect privacy that, in reality, does not exist. This is not to suggest that companies intend to mislead consumers, but rather that consumers today associate certain practices with “privacy policy” just as they associate certain terms and conditions with the word “free.”

Because the term “privacy policy” has taken on a specific meaning in the marketplace and connotes a particular level of protection to consumers, the Federal Trade Commission (“FTC”) should regulate the use of the term “privacy policy” to ensure that companies using the term deliver a set of protections that meet consumers’ expectations and that the term “privacy policy” does not mislead consumers during marketplace transactions.

¹ Often consumers are not provided with a means to “opt out” of information sharing.

I. INTRODUCTION

Ten years have passed since the FTC's last comprehensive hearings on the future of consumer protection. In that time, the FTC has pursued a self-regulatory approach to protecting the privacy of personal information, working with industry to deliver market-based approaches ranging from industry best practices, self-regulatory initiatives, advances in technology, and consumer education.

A core goal of these efforts has been to publicize how personal information is handled by companies, in the belief that, if armed with accurate information, consumers will make privacy choices consistent with their personal needs. The FTC has established a set of disclosures that responsible companies should provide to consumers in order to facilitate the consumers' exercise of informed choice about privacy in the marketplace.

Ten years later, it is appropriate to ask what effects these disclosures have had on consumers' experiences in the marketplace. Have improved privacy disclosures allowed consumers to achieve the level of privacy they desire in marketplace transactions? Are consumers more at ease with respect to privacy in marketplace transactions today than they were ten years ago? What is the effect of the existence of "privacy policies" at most of the leading websites? What do consumers think when they see the term "privacy policy"?

This article attempts to answer these questions based on existing peer-reviewed research and consumer surveys conducted in the academic sector. The article examines the strengths and limitations of the notice-based approach to facilitating privacy in the consumer marketplace. Using (1) survey data on consumers' privacy expectations, (2) existing research on whether and in what instances consumers read and comprehend notices, (3) the role information asymmetry and psychological barriers to information processing and risk assessment play in privacy decision-making, and (4) insights about interface design and information presentation, this article identifies several factors that limit the ability of the notice-based approach, operating alone, to meet the varying privacy needs of consumers in the marketplace. It concludes that:

- Without a baseline set of information practices, the term "privacy policy" is confusing to the consumer;

- The lack of common disclosure language undermines consumers' ability to "shop for privacy," thereby undermining businesses' ability to compete on privacy;
- Shortened notices are a promising step toward encouraging a successful privacy marketplace for the consumers who read notices;
- Privacy must be "usable" if it is to serve consumer needs; therefore, incorporating expertise from fields such as human computer interaction and psychology is imperative; and
- If consumers are not able to make informed choices about information privacy and computer security, then it is inevitable that bad actors will undermine consumer privacy and the security of the network infrastructure.

At this ten-year interval, it is important to consider the effect of the FTC's approach to privacy. Research provides important information about the strengths and limitations of the FTC's work to date. The FTC should use this information to refine and adjust its policy to reflect what we know today about consumer expectations and actions in the marketplace. In addition, this article's conclusions, listed above, suggest several additional interventions in the marketplace:

- Require businesses that advertise a "privacy policy" to provide some baseline privacy protections that meet established consumer expectations;
- Standardize disclosures and terminology to facilitate comparison shopping by consumers and competition among firms based on privacy practices;
- Shorten notices to reduce the transaction costs associated with reading long, indecipherable End User License Agreements ("EULAs"); and,
- Include information from other disciplines, including usability and human computer interaction, in future privacy and security initiatives.

II. THE FTC'S APPROACH TO CONSUMER PRIVACY

Just over ten years ago, the FTC conducted its last forward-looking proceeding in which it analyzed the future of consumer protection in a high-tech economy. In a report from that proceeding, the FTC concluded that the essential elements of a balanced consumer protection program are:

- Coordinated law enforcement by state and federal agencies against fraud and deception;
- Industry self-regulation and private initiatives to protect consumers; and
- Consumer education through the combined efforts of government, business, and consumer groups.²

The report continues:

The hearing record is replete with examples of private initiatives: industry self-regulation programs and plans to develop and expand such programs, technology-based consumer protections and self-help opportunities, and commitments to undertake new consumer education programs. These and other initiatives will be crucial in providing consumer protection in the new marketplace.³

Over the past ten years, the FTC has pursued these three goals. It has brought an impressive array of actions under the agency's authority to prosecute unfair or deceptive trade practices.⁴ It has fostered self-regulatory programs and it continues to operate multilingual consumer outreach both online and offline.

The FTC established five Fair Information Practice Principles (“FIPPS”)—notice, choice, access, security and accountability—as the

² Federal Trade Commission, *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (hearing report, May 1996); 46 (formatting added). Also available online at http://www.ftc.gov/opp/global/report/gc_v2.pdf.

³ Ibid.

⁴ Marcia Hoffman, “Federal Trade Commission Enforcement of Privacy,” in *Proskauer on Privacy* (New York: Practicing Law Institute, 2006).

framework for self-regulatory and regulatory initiatives. The Commission's approach omitted several important data protection principles that were recognized by the Organization for Economic Cooperation and Development Guidelines ("OECD"), including the concepts of "data minimization," which requires companies to restrict the amount of personal information collected to only that which is necessary for a transaction, and "purpose specification," which requires companies to have a clear and legitimate purpose for data collection.

The absence of these two principles has led firms to collect extraneous information and to repurpose information without consumer consent. After adopting its limited set of FIPPS, the FTC highlighted the importance of notice and security. The agency did intervene to set standards for children's privacy that are stronger than the norm; the Children's Online Privacy Protection Act ("COPPA") requires prior parental consent before personal information can be collected from children under the age of thirteen.⁵ In general, though, the agency put substantial resources behind encouraging adaptation of notice, and the development of "short notices." The market-based approach to privacy in the electronic commerce sphere adopted by the FTC was a departure from a tradition of privacy laws, such as the Fair Credit Reporting Act of 1970 ("FCRA") and the Privacy Act of 1974, which embraced a full set of FIPPS to protect personal information.

Most e-commerce sites today have privacy policies, but whether these policies provide privacy protection remains an open question. The FTC has not evaluated the basic assumption of the market-based model to privacy protection: that with good information consumers will make good choices. Echoing the recommendations from the 1995 hearings, Chairman Majoras seeks to employ the same techniques used to protect privacy during the last decade:

First, we must study and evaluate new technologies so that we are as prepared as possible to deal with harmful, collateral developments. Second, we need to bring appropriate law enforcement actions to reaffirm that fundamental principles of FTC law apply in the context of new technologies. Third, we must look to industry to implement self-regulatory regimes and, more importantly, to

⁵ *Children's Online Privacy Protection Act of 1998*, Public Law 105-277, codified at U.S. Code 15 (2000), §§ 6501 *et seq.*

develop new technologies. Finally, we need to educate consumers so that they can take steps to protect themselves.⁶

At this important juncture, it makes sense to evaluate the strengths and weaknesses of these techniques. Before the FTC decides what approaches to pursue during the next decade, we suggest that the agency critically reflect on research that explores the effectiveness of the self-regulatory system.

The FTC has held close the assumption that introducing additional information about companies' data practices into the marketplace through self-regulatory systems, combined with consumer self-help, will allow consumers to adequately protect their privacy as they see fit. But research shows that consumers continue to have high levels of concern for privacy of personal information. It also reveals that the EULAs and privacy policies used to convey this information to consumers are not effective—they are rarely read and are in many instances unreadable. More importantly, consumers appear to believe that the term "privacy policy" conveys a specific level of privacy protection. Confusion exists among consumers concerning what rights they have and can exercise over personal information. Interestingly, while the FTC has pursued self-regulatory solutions to consumer privacy, the large majority of consumers believe incorrectly that laws protect their personal information from secondary use.

III. RESEARCH DEMONSTRATES THE LIMITS OF THE DISCLOSURE-BASED APPROACH

A. CONSUMERS CARE DEEPLY ABOUT PRIVACY

Surveys conducted by the Annenberg Public Policy Center show that Americans care deeply about the privacy of their personal information and that despite the FTC's ten-year commitment to self-regulation,⁷ they are nevertheless concerned about information collection.⁷ A 2003 Annenberg survey found that 70% of advanced

⁶ Deborah Platt Majoras, "Finding the Solutions to Fight Spyware: The FTC's Three Enforcement Principles," (remarks, Anti-Spyware Coalition, Washington, D.C., February 9, 2006): 3, <http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf>.

⁷ Unless otherwise noted, the public polling data presented are from two national surveys created by Professor Turow and carried out by the firm ICR/International Communication Research of Media, Pennsylvania. For the 2003 survey, *infra* note 8, ICR interviewed by phone a nationally representative sample of 1,200 adults who were using the Internet at home.

users agreed or agreed strongly with the statement, "I am nervous about websites having information about me."⁸ In 2005, the same response was reported by 79% of respondents.⁹ Individuals also believe that they are put at risk as a result of information collection. Only 17% agreed with the proposition, "What companies know about me won't hurt me."¹⁰

A high level of concern is also reported about both commercial and government collection of personal information. In 2003, 92% reported that they would be concerned if marketers were "collecting information about your household members' activities without your knowledge or consent."¹¹ Similarly 83% would be concerned if the government was "collecting information about your household members' activities without your knowledge or consent."¹² (52% believed the federal government was doing that.¹³) Respondents also believe that they should be in control of marketing communications. For instance, 94% reported that websites should ask for permission before sending ads.¹⁴

B. CONSUMERS FUNDAMENTALLY MISUNDERSTAND THE "PRIVACY POLICY" LABEL

Supporters of privacy self-regulation suggest that Americans' high levels of concern will be alleviated when they begin to examine their options for releasing personal data. Professor Alan Westin, for

For the 2005 survey, *infra* note 9, ICR interviewed by phone a nationally representative sample of 1,200 adults who said they used the Internet in the past month.

⁸ Joseph Turow, *Americans and Online Privacy: The System is Broken* (Philadelphia: Annenberg Public Policy Center, June 2003): 16. Also available online at <http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf>.

⁹ Joseph Turow, Lauren Feldman and Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline* (Philadelphia: Annenberg Public Policy Center, June 2005): 4. Also available online at http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/Turow_APPC_Report_WEB_FINAL.pdf.

¹⁰ Ibid.

¹¹ Turow, *Americans and Online Privacy*, 19–20.

¹² Ibid.

¹³ Ibid., 19.

¹⁴ Ibid., 28.

example, has written that most Americans take an informed cost-benefit tack in relation to their information online and offline.¹⁵ "They examined the benefits to them or society of the data collection and use, wanted to know the privacy risks and how organizations proposed to control those, and then decided whether to trust the organization or seek legal oversight."¹⁶ This characterization of most Americans as being aware of their online privacy options supports the viewpoint of Internet industry players that posting an accurate privacy policy on every site would create a world of optimal consumer privacy in which each individual shopped with his or her mouse for privacy that matched his or her personal needs.

Unfortunately that does not appear to be happening. One could assume from this that consumers do not care, the argument being that companies give individuals information and they ignore it or fail to value the privacy choices it offers. However, research tells a far more complex story about why privacy disclosures alone have failed to alleviate the privacy concerns of individuals.

The push for privacy disclosures has resulted in a world of legalistically phrased privacy policies that begin by assuring the consumer that the site cares about his or her privacy, but then proceeds to confuse the consumer with technical language about "affiliate" and "non-affiliate" sharing, required disclosures, distinctions between personally identifiable information ("PII") and aggregate data, inapplicability with regard to other sites, or content that may be included or accessed from the site, and finish with the caveat that the privacy policy can change at any time, with or without notice.¹⁷

Both the 2003 and 2005 Annenberg surveys revealed, however, that American adults do not know that privacy policies merely tell people how the site will use their information: whether or not, and how, they will share it with affiliates and outside firms.¹⁸ Most

¹⁵ A. F. Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues* 59, no.2 (2003): 445.

¹⁶ Ibid.

¹⁷ For example, of 64 website privacy policies that were reviewed between 2001 and 2003, Jensen and Potts found that eight (13%) offered no mention of how changes to the policy would be conveyed to the user, twelve policies (19%) offered to notify users through email and a posting on the policy page, and 44 policies (69%) required users to check the policy page periodically. C. Jensen and C. Potts, "Privacy Policies as Decision-making Tools: An Evaluation on Online Privacy Notices," in *CHI 2004 Connect: Conference Proceedings* (New York: ACM Press, 2004), 471–78.

¹⁸ Turow, *Americans and Online Privacy*, 3; Turow, Feldman and Meltzer, *Open to Exploitation*, 3.

Americans believe, logically, that the phrase “privacy policy” signifies that *their information will be kept private*. In the 2003 survey, 57% of the nationally representative sample of 1,200 adults who were using the Internet at home agreed or agreed strongly with the statement, “When a web site has a privacy policy, I know that the site will not share my information with other websites or companies.”¹⁹ In the 2005 survey, questioners asked 1,200 nationally representative adults who said they had used the Internet in the past month whether that statement is true or false; 59% answered it is true.²⁰

C. CONSUMERS MISUNDERSTAND ONLINE DATA COLLECTION

The misunderstandings do not stop with the label. The 2003 survey found that 59% of adults who use the Internet at home know that websites collect information about them even if they do not register;²¹ however, they do not understand that data-flows behind their screens connect seemingly unrelated bits about them.²² The survey’s interviewers asked respondents to name a site they valued and then went on to ask their reaction to click-stream advertising,²³ which is actually a common way that sites track, extract and share information to make money from advertising. Of the surveyed adults who go online at home, 85% stated that they did not agree to the collection and aggregation of their data across multiple sites for purposes of click-stream advertising, even by a “valued” site.²⁴ When offered a choice of using a valued site for free and letting information be collected, or paying for the site and not letting information be collected, 54% of adults who go online at home said that they would rather find the information offline than exercise either option presented.²⁵

¹⁹ Turow, *Americans and Online Privacy*, 3.

²⁰ Turow, Feldman and Meltzer, *Open to Exploitation*, 20.

²¹ Turow, *Americans and Online Privacy*, 3.

²² Ibid.

²³ Ibid.

²⁴ Ibid.

²⁵ Ibid.

Among the 85% who did not accept the data-collection practice, one in two (52%) had earlier said that they gave or would likely give the valued site their real name and email address.²⁶ Yet those bits of information are what a site needs to begin creating a stream of data about them—the very flow, personally identifiable or not, that they refused to allow in response to the scenario. Moreover, 63% of the people who said they had provided this data had also agreed that the mere presence of a website privacy policy means that the website will not share data with other firms.²⁷ Bringing these two results together suggests that at least one out of every three respondents who refused to barter their information either do not understand or do not think through the privacy outcomes of basic data-collection activities on the Internet.

Similarly, other fundamental processes involved in online interactions are not very well understood by the consumer. In a related survey, Acquisti and Grossklags show that individuals are often unable to name obvious parties, beyond the merchant and the consumer, that have access to consumer data during and after an online credit card transaction, such as the credit card company.²⁸ These findings help uncover the important distinction between knowledge about commercial practices that is active and actionable, and knowledge that is passive or completely lacking. Most consumers have some passive knowledge about the roles played by credit card companies, other third parties, and technical processes, but it is doubtful that this knowledge is always available to them when they are actively making decisions.

D. CONSUMERS MISUNDERSTAND MANY RULES ABOUT PRIVACY IN THE MARKETPLACE

These misconceptions about information privacy and data practices are, however, merely the tip of an iceberg of consumer confusion concerning their rights and merchants' rights to consumer information

²⁶ Ibid.

²⁷ Ibid., 23.

²⁸ When 119 university staff and students were confronted with the open-ended question: "You completed a credit-card purchase with an online merchant. Besides you and the merchant Web site, who else has data about parts of your transaction?" 34.5 percent of the sample answered "nobody," 21.9 percent answered "my credit card company or bank," and 19.3 percent answered "hackers or distributors of spyware." A. Acquisti and J. Grossklags, *Privacy and Rationality in Individual Decision Making, IEEE Sec. & Privacy* 3, no. 1 (2005): 26–33.

in the marketplace. Table 1 lists true-or-false statements that the 2005 Annenberg survey presented to its representative national sample.²⁹ The answers indicate a low level of understanding of consumer rights and redress in the marketplace. A high proportion of consumers believe they have certain privacy rights—notably consistent with those provided under FIPPS—when they do not. Others simply have no idea what rights they have.

Table 1: True/false responses to statements about rules of profiling, behavioral targeting, price discrimination and recourse in the marketplace. (1,500 persons sampled)

	%T	%F	%DK
Most online merchants give me the opportunity to see the information they gather about me. <i>47% did not know the right answer</i>	23	53	25
Most online merchants allow me the opportunity to erase information they have gathered about me. <i>50% did not know the right answer</i>	19	50	30
A website is allowed to share information about me with affiliates without telling me the names of the affiliates. <i>49% did not know the right answer</i>	51	29	20
It is legal for an online store to charge different people different prices at the same time of day. <i>62% did not know the right answer</i>	38	29	33
Respondent correctly identifies the name of a credit-reporting agency. <i>66% did not know the right answer</i>	34	66	--
By law, a site such as Expedia or Orbitz that compares prices on different airlines must include the lowest airline prices. <i>68% did not know the right answer</i>	37	32	31

²⁹ Turow, Feldman and Meltzer, *Open to Exploitation*, 15.

Table 1: (continued)			
It is legal for an offline store to charge different people different prices at the same time of day. <i>71% did not know the right answer</i>	29	42	29
Bold numbers indicate the correct answer. Sums greater than 100% result from rounding errors. DK=Don't Know			

A 2007 Golden Bear telephone survey of Californians reinforces the idea of consumer misunderstanding about online marketplace privacy policies and rules.³⁰ This survey focused on people who have actually purchased items on the Internet and, as such, would presumably be more informed than participants in the Annenberg studies, who were adults who used the Internet for any reason. Moreover, the statements about rules and privacy policies in the Golden Bear survey were more varied than those in the Annenberg study.

Despite their presumably greater stake in commerce and privacy than the Annenberg respondents, the Golden Bear respondents followed the same pattern; almost 70% of the respondents knew that sites are allowed to keep records of their addresses and purchase histories. The respondents' knowledge was much worse, however, with respect to the other statements about privacy policies and marketplace rules, as Table 2 shows. Note that when presented with a privacy-policy statement that was similar to the one in the Annenberg study—if a website has a privacy policy, it means that the site cannot sell information about your address and purchase information to other companies—the percentage of respondents who answered incorrectly was very similar, 55% in Golden Bear compared to 59% in Annenberg.

³⁰ The 2007 Golden Bear Omnibus Survey was a random-digit telephone survey of 1,186 English- and Spanish-speaking adults in California. It was conducted by the University of California's Survey Research Center using Computer-Assisted Telephone Interviewing (CATI) to landline and wireless phones from April 30, 2007, to September 2, 2007. It was funded by the Survey Research Center. The privacy questions were funded by the Samuelson Clinic.

Table 2: True/false responses to statements about rules of the online marketplace.

	%T	%F	%DK
If a website has a privacy policy, it means that the site cannot keep records of your address and purchase history. (188 persons sampled) <i>30.9% did not know the right answer</i>	19.7	69.1	11.2
If a website has a privacy policy, it means that the site cannot give information about your address and purchases to the government. (208 persons sampled) <i>45.2% did not know the right answer</i>	36.1	54.8	9.1
If a website has a privacy policy, it means that the site cannot use information to analyze your online activities. (205 persons sampled) <i>47.8% did not know the right answer</i>	37.1	52.2	10.7
If a website has a privacy policy, it means that the site cannot buy information about you from other sources to analyze your online activities. (251 persons sampled) <i>50.6% did not know the right answer</i>	39.8	49.4	10.8
If a website has a privacy policy, it means that the site cannot share information about your address and purchases with affiliated companies that are owned by the website. (207 persons sampled) <i>55% did not know the right answer</i>	47.8	44.9	7.2
If a website has a privacy policy, it means that you have the right to require the website to tell you what other businesses purchased your personal information. (208 persons sampled) <i>60.1% did not know the right answer</i>	51.9	39.9	8.2

Table 2: (continued)	%T	%F	%DK
If a website has a privacy policy, it means that you have the right to obtain help from the website, if information you provided to it was used for identity theft. (198 persons sampled) <i>64.1% did not know the right answer</i>	49.5	35.9	14.6
If a website has a privacy policy, it means that the site cannot sell information about your address and purchase information to other companies. (231 persons sampled) <i>64.5% did not know the right answer</i>	55.4	35.5	9.1
If a website has a privacy policy, it means that you have the right to sue the website for damages if it violates your privacy. (230 persons sampled) <i>65.6% did not know the right answer</i>	53	34.3	12.6
If a website has a privacy policy, it means that you have the right to access your personal information stored on the site and correct it. (222 persons sampled) <i>72.1% did not know the right answer</i>	56.8	27.9	15.3
If a website has a privacy policy, it means that you have the right to be notified if the website has a security breach that leaks information about you to others. (215 persons sampled) <i>75.4 did not know the right answer</i>	64.7	24.7	10.7
If a website has a privacy policy, it means that you have the right to require the company to delete your personal information upon your request. (213 persons sampled) <i>77% did not know the right answer</i>	68.1	23	8.9
Bold numbers indicate the correct answer. Sums greater than 100% result from rounding errors. DK=Don't Know.			

E. PRIVACY NOTICES ALONE ARE INSUFFICIENT

Despite self-regulatory efforts, there remains substantial confusion among consumers about information privacy. Much of the FTC's attention has focused on the development of improved disclosures. Surveys, user studies, and focus groups do support the agency's belief that users would welcome well-crafted, short notices in the hope that they will ease comprehension of privacy policies.

In research supported by the National Science Foundation Science and Technology Center, Team for Research in Ubiquitous Secure Technologies ("TRUST"),³¹ researchers at U.C. Berkeley's Samuelson Clinic have examined the utility of short notices and variations on notice timing in communicating about privacy, security, and other consequences of software installation.³² The installation of downloadable software almost always involves the click-through to privacy notices and EULAs. Notices are usually presented in a separate screen during installation and are reasonably accessible to the user. Users are involved in a main task of evaluating and deciding whether to install a piece of software. Given that information about security, privacy, and functionality are disclosed during the installation process, this is a natural context in which to explore the utility of such notices and disclosures.

Recent studies involving EULAs suggest that they are largely ineffective as a means of communicating with consumers. EULAs, terms-of-service agreements ("ToS"), and privacy policies present complex legal information. Research shows that notices' complexity

³¹ This work was generously supported by the NSF Science and Technology Center, Team for Research in Ubiquitous Secure Technologies ("TRUST"), NSF CCF-0424422. Computer trustworthiness continues to increase in importance as a pressing scientific, economic, and social problem. As a consequence, there is an acute need for developing a much deeper understanding of the scientific foundations of cyber security and critical infrastructure systems, as well as their implications for economic and public policy. In response to this need, TRUST is devoted to the development of a new science and technology that will radically transform the ability of organizations (software vendors, operators, local and federal agencies) to design, build, and operate trustworthy information systems for our critical infrastructure. The Center brings together a team with a proven track record in relevant areas of computer security, systems modeling and analysis, software technology, economics, and social sciences. See <http://trust.eecs.berkeley.edu/> for details of all of TRUST's research.

³² For detailed results of the studies, see Nathaniel Good and others, "Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware," in *Proceedings of the Symposium on Usable Privacy and Security* (New York: ACM Press, 2005), 43–52; Nathaniel Good and others, "Noticing Notice: A Large-scale Experiment on the Timing of Software License Agreements" in *Proceedings of CHI 2007* (New York: ACM Press, 2007), 607–16.

hampers users' ability to understand such agreements. For example, Jensen and Potts studied a sample of 64 privacy policies from high-traffic and healthcare websites.³³ They found that the policies' formats, locations on the websites, and legal content severely limit users' ability to make informed decisions based on them.³⁴

In another study that produced similar results, Grossklags and Good evaluated the notice practices of 50 popular downloadable programs.³⁵ The location and presentation of the notices differed from vendor to vendor, which would make it more difficult for consumers to find relevant information. These notices were often difficult to understand or even read. The average EULA was over 2500 words long and would require approximately thirteen minutes for a consumer of average reading skill to parse, according to accepted reading metrics. Font sizes were often too small to be read easily and notices were displayed in comparatively small windows, for example, showing only one percent of the complete notice text at a time.

Research indicates that simplifying the notices has a limited effect. Masson and Waldron showed that simplifying the language of legal contracts, for example, by using easier words and replacing obscure terms with common ones, could not achieve very high degrees of comprehension.³⁶ This is because "non-experts have difficulty understanding complex legal concepts that sometimes conflict with prior knowledge and beliefs."³⁷

Vila and others ask whether users will ever bother to read or believe privacy policies at all.³⁸ They claim that because the cost of

³³ Jensen and Potts, "Privacy Policies as Decision-making Tools: An Evaluation on Online Privacy Notices."

³⁴ Ibid.

³⁵ Jens Grossklags and Nathan Good, "Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers," in *Lecture Notes in Computer Science* (Berlin: Springer, 2008), 341–55. Originally presented at Useable Security (USEC'07), February 15–16, 2007. Also available online at <http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags07-USEC.pdf>.

³⁶ M.E.J. Masson and M.A. Waldron, "Comprehension of Legal Contracts by Non-experts: Effectiveness of Plain Language Redrafting," *Applied Cognitive Psychology* 8 (1994): 67–85.

³⁷ Ibid.

³⁸ T. Vila, R. Greenstadt and D. Molnar, "Why We Can't be Bothered Reading Privacy Policies - Models of Privacy Economics as a Lemons Market," in *Proceedings of the Fifth International Conference on Electronic Commerce* (Pittsburg: ICEC, 2005), 403–07. Also available online at <http://www.eecs.harvard.edu/~greenie/econprivacy.pdf>.

misrepresentation in a privacy policy is low and that some of the privacy policies are not trustworthy, users do not feel it is worth their time to read or pay attention to them.³⁹ In contrast, results from the 2003 Annenberg survey suggest that relatively high proportions of adults with the Internet at home trust privacy policies; 71% agreed or agreed strongly, “I look to see if a website has a privacy policy before answering any questions.”⁴⁰ Anecdotal evidence does, however, support the impression that people do not read the policies. One software provider included a \$1000 cash prize offer in a EULA that was displayed during every software installation. It took four months and 3,000 downloads of the software for someone to notice the clause and claim the prize.⁴¹

Among 222 study participants, the Samuelson Clinic found that only 1.4% reported reading EULAs often and thoroughly, 66.2% admit to rarely reading or browsing the contents of EULAs, and 7.7% indicated that they have not noticed these agreements in the past or have never read them.⁴²

Short and layered notices are one method that has been proposed to overcome these problems. The Samuelson Clinic has performed a controlled study of short notices and timing of notices. The study examined whether consumers were happy with their installation decisions after they were fully informed of the program’s activities; this is termed “regret.” When downloading and installing programs, subjects were shown either the EULA by itself or the EULA and a short notice highlighting core aspects of performance, privacy and security.

During the post-experimental survey, all study participants were shown the short notices. When asked whether they would install the programs they chose to install during the experiment, participants who received the short notices during the study were less likely to reverse their earlier decision to install software. However, many users, both those who originally received the short notice and those who did not, expressed regret about their installation decisions after reading the short notice during the exit interview. Overall, the incidence of regret

³⁹ Ibid.

⁴⁰ Turow, *Americans and Online Privacy*, 18.

⁴¹ Larry Magid, It Pays To Read License Agreements, <http://www.pepitstop.com/spycheck/eula.asp> (accessed January 22, 2008).

⁴² See 2007 Golden Bear Omnibus Survey.

was high. Importantly, however, the incidence of regret was lower when short notices were received before program installation.

F. OTHER FORCES ALSO PREVENT CONSUMERS FROM SUCCESSFUL PRIVACY PROTECTION

Beyond the issues of whether consumers read and comprehend privacy policies, individuals' ability to make marketplace privacy decisions that reflect their needs is hampered by several factors. Incomplete information is a major difficulty. Even when they read privacy notices and EULAs, consumers have trouble evaluating the consequences of disclosing the bundles of information that companies say they are taking. Consumers have difficulty assessing and valuing certain privacy risks, which makes their decisions seem unpredictable, even random. Sometimes risks become known only after a security breach or privacy invasion.

Moreover, while many consumers are certainly aware of many privacy risks, they may not be well informed about the magnitude of these risks in certain circumstances. Acquisti and Grossklags report, for example, that 73% of respondents in their survey underestimated the risk of becoming a victim of identity theft.⁴³

Adding to the problem of incomplete information is the challenge of grasping the abilities of technologists to take seemingly innocuous items of information and link them in new, unexpected ways. For example, when asked, "Imagine that somebody does not know you but knows your date of birth, sex, and zip code. What do you think the probability is that this person can uniquely identify you based on those data?", 68.6% answered that the probability was 50% or less (and 45.5% of respondents believed that probability to be less than 25%). According to Carnegie Mellon University researcher Latanya Sweeney, however, 87% of the US population may be uniquely identified personally through a 5-digit zip code, birth date, and sex. To expect individuals to foresee such possibilities is unreasonable.⁴⁴

⁴³ Acquisti and Grossklags, *Privacy and Rationality*.

⁴⁴ Ibid., 24.

Even if individuals have access to complete information about privacy risks and modes of protection, they might not be able to process enough data to formulate a rational privacy-sensitive decision. Human beings' rationality is bounded, which limits our ability to acquire and then apply information. Furthermore, consumers are busy and experience many demands on their attention. They cannot be expected to be familiar with all the vagaries of technologies, e-commerce, and evolving business practices.

G. CONSUMERS ARE LIMITED IN THEIR ATTEMPTS TO PROTECT THEIR INFORMATION

Evidence abounds that consumers do try to protect their privacy. Survey results released in June 2004 by Privacy & American Business found that two-thirds of Americans have taken some steps to protect their privacy.⁴⁵ In fact, 87% indicated that they had asked a company to remove their information from a marketing database; 60% decided not to patronize a store because of doubts about the company's privacy protections; and 65% had declined to register at an e-commerce site because of privacy concerns.⁴⁶ Among individuals that Westin has described as the "privacy unconcerned," 47% reported that they engaged in four out of seven identified privacy-protecting behaviors, while 65% of the "privacy pragmatists" had engaged in these behaviors.⁴⁷

Situational characteristics can reduce consumers' efforts to protect their information. For example, Spiekermann, Grossklags, and Berendt observed 171 study participants while they shopped online, specifically when they interacted with an anthropomorphic sales advisor. By answering questions posed by the advisor, study participants could receive recommendations about products. The advisor also asked questions that were highly intrusive of privacy or that requested irrelevant information. Participants could simply have refused to respond to these questions, thereby protecting themselves against potential threats. However, regardless of the strength of the participants' self-reported privacy preferences, their actual responses

⁴⁵ Privacy & American Business, "New National Survey on Consumer Privacy Attitudes to be Released at Privacy & American Business Landmark Conference," news release, June 10, 2004.

⁴⁶ Ibid.

⁴⁷ Westin, "Social and Political Dimensions of Privacy," 445.

to the advisor revealed much more information than their self-reported preferences predicted, even among the “privacy-concerned” individuals. These results demonstrate the power of interactive marketing techniques to lead even privacy-motivated consumers to behave in ways that appear contradictory to their stated preferences.⁴⁸ The similarity between the behavior of the “unconcerned” participants and the behavior of participants who claim to be highly concerned about privacy suggests that Westin’s dichotomy may be less useful than previously thought in capturing the nuances of consumers’ attitudes on privacy.

Further evidence that we need a more differentiated understanding of protection behaviors is provided by Acquisti and Grossklags.⁴⁹ They found that at least 75% of the consumers did adopt at least one strategy or technology, or otherwise took some action, to protect their privacy, such as interrupting purchases before entering personal information or providing incorrect information in website forms.⁵⁰ However, they also found that use of specific technologies was consistently low across the sample population.⁵¹ For example, 67% of respondents never encrypted their email, 82% never put a credit alert on their credit report, and 82% never removed their phone numbers from public directories.⁵²

Other findings suggest that while people would like to protect their privacy, and try to at the most basic levels, a large proportion of these people do not have the knowledge necessary to move beyond the very basics of privacy-protective behavior. Before concluding that people do not put a credit alert on their credit report because they are lazy or uncaring, recall the Annenberg survey finding that 66% do not know the name of a credit agency and 76% do not correctly respond “false” to the statement, “the Federal Trade Commission will correct errors in credit reports if it is shown proof of the errors.”

⁴⁸ S. Spiekermann, J. Grossklags and B. Berndt, “E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior,” in *Proceedings of the 3rd ACM Conference on Electronic Commerce*, (New York: ACM Press, 2001), 38–47. Also available online at http://people.ischool.berkeley.edu/~jensg/research/paper/grossklags_e-Privacy.pdf.

⁴⁹ Acquisti and Grossklags, *Privacy and Rationality in Individual Decision Making*, 26–33.

⁵⁰ Ibid.

⁵¹ Ibid.

⁵² Ibid.

In the online environment, the complexity of privacy-protecting actions increases, and thus the likelihood that Americans perform them decreases substantially. The 2003 Annenberg survey asked American adults who use the Internet at home if they performed certain activities in relation to controlling their information online; 65% said that they have erased unwanted cookies at least once. This finding is consistent with the finding that a clear majority of the sample—59%—was aware of what cookies do; people know that when they go online, sites collect information on them even if they do not register. The percentage applying other privacy tools drops steeply, however. Only 43% said that they have used filters to block unwanted email, 23% said they have used software that looks for spyware, and 17% said they have used anonymizers—“software that hides your computer’s identity from websites that they visit.”

IV. WHAT THE FTC MUST CONFRONT IN THE NEXT DECADE

A. AMERICANS’ CONTINUING CONCERNS AND CONFUSIONS ABOUT INFORMATION PRIVACY

Research indicates that American consumers care deeply about information privacy and worry that it is not well protected. It also reveals that great majorities of American consumers do not grasp basic facts about companies’ data collection practices, do not know the laws that govern data protection, do not read or comprehend the notices that are supposed to explain data practices and afford privacy choices, and are confronted with many social and psychological factors that undermine their ability to protect their privacy during marketplace transactions.

Most fundamentally, research indicates that a large majority of American adults believe that the existence of a “privacy policy” on a website indicates some level of substantive privacy protection for their personal information. The finding is not an aberration. Two major national surveys performed two years apart, in 2003 and 2005, revealed virtually the same percentage of Americans—almost 60%—believed that “when a website has a privacy policy, that means it will not share information about them with other websites or companies.”⁵³ In the 2005 survey, where the statement was presented in true/false

⁵³ Turow, *Americans and Online Privacy*, 4; Turow, Feldman and Meltzer, *Open to Exploitation*, 20.

form, 59% incorrectly said the statement was true and an additional 16% said they did not know if it was true or false.⁵⁴

Because American consumers mistakenly believe that a “privacy policy” indicates a level of substantive privacy protection, they do not read them. The failure to read privacy policies leaves consumers unaware of data practices such as data-mining and allows a wide range of practices that are inconsistent with consumer expectations to avoid consumer scrutiny.

Under the Federal Trade Commission’s notice and choice regime, the operating assumption is that people will make good choices if they are provided with good information. Our studies have found that Americans do not have good, i.e., full and understandable, information about data practices that affect their privacy.⁵⁵ More significantly, even if full and understandable information is provided in a short format, consumers retain the belief that the mere invocation of the term “privacy policy” creates a baseline set of protections for their information. That belief, along with other cognitive biases, limits the number of consumers who read and act on such privacy notices. If a website contains a privacy policy that states it will reveal users’ data to affiliates or other companies without the users’ permission, then the privacy of consumers who stop reading once they see that a privacy policy exists is undermined.

B. THE CURRENT NOTICE-BASED APPROACH HAS CONSEQUENCES FOR THE SECURITY OF THE NETWORK ITSELF

Consumers’ basic misunderstanding of the purpose of privacy policies is one of many misconceptions that contribute to confusion in the online marketplace. When consumers do not read, or read but cannot understand, privacy notices and EULAs on websites and software, they may unwittingly install malicious programs that exploit consumer machines to the detriment of the entire Internet. Unless “privacy policies” provide some baseline privacy protections, the notice-based privacy regime will continue to unintentionally lead consumers to “consent” to invasive program installations and other practices. By doing so, they lower the security protections of the entire network, not just their own computers.

⁵⁴ Turow, Feldman and Meltzer, *Open to Exploitation*, 15.

⁵⁵ See Turow, *Americans and Online Privacy*; Turow, Feldman and Meltzer, *Open to Exploitation*.

One case in point is the 2005 wide-scale installation of a “rootkit” by purchasers of music CDs.⁵⁶ In an attempt to control the distribution of songs on the CD, Sony bundled a program that ran silently in the background and opened many computers to security vulnerabilities. Similarly, spyware, even if “consensually” installed pursuant to a EULA, can allow millions of computers to be controlled by others. This allows bad actors to create “botnets,” e.g. zombie networks of consumers’ computers, which can be remotely directed to engage in denial-of-service attacks and other malicious acts.

C. THE NEED TO ADOPT THREE POLICIES TO SUPPORT INFORMATION PRIVACY

To advance privacy, the Federal Trade Commission should take the following three steps:

1. THE FTC SHOULD POLICE THE TERM “PRIVACY POLICY”

Two national surveys by the Annenberg Public Policy Center revealed that to a majority of American consumers, “privacy policy” carries a particular meaning: that a website will not disclose personal information to others without the consumer’s permission. While many websites begin their privacy policies with the claim that “your privacy is important to us,” many of these same policies disclose further down that the websites collect quite a bit of the information from their users and often do share the information with affiliates, marketers, or other entities. Note, too, that information-sharing agreements with third parties generally are under no legal requirement to be disclosed; there is no other source for this omitted information. The result is a situation where consumers assume that the privacy policy label indicates that the site will not share data, whereas the opposite may be true and the policy may or may not state what is done with the information.

Given consumers’ expectations, the use of the term “privacy policy” absent some baseline privacy protections, ought to be considered deceptive. The Commission evaluates potentially deceptive marketing communications to consumers based upon

⁵⁶ Deirdre K. Mulligan and Aaron K. Perzanowski, “The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident,” *Berkeley Technology Law Journal* 22 (2007): 1157.

whether the representation is “likely to mislead reasonable consumers under the circumstances. The test is whether the consumers’ interpretation or reaction is reasonable.”⁵⁷ The FTC’s guidance specifies that communications should be judged upon “the basis of the net general impression conveyed . . .”⁵⁸ The Policy Statement on Deception advances five model questions for evaluating a representation: how clear is the representation, how conspicuous is any qualifying information, how important is the omitted information, do other sources for the omitted information exist, and how familiar is the public with the product or service?⁵⁹

Given consumer expectations, the use of the label “privacy policy” by websites that share information about their users without user permission is deceptive. First, surveys demonstrate that reasonable consumers believe that the mere presence of a privacy policy means that substantive protections are in place to prevent the sharing of their information. Websites’ top-level assertions about privacy are often very clear; sites abound with privacy seals and claims that “your privacy is important to us.” As such, “privacy” is used as a marketing tool, a type of quality representation that consumers find meaning in and rely upon. Qualifying information, by contrast, is buried within privacy policies in the fine print. As we have shown, this qualifying information is often not understandable and often goes unread by consumers who presume that the policies extend many rights, and thus are not necessary to read.⁶⁰ In cases where sites share information without consumer consent, therefore, the use of the term “privacy policy” is deceptive under FTC guidelines.

The Federal Trade Commission should rule, then, that websites using the label “privacy policy” are deceptive unless those sites promise not to share information about their users without their permission. While sites that engage in such sharing without user permission should be required to make disclosures, they should not be allowed to refer to such disclosures as “privacy policies.”

⁵⁷ James C. Miller III, *FTC Policy Statement on Deception* (October 14, 1983). Also available online at <http://www.ftc.gov/bcp/policystmt/ad-decept.htm>.

⁵⁸ Ibid.

⁵⁹ Ibid.

⁶⁰ See Turow, *Americans and Online Privacy*; Turow, Feldman and Meltzer, *Open to Exploitation*.

2. PRIVACY MECHANISMS SHOULD BE VETTED BY USABILITY AND OTHER EXPERTS

Currently, notices are written to satisfy lawyers. The notices do not help consumers make privacy choices that reflect their privacy interests. If the FTC wants consumers to make smart decisions on privacy, then experts in usability and other areas need a seat at the table. Such experts need to help craft privacy-protecting mechanisms. Consumers would benefit from the involvement of experts in usability and psychology in designing notices and other privacy mechanisms. Research at the Samuelson Clinic and elsewhere is beginning to identify the features that can improve the chances that consumers read, comprehend and act upon privacy notices in a manner consistent with their needs and expectations. The FTC needs to avail itself of that research and the expertise behind it.

3. THE FTC SHOULD SET BENCHMARKS FOR SELF-REGULATION

In announcing the 2006 Tech-ade hearings, Chairman Majoras asked:

[W]hat have we learned over the past decade? How can we apply those lessons to what we do know, and what we cannot know, as we look to the future? And how can we best protect consumers in a marketplace that now knows no bounds, that is virtual, 24-7, and truly global?⁶¹

The FTC would be better equipped to evaluate what it has learned about self-regulation if it had adopted a reasonable recommendation offered by Privacy Rights Clearinghouse Executive Director Beth Givens in 1996—that the agency set performance benchmarks for self-regulation.⁶² Without benchmarks, self-regulation and regulation, for that matter, have no clear metrics for measuring success. Accordingly, we recommend that the FTC define clear benchmarks for its privacy initiatives—educational, regulatory and self-regulatory—and evaluate its approach against those benchmarks between now and 2016.

⁶¹ See Majoras, Anti-Spyware Coalition.

⁶² FTC, *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, n. 156 (Dec. 2006).

V. CONCLUSION

The next decade will bring new technologies that will be able to extract far more information from and about Americans than was previously possible.⁶³ These technologies will raise new and complex privacy issues. The FTC should plan its activities for the next decade based on a reasoned assessment of its policy initiatives over the last ten years. While some progress has been made, it is clear that consumers remain unable to fully effectuate their privacy rights in the marketplace. Providing consumers with more information about data practices has not led to greater consumer confidence or to a rich marketplace of privacy options for consumers. It is clear that if the FTC continues to pursue a market-based approach, additional interventions are necessary to ensure that consumers are not misled and have straightforward information available that facilitates privacy choices.

⁶³ Turow, *supra* note 1.



Internet privacy and institutional trust: insights from a national survey

JOSEPH TUROW
MICHAEL HENNESSY

Annenberg School for Communication, University of Pennsylvania, USA

Abstract

What does the US public believe about the credibility of institutional actors when it comes to protecting information privacy online? Drawing on perspectives of environmental risk, this article addresses the question through a nationally representative telephone survey of 1200 adults who go online at home. A key result is that a substantial percentage of internet users believes that major corporate or government institutions will both help them to protect information privacy and take that privacy away by disclosing information to other parties without permission. This finding and others raise questions about the dynamics of risk-perception and institutional trust on the web.

Key words

government • home • internet • marketing • media • online
• privacy • risk

The internet is an important crossroads where institutions in US society communicate with members of the public. Marketers, media firms, other businesses and governments interact with online users in ways that involve retrieval of information about the users' actions, interests and personal characteristics. Yet surveys conducted over the past few years indicate consistently that the majority of American adults are worried about websites

taking information from them without their knowledge as well as sharing data about them with other organizations. Resisting advocacy group demands for government regulation, major organizations with stakes in the online world have insisted that self-regulation works. Through their trade associations, they have set up models for privacy policies and information exchange. Publicizing these guidelines, they argue that members of the public should trust them to respect people's information wishes as well as to help people learn to protect their information privacy.

Policymakers have been wrestling over the acceptability and credibility of these approaches to members of the public. The present study addresses the issue from a perspective of environmental risk and the public's trust of institutions. Sociologists of risk point out that in the contemporary era, hazards in the environment are increasingly diffused rather than directly visible. They note that the uncertainty invites battles over the reality of the risks and their causes. From this perspective, the issue of internet privacy can be seen as a struggle over the public's construction of diffused risks, what institutional actors are to blame for them and which to trust to reduce them. Although the topic of institutional blame and trust lies at the heart of discussions of internet policy, researchers have not addressed it with the depth and complexity that it deserves.

That is the aim of this article. It explores views on internet privacy and institutional trust through a nationally representative telephone survey of 1200 adults who go online at home. A key finding is that a substantial percentage of internet users believes that major corporate or government institutions will both help them to protect information privacy and take that privacy away by disclosing information to other parties without permission. This and other results raise questions about why members of the public might agree simultaneously with clashing beliefs about institutional actors' roles in risk-creation and risk-reduction.

RISK AND TRUST ONLINE

At the beginning of 2004, about 57 percent of US households were connected to the internet (Horriigan, 2004). Around that period, Americans were going online more than one hour a day (Cole et al., 2003: 19). Moreover, a large body of literature was indicating that the internet was becoming integrated into many common societal activities. As Pew Project director Lee Rainie noted about the internet as early as 2001, 'every day it looks more and more like the rest of America' (Pew Internet & American Life Project, 2001).

While the online experience has been integrating deeply into US life, expressions of concern about the violation of information privacy have proliferated. Perhaps because of media coverage of the topic (Turow et al., 2000), surveys conducted over the past few years indicate that the majority of American adults are worried that websites collect information from them without their

permission and share data about them with other organizations. For example, Alan Westin's Privacy and American Business consultancy found that in 2002, 56 percent of US adults believed that most businesses did not 'handle personal information they collect in a proper and confidential way'. In 1999, 34 percent had answered that way. Westin concluded that higher percentages of Americans had become sensitive to privacy issues online; in 2001 he said that only 8 percent were 'unconcerned' about the issue (Westin, 2003: 290).

The sociology of risk and trust

In trying to understand the social dynamics behind this broadly recognized US public concern about internet privacy, it is useful to link these worries to the literature about the relationship between risk and trust. As Oscar Renn and colleagues noted, risk can be conceived as both 'a potential for harm' and the 'social construction of worry' (2000: 35). Their dual definition reflects that although an actual physical reality of danger may exist around a particular phenomenon, the way that people understand a potential danger plays a large role in determining its centrality as a topic within their society. Sociologists of risk point out that the notion of a hazardous environment has grown in the late modern age, as media and interpersonal sources make people aware of the dangers posed to them by industrial activities. Examples include hearing that genetically-modified crops are unhealthy for humans and animals to eat or that cars and factories contaminate the air to the point that they may cause lung problems. The common thread among such dangers is that they are not visible to the general population; belief in their existence is (or is not) justified by the reports of dueling experts. Maurie Cohen notes that without any means to definitively ascertain these phenomena the public argument about environmental dangers becomes 'a battleground over cultural symbols. In choosing sides, ordinary people must judge the credibility of expert institutions and contrast these interpretations with their own experiences' (Cohen, 2000: 25).

Cohen's idea of credibility is close to Fukuyama's definition of trust: belief that an actor is involved in 'regular, honest and cooperative behavior, based on commonly shared norms' (Fukuyama, 1996: 26). It is likely that whether or not people find assurances by particular institutional actors trustworthy regarding safety would depend on the extent to which people believe that those actors understand public norms about risk, and cooperate to let society know honestly how 'the facts' of potential dangers, as they know them, match the norms. Lack of institutional trust can be socially corrosive, particularly if it is generalized to a wide range of organizations. William Freudenberg (2000) emphasizes that during the past century there has been a dramatic growth of societal interdependence. As the process has advanced, he says:

There has been a substantial decline in the ability of the broader society to assure that its specialists do indeed serve the interests of the larger collectivity and that its 'responsible officials' do indeed act responsibly. (2000: 108)

Debates about online risk

In the USA, marketers, media and government specialists use people's information in a broad gamut of ways and with varying concerns for how far the data travel. Although many of these emphasize personally identifiable information, not all of them do. Tracking people anonymously still can lead to useful targeting for marketers. An important example is the Claria Corporation, which places its 'Gator' tracking files into people's computers when they download free software such as the Kazaa file-sharing program.

The idea that internet users' electronic actions are becoming increasingly transparent has alarmed some. Many critics emphasize the danger that some kinds of personal information may fall into the hands of companies or people who could take advantage of the consumer (see for example, Schwartz, 2003). Others note that sites' application of email addresses in the service of marketing has helped the proliferation of unwanted email on the web, adding to a spam epidemic which has internet users and their service providers steaming (Hansell, 2003). In the wake of the anti-terror Patriot Act of 2001, critics also worry that various government agencies will expand the tracking and generalizing about consumers on the web that had until recently seemed to be the domain of business (Jesdanun, 2003). They point out the profound damage that errors or names on suspect lists can cause individuals and families.

Concerned about what they agree are substantial risks to personal data that citizens incur when going online, privacy advocates have urged a variety of approaches to online information-gathering activities. They have encouraged technological solutions that will allow web users to protect their information.¹ They have lobbied for legislation that would stop companies from collecting certain forms of information. And they have demanded that online actors be required to tell consumers about the extent to which, and way in which, they collect and exploit people's electronic information.²

Marketers and commercial websites have resisted the possibility of government edicts and offered self-regulation as a model. The Direct Marketing Association, the Association for Internet Marketers and the Internet Advertising Bureau are among the organizations that represent a variety of information-hungry stakeholders such as major advertisers, banks, credit card companies and software companies. They have set up models for privacy policies and information exchange which, they argue, can ensure that consumers will be able to control whether websites can share their information about them. For example, the Direct Marketing Association (2003) notes 'the DMA Promise' in its online 'helpful guide' to consumers: 'The Direct Marketing Association Privacy Promise is an assurance to consumers that US Marketers who are DMA members will use your information in a manner that respects your wishes'.

Such language is the rhetoric of trust. The Direct Marketing Association statement describes an approach consistent with Fukuyama's definition of trust as 'regular, honest and cooperative behavior, based on commonly shared norms'

(1996: 26). Companies that support self-regulation online argue that members of the public will agree that the companies are credible sources for helping them learn how to protect their privacy on their sites. In Freudenberg's (2000) terms, they contend that they are carrying out their responsibilities with the degree of vigor necessary to merit societal trust.

Do Americans believe that? To what extent does the US public perceive that institutional actors who are regularly involved with the internet are likely to help them learn how to protect their privacy? Alternatively, to what extent does the public think that these actors are likely to share their information with others without their knowledge? Does personal experience – expertise with the web, time online or a bad privacy experience on the internet – predict more or less trust of institutional experts than that held by most Americans who are online? Although answers to these questions are crucial to establishing benchmarks of institutional trust regarding this emerging medium, researchers have not addressed them. Our national survey was designed to do this.

METHOD

Survey

The survey instrument we created was implemented by the International Communication Research (ICR) survey research firm from 30 January to 21 March 2003. Telephone interviews, which averaged 20 minutes, were completed with a nationally representative sample of 1200 adults aged 18 and older who said responded 'yes' when asked 'Do you use the internet at home?' Respondents were selected using a random digit dial sample to screen households for adults age 18 or older who use the internet at home; of the households that we telephoned, 53.3 percent had at least one household member who met our eligibility requirements – a percentage similar to the 2001 Consumer Population Survey. Among those households, the percentage of eligible individuals who completed an interview was 66.4 percent. The data were weighted by age, education and race to the 2001 Consumer Population Survey, which asked adults aged 18 or older questions similar to that used in the internet privacy study to ascertain internet use at home.³

Interviews

The interviews explored demographic, attitudinal, knowledge and activity patterns related to the internet. Among these, respondents' own assessment were solicited of their abilities to 'go online or navigate the internet', that is, whether they considered themselves 'beginners', 'intermediate users', 'advanced users' or 'expert users'. Other questions led to the development of six new variables: three behavioral, two attitudinal and one concerned with regulatory policy. In addition, two scales were developed to measure the respondents' trust in the online world's major institutional actors. We expected to find that the behavioral, attitudinal and policy variables would be

associated with the two institutional trust scales to predict people's disposition for personal action and government regulation in the name of privacy.

The behavioral measure, 'active wariness', brings together activities where the respondents showed an active concern about web privacy. They were asked if they: 'Argued with a family member about personal or family information that the person released to a chatroom or on email' (2.2% said yes); 'Had an incident where you worried about something a family member told a website' (1.7% said yes); 'Chose not to register on a website because it asked you for personal information to get into the site' (34.6%); 'Talked with a family member about how to deal with requests for information from websites' (12.4%); and 'Searched for instructions on how to protect information about yourself on the web' (5.9%).

The behavior variable, 'disclosing behavior', addressed whether the respondents gave out information on websites (the range of responses was 'always', 'sometimes', or 'never'; these items were recoded to 'always' versus the other values). The behaviors and their prevalence were: 'Give mail address' (12.3%), 'Give email address' (19.2%), 'Give real name' (33%) and 'Give age' (47.8%). The variable 'protecting behavior' was computed from a set of dichotomous items asking about the respondent's behavior in preventing information disclosure through the following actions: 'Used software that looks for spyware on your computer' (22.8%); 'Used software that hides your computer's identity from websites that you visit' (17.8%); 'Used a filter program to block unwanted emails' (44.4%); and 'Erased all or some of the unwanted cookies on your computer' (67.9%).

The two measures of attitudes related to 'fear of disclosure' and 'trust of the internet'. The 'fear of disclosure' variable was constructed from seven five-point Likert items (from strongly agree to strongly disagree) which reflected a concern about lack of control over personal information on the web: 'I am more concerned about giving away sensitive information online than about giving away sensitive information any other way'; 'I should have a legal right to know everything that a website knows about me'; 'My concern about outsiders learning sensitive information about me and my family has increased since we've gone online'; 'I look to see if a website has a privacy policy before answering any questions'; 'Teenagers should have to get their parent's consent before giving out information online'; 'I sometime worry that members of my family give information they shouldn't about our family to web sites'; and 'I am nervous about websites having information about me'.

The 'trust of the internet' variable tapped into the respondents' general belief in the online world's credibility regarding privacy. It was constructed from two five-point Likert items (strongly agree to strongly disagree): 'I trust websites not to share information with other companies or advertisers when they say they won't'; and 'When a website has a privacy policy, I know that the site will not share my information with other websites or companies'.

The 'regulation' variable measured peoples' sense of the effectiveness of different forms of possible regulation of the internet regarding privacy. It was constructed from three items concerning the respondents' perception of the effectiveness of potential laws that would hinder companies' ability to collect personal information from online users without their consent. The items were: 'A law that requires website privacy policies to have easy-to-understand rules and the same format'; 'A law that requires companies that collect personal information online to help pay for courses that teach internet users how to protect their privacy online'; and 'A law that gives you the right to control how websites use and share the information they collect about you'.

When it came to measuring the respondents' trust in the online world's major institutional actors, complexity in response was allowed for by taking two routes, one positive and the other negative. The positive expression of trust was the belief that an institutional actor would help or teach the respondent to protect personal information online. We asked each person:

Please think about your ability in the next five years to control personal information collected about you online. On a scale of 1 to 5, with 5 being the most important and 1 being the least important, how important a role will [insert name of institution] play in helping or teaching you to protect your personal information online?

The major institutional actors selected were: 'Your internet service provider', 'Banks or credit card companies', 'Major advertisers', 'Microsoft Corporation', 'Privacy protection software companies' and 'The government'. These were presented in random order across the respondents. The alpha for the six-item scale was .79 (scale mean=3.49, $SD=.94$, range=1–5), a high score that indicates its component statements were internally consistent.

The negative expression of trust was a belief that an institutional actor would release or share information about the respondent without the person's knowledge or consent. We phrased the 'institutional disclosing' question by asking each person:

On a scale of 1 to 5, with 5 being the most important and 1 being the least important, how likely will [name of institution] be to release or share information about you by accident or on purpose without your knowledge or consent?

The institutional actors were identical to the previous list and were ordered randomly across respondents. The alpha for the six-item scale was also a high .79 (scale mean=3.29, $SD=.95$, range=1–5).

Multivariate analysis

For multivariate analysis, structural equation modeling and the AMOS program were used (Kline, 1998a). Measurement modeling (Kline, 1998b) was employed to investigate the factor structure of the relationships between the

information-protecting and information-disclosing tendencies of the six internet-related institutional actors. Seemingly unrelated regression (Wonnacott and Wonnacott, 1986) was used to identify the important predictors of the institutional belief outcomes. To assess the fit of simultaneous equation models, the χ^2 test as well the Goodness of Fit Index (GFI) and the Tucker-Lewis Index (TLI) were used.⁴

RESULTS

Respondents' demographics

The sample comprised 49 percent of men and 51 percent of women; 77 percent designated their ethnicity as white, 13 percent were black or Hispanic, 7 percent gave their ethnicity as 'other' and 4 percent did not respond. One-third of the respondents were aged 18 or younger, 24 percent ranged from 35 to 44, 21 percent from 45 to 54, 11 percent from 55 to 64 and 8 percent were aged 65 or older (3% did not respond). More than half (56%) were parents of children under 18. Fully 39 percent graduated from college or higher, 22 percent attended some college, 32 percent graduated from high school or technical school and 7 percent did not graduate from high school. Although a substantial percentage (26%) said their household brought in more than \$75,000 annually, an accurate estimate of the sample's income distribution is difficult because one-fifth of the respondents did not want to reveal it.

Almost half the adult population (46%) who use the internet at home had been going online from home for fewer than five years. Of the adults, 13 percent have been online from home for five years and 36 percent have been online for six years or more; 4 percent 'don't know'. The great majority of adults who used the web at home ranked themselves in the middle (intermediate or advanced) rather than lowest or highest range (beginner or expert) of abilities when it comes to navigating the internet; 14 percent considered themselves beginners and 13 percent called themselves experts, while 42 percent considered themselves intermediates and 30 percent said that they were advanced.

Online attitudes and behaviors

Where do these people fall when it comes to the measures of attitudes, behaviors and institutional trust that we noted? As the measures of the 'trust in the internet' in Table 1 indicate, when it comes to trusting the internet as a space where websites will protect information, the respondents are divided: some find website assurances credible and others do not. Nevertheless, these same people acknowledge a broad sense of risk about internet privacy; the average score on the five-category 'fear of disclosure' variable is a fairly high 3.757.

Yet the respondents' reported behavior does not mesh consistently with the fear. Their approach to giving websites information about themselves does reflect caution (as seen in a low disclosing behavior mean). Despite this wariness, the respondents indicated a low use of computer programs that can

• Table 1 Sample statistics and correlation matrix of all variables ($N=1032$)

VARIABLE MAX	N	MEAN	SD	MIN	MAX
Active wariness	1032	.590	.831	0	5
Fear of disclosure	1032	3.757	.696	1.167	5
Internet trust	1032	3.021	1.307	1	5
Self-repeated skill level	1032	2.504	.879	1	4
No. of years online	1032	5.671	2.088	1	8
Efficacy of regulation	1032	3.133	.650	1	4
Respondents' information-disclosing actions	1032	1.132	1.212	0	4
Respondents' information-protecting actions	1032	1.563	1.218	0	4
Institutional protecting scale	1032	3.281	.946	1	5
Institutional disclosing scale	1032	3.483	.925	1	5

protect their information from leaving their computers (as seen for ‘protecting behavior’). In fact, most of the respondents were not even high on active wariness, the measure of their general discussion and search for ways to protect their information privacy.

Perhaps because of their high concern about information privacy but relatively low involvement in specific protecting behaviors or attempts to learn about them, the respondents tended to like regulations that would force online firms to help internet users to protect their privacy. The regulation index mean of 3.13 out of 4 reflects that 86 percent of the respondents believed ‘a law that requires website privacy policies to have easy-to-understand rules and the same format’ would be somewhat or very effective; 84 percent agreed with the probable effectiveness of ‘A law that gives you the right to control how websites use and share the information they collect about you’; and 74 percent similarly endorsed ‘A law that requires companies that collect personal information online to help pay for courses that teach internet users how to protect their privacy online’.⁵

Conflict over institutional actors

The data indicate that adults who go online at home feel conflicted about whether key institutional actors – corporate or the government – will help them with their information privacy. A good way to see this is in Table 2, which presents a new variable merging the answers to the two sets of questions on each actor or set of organizations. If a respondent answered that the actor would be important in helping to protect information online

(a 4 or 5) and then said it would be unlikely to disclose information (a 1 or 2 on that variable), we considered that the person trusts the actor to help actively with information privacy. If a respondent answered that the actor was unlikely to help protect information (a 1 or 2) but then said it would be likely to disclose information (a 3 or 4), we considered that the person did not trust the institution to help actively with information privacy. If the person indicated that the actor was ‘unimportant’ with helping to protect information *and* unlikely to release it – or in the middle (a 3) on these issues – we considered that the respondent felt neither strongly trusting nor distrusting about the institution when it came to information privacy. Finally, if the respondent indicated that the institution would be important in helping to protect online information but then indicated that it was likely that the same institution would disclose personal information, we considered that person strongly conflicted.

Table 2 shows that with the exception of major advertisers, straight trust or distrust is not the mode when it comes to information privacy. Between one-third and half of the respondents simply sit on the fence, not believing that they can trust or distrust an institutional actor when it comes to privacy. Even more interesting is the substantial percentage of strongly conflicted people: between one-third and one-quarter are conflicted about how these key institutions of the digital world relate to their privacy. They seem to feel that while institutional actors will help them to control their information online, those same actors (or others parts of them) will take that information privacy away.

- Table 2 Trust/distrust that institution will help to protect information online and not release it without knowledge or consent

	DISTRUST %	TRUST %	NEITHER %	CONFICTED %
Major advertisers (N=1198)	40	4	34	23
Microsoft (N=1189)	15	12	50	23
The government (N=1191)	17	13	43	26
Banks/credit card companies (N=1198)	16	18	35	31
Internet service providers (N=1196)	16	18	35	31
Makers of privacy protection software (N=1188)	8	25	45	23

The different N for each variable reflects when respondents said ‘don’t know’ or ‘refused’ on both ‘protect’ and ‘release’.

A look at the mean answers of the institutional actors on the individual ‘protect’ and ‘disclose’ reinforces the points in Table 2 and extends them. It turns out that major advertisers were collectively the only institutional actor with a mean below 3 on ‘protect’, while makers of privacy protection software were collectively the only actor with a mean below 3 on ‘disclose’. Microsoft, the government, banks/credit card companies and internet service providers all fall between 3 and 4 (that is, in the ‘important’ and ‘likely’ range) on both ‘protect’ and ‘disclose’. On each of these four actors, the ‘protect’ means are higher than the corresponding ‘disclose’ mean. Yet the differences, while statistically significant, are small – less than .5 in each case.

Taken together, the means and the cross tabulations indicate three related points. First, the respondents tend to rank the institutions as somewhat more important for protecting their information than having the likelihood to disclose it. Second, the generally small differences between the means of the two protecting and disclosing items by institutional actor reflect that when it comes to Microsoft, the government, banks/credit card companies and internet service providers, the proportions of respondents who see most of the actors as important for helping them to protect their information are not that different from the proportions who believe that it is likely that they will disclose their information without people’s knowledge or consent (for example, while 51% of the respondents said that the government would be important to helping to protect privacy, 44% said that it was likely that the government would disclose information about them). Third, a substantial proportion of the adult population that uses the internet at home says that institutional actors both will disclose and help to protect their personal information online.

Associations with conflicted institutional trust

A logical next question is whether any of the behavioral or attitudinal variables that were measured help to predict or explain this conflicted understanding of institutional actors. When correlated, the demographic variables noted earlier – gender, ethnicity, education, family income and parental status – show no patterned association with institutional trust. Table 3 presents a correlation matrix of all the previously described attitudinal and behavioral variables, with the institutional actors brought together in the institutional disclosing and institutional protecting scales.

Most of these significant correlations make sense. The respondents with higher online skills, for example, have lower fear of disclosure, presumably because they believe that their knowledge helps them to avoid organizations that eke personal information from web users. Similarly, we can suggest that higher skill associates with reduced trust because of greater awareness of the surreptitious behavior of websites and marketers. High skill levels presumably come with greater skepticism and so seem to attenuate the belief in the

• Table 3 Correlation matrix of all variables (N=1032)

RESPONDENT'S- INFORMATION DISCLOSING ACTIONS	ACTIVE WARRINESS	FEAR OF DISCLOSURE	INTERNET TRUST	SELF- REPORTED SKILL LEVEL	NO. OF YEARS ONLINE	EFFICACY OF REGU- LATION	RESPONDENT'S INFORMATION- DISCLOSING SCALE	RESPONDENT'S INSTITU- TIONAL PROTECTING ACTIONS	RESPONDENT'S INSTITU- TIONAL DISCLOSING SCALE
Fear of disclosure	0.2290	1.0000							
Internet trust	-0.0999	0.0416	1.0000						
Self-reported skill level	0.1014	-0.1249	-0.0423	1.0000					
No. of years online	0.0927	-0.0632	-0.0747	0.3532	1.0000				
Efficacy of regulation	0.0362	0.2564	0.0940	-0.0923	-0.1075	1.0000			
Respondent's information- disclosing actions	-0.0460	-0.1669	0.1182	0.0708	0.0747	-0.0325	1.0000		
Respondent's information- protecting actions	0.2369	0.0235	-0.0496	0.4219	0.1956	-0.0033	-0.0310	1.0000	
Institutional disclosing scale	0.0548	0.1354	-0.1377	-0.0855	-0.0306	0.0184	-0.0214	-0.0133	1.0000
Institutional protecting scale	0.0007	0.2308	0.1014	-0.0927	-0.1113	0.2103	0.0032	0.0381	0.1846

possibility of effective regulation of the access and distribution of personal information. Optimism about the effectiveness of regulations links to optimism that institutional actors will help people to protect their personal information; it is unrelated to the belief that the actors will disclose information without permission. Similarly, general internet trust is related positively to the information-protecting functions of institutional actors and negatively related to the information-disclosing ones.

However, three of the associations in the table defy easy understanding. One reflects what Table 2 shows: to a substantial proportion of US adults who go online at home, the importance of each institutional actor's role in protecting personal data is associated positively with the expectation that the actor will disclose personal information either by accident or on purpose. Table 3 mirrors that finding in the .1846 correlation between 'institutional disclose' and 'institutional protect', and pushes this odd finding further. It shows that the skill of participants and their fear of disclosure both associate with the conflicting attitudes that relate to institutional trust and disclosure. It is hard to understand why fear of disclosure is associated positively with both a trust in protection and a belief that the organizations betray that trust by disclosing information. Similarly, it is mysterious why self-reported skill is associated negatively with both a trust in protection and a belief that organizations betray that trust by disclosing information.

Testing the associations

In view of these hard-to-explain correlations, it might be suggested that the positive association between the two seemingly contradictory institutional scales is really due to one or another of the institutional actors reflected in the scale being differentially related to the variables in a way that is not evident. We might also worry that the correlation between the two institutional scales is the result of simple measurement error which obscures the true correlation (or lack of correlation) between the five items measuring institutional disclosing and institutional protecting.

Ruling out the second possibility – that of measurement error between the institutional variables – requires confirmatory factor analysis. It estimates the correlation between the two implied latent variables ('the importance of protecting information' and 'the likelihood of disclosing information') after adjusting for any measurement error. For each latent variable, the analysis used the responses to the question asked regarding each of the six institutional actors. The focus is the correlation between these two constructs.

The analysis found that the two key measures – the TLI and GFI – were excellent ($GFI = .969$ and $TLI = .944$). Moreover, the standardized regression coefficients relating the constructs to the indicators were, in all but two cases, a high .60 or larger.⁶ The correlation between the constructs was estimated to be .27, discernable from zero and larger than the correlation between the scale

values (.1846) shown in Table 3, which are not adjusted for measurement error. The finding indicates that the positive correlation between the scale values is not the result of measurement error.

To rule out the other possibility – that the strange relationship between the institutional scales is due to a specific institutional actor's strange relationship with the skill or fear variables – Table 4 looks at the correlation of each of the separate institutional domains with the 'fear of disclosing' and 'skill' variables. Note that in the case of each variable, the direction of the correlation with institutional protecting and institutional disclosing that we saw in the matrix remains for statistically significant correlations. This means that the relationships that 'institutional protecting' and 'institutional disclosing' have with 'fear of disclosure' and 'skill' are not the result of a fluke sensibility of respondents regarding one institutional actor. Rather, the relationships reflect the simultaneous operation of opposing expectations toward the major institutional actors with respect to personal data on the internet.

Regression analysis of the institutional belief items

These tests of association confirmed the validity of the seemingly contradictory correlations noted between institutional trust and disclosure. The final step was to investigate whether the curious associations with disclosure fear and skills continue to be seen when controlling for the other variables. The results are shown in Table 5. The rows of this table contain the results for the predictor variables and the columns contain the regression results for each institutional scale.⁷ The table indicates that 'active wariness',

- Table 4 Correlations of respondent's fear of disclosure and internet skill with the respondent's perception that the institutional actor will protect or disclose personal information

INSTITUTION	RESPONDENT FEAR OF DISCLOSURE*	RESPONDENT INTERNET SKILL*	RESPONDENT FEAR OF DISCLOSURE**	RESPONDENT INTERNET SKILL**
Internet service provider	0.1158	-0.0787	0.0935	-0.696
Banks/credit card companies	0.1512	-0.0236	0.0719	-0.1068
Major advertisers	0.1420	-0.0908	0.0896	0.0546
Microsoft	0.1686	-0.0982	0.1273	0.0030
Privacy protection software companies	0.1850	-0.0786	0.0939	-0.1263
Government	0.1401	-0.0503	0.0892	-0.0947

Entries are correlation coefficients. All bold italic entries are discernable from zero in value at the 95% confidence level or more.

*Correlation with the perceived likelihood that the specific institutional actor will protect personal information (N=1147–1197).

**Correlation with the perceived likelihood that the specific institutional actor will disclose personal information (N=1151–1197).

'disclosing behavior' and 'protecting behavior' do not by themselves predict whether adult home users of the internet believe that the institutional actors will help people to protect or disclose their information online. Time online is related to the decreasing belief that institutional actors will help to protect personal information. Internet trust and favoring regulation predict a belief that institutional actors will protect and not disclose. Having more self-reported skill also associates with the optimistic opinion that institutional actors will not disclose information without permission. Unlike in Table 3, when controlling for other variables, it does not associate positively with the pessimistic opinion that institutional actors will disclose information permission. Fear of disclosure, by contrast, still relates oddly to both. As in Table 3's correlation matrix, fear of disclosure associates positively with both institutional protecting and institutional disclosing.

DISCUSSION

Each of the significant relationships is provocative and invites further thinking and research on the dynamics of institutional trust. For example, it may seem logical that a greater number of years using the internet associates with a decreasing belief that the institutional actors' can be trusted to help people online to protect information. This might come about because people who have been online for some time may have become more knowledgeable about the surreptitious ways in which websites and internet marketers try to get information. It may seem logical also that having more skill links to a view that institutional actors will not disclose information without permission. It might be taken to mean that greater self-reported expertise means greater trust in the establishment. These two interpretations do not necessarily exclude each other. However, they do invite questions about

- Table 5 Results of seeming unrelated regression predicting institutional protecting and disclosing outcomes ($N=1032$)

PREDICTORS	INSTITUTIONAL PROTECTING SCALE	INSTITUTIONAL DISCLOSING SCALE
Active wariness	-.032	.022
Fear of disclosure	.260	.181
Internet trust	.046	-.107
Self-reported skill level	-.026	-.085
No. of years online	-.030	-.005
Efficacy of regulation	.208	-.015
Disclosing behavior	.029	.019
Protecting behavior	-.006	.006
Intercept	1.94	3.17
R ²	.0924	.045

Bold, italic coefficients are discernable from zero at the 95% level or more.

why skill should have a very different relationship to trust than time online does – especially when time online and skill are correlated significantly with one another (see Table 1). The finding deserves further investigation.

Yet it is Table 4's association of fear of disclosure with the opinion that institutional actors will both protect internet information and disclose it that raises the most interesting challenge to understanding. In so doing, it forces the positive correlation of users' beliefs in both institutional protection and institutional disclosure to the center of attention. The message here is that, irrespective of their background and beliefs (and especially if they are fearful about information privacy), adults who use the internet at home simultaneously tend to voice two potentially contradictory beliefs: that major institutional actors will work to help them protect their personal information online, yet disclose information to other parties without internet users' permission or knowledge.

From the standpoint of the sociology of risk, this study's findings highlight the idea that members of the public might agree simultaneously with clashing beliefs about the roles of institutional actors in risk-creation and risk-reduction. This, in turn, begs the question: why? One answer is that much of the public is simply confused by the battles over responsibility for the environmental risks regarding information privacy. The segment of the public which defines the privacy risk as high – that is, the more fearful part – is also more likely to be befuddled by advocacy groups' claims blaming various major institutional actors (e.g. major advertisers, Microsoft, even the government) and those actors' claims that they are part of the solution, not the problem. The other possible causal direction is that people who are confused by the claims and counterclaims might become more fearful and so define the privacy risk as high.

A very different explanation for the public's clashing beliefs about institutional actors' inconsistencies is that far from reflecting confusion, it mirrors a sophisticated public understanding of the institutions that they are being asked to trust or distrust. This view would argue that the government, banks and credit card companies, software manufacturers and even major advertisers are all large and variegated. Therefore, it is not at all unbelievable that parts of these organizations try to cultivate public trust by helping people to protect their information even while other parts take their information without consent. Accordingly, it is quite reasonable for people to state that the same institutional actors will help to protect information and will disclose it at the same time.

There is indirect support for the proposition that confusion rather than sophisticated understanding lies at the root of the public's clashing beliefs about institutional actors' trustworthiness. The support lies in the finding that the clash of protecting and disclosing scales is associated in Table 4 with increased fear, but not with variables that would seem to be linked to

relatively sophisticated understanding of the internet: skill, belief in regulation and (possibly) time online.

Widespread confusion about whether institutional actors will help to protect or disclose information may imply a kind of 'privacy paralysis' at the individual level. People may feel that reaching out to institutions for help in protecting their privacy on the web is either unnecessary or ineffective. Because it appears that the confusion is linked to feelings of fear and high risk, the effectiveness of attempts by institutional actors to educate the public credibly about internet privacy may well be at stake. These intriguing findings suggest that further research is needed into the dynamics of institutional trust on the web.

Notes

- 1 A technological solution that has gained industry traction during the past few years is the Platform for Privacy Preferences (P3P). Its goal is to provide a web-wide computer-readable standard manner for websites to communicate their privacy policies automatically to users' computers. In this way, visitors can know immediately when they get to a site whether they feel comfortable with its information policy. P3P 'user agents' are built into the Internet Explorer 6.0 and Netscape Navigator web browsers. An ingenious AT&T program called Privacy Bird is a P3P user agent that works with Internet Explorer 5.01 and higher. It displays a bird icon on the browser which changes color and shape to indicate whether or not a website's P3P policy matches a user's privacy preferences. The beta-version software is free (see <http://www.privacybird.com/>).
- 2 For a list of 'privacy, speech and cyber-liberties bills in Congress', see the Electronic Privacy Information Center's site: http://www.epic.org/privacy/bill_track.html
- 3 Our unweighted data was actually remarkably similar on these categories to the CPS as well as Centris and Pew Internet and American Life surveys from 2002. We used the CPS because of its huge number of respondents (143,000) and reputation as the gold standard for weighting.
- 4 Assessment of model fit for simultaneous equation models is a complex issue. Many measures exist that vary on different dimensions (Kenny and McCoach, 2003). A χ^2 test is used commonly to compare the predicted covariance matrix of the observed variables for the model with the actual covariance matrix: small values suggest only minor differences between the two matrices and therefore a good fit of the model to the data. However, χ^2 is usually augmented by other measures that are not a direct function of sample size and represent more of a continuous index of fit rather than a dichotomous decision rule (Hu and Bentler, 1995). Both the GFI and the TLI should be at least 0.90 to reflect an adequately fitting model (Kline, 1998a).
- 5 Despite broad support for all three policies, we did note an important difference in response to the third policy in relation to the first two. Compared to a law that would help them to learn how to control their privacy, substantially more of those interviewed (40% and 41%, respectively, compared to 28%) believed that legislation requiring easy-to-understand rules and the right to control information would be 'very effective'. Although the respondents did not dismiss the possibility that formal learning about privacy tools can help society to deal with information control, they seemed to believe that government and corporate action which helps them to learn straightforwardly what is going on is preferable.

- 6 Because the sample is so large, the chi square is not diagnostic of fit. We found it to be 200.9, $df=53$.
- 7 As expected, the two dependent variables should not be treated independently: the correlations of the residuals are positive (.175) and the correlation matrix of residuals had a significant off diagonal component, $\chi^2=31.47$, $df=1$, $p<.01$ (Breusch and Pagan, 1980).

References

- Bruesch T. and A. Pagan (1980) 'The Lagrange Multiplier Test and its Applications to Model Specification in Econometrics', *Review of Economic Studies* 47(1): 239–54.
- Cohen, M. (2000) 'Environmental Sociology, Social Theory and Risk', in M. Cohen (ed.) *Risk in the Modern Age*, pp. 3–31. New York: St Martin's Press.
- Cole, J., M. Suman, P. Schramm, R. Lunn and J. Aquino (2003) *Surveying the Digital Future, Year Three*. Los Angeles: UCLA Center for Communication Policy.
- Direct Marketing Association (2003) 'The DMA Privacy Promise', URL (consulted 8 October 2003): <http://www.dmaconsumers.org/privacy.html>
- Freudenberg, W. (2000) 'The "Risk Society" Reconsidered: Recreancy, the Division of Labor and the Social Fabric', in M. Cohen (ed.) *Risk in the Modern Age*, pp. 107–22. New York: St Martin's Press.
- Fukuyama, F. (1996) *Trust: the Social Virtues and the Creation of Prosperity*. London: Penguin.
- Hansell, S. (2003) 'It Isn't Just the Peddlers of Pills: Big Companies Add to Spam Flow', *New York Times*, 28 October, p. A-1.
- Horrigan, J.B. (2004) 'Broadband Penetration on the Upswing', Pew Internet & American Life Project, April, URL (consulted May 2004): http://www.pewinternet.org/pdfs/pip_broadband04.datamemo.pdf
- Hu, L.-T. and P.M. Bentler (1995) Evaluating Model Fit', in R.H. Hoyle (ed.) *Structural Equation Modeling: Concepts, Issues, and Applications*. pp. 76–99. Thousand Oaks, CA: Sage.
- Jesdanun, J. (2003) 'New Law Would Threaten Data-scrambling', *Chattanooga Times*, 1 April, p. 4.
- Kenny, D. and B. McCoach (2003) 'Effect of the Number of Variables on Measures of Fit in Structural Equation Modeling', *Structural Equation Modeling: A Multidisciplinary Journal* 10(3): 333–51.
- Kline, R. (1998a) *Principles and Practice of Structural Equation Modeling*. New York: Guilford Press.
- Kline, R. (1998b) 'Software Programs for Structural Equation Modeling: AMOS, EQS and LISREL', *Journal of Psychoeducational Assessment* 16: 343–64.
- Pew Internet & American Life Project (2001) 'More Online, Doing More', press release, 18 February, URL: <http://www.pewinternet.org/releases/release.asp?id=15>
- Renn, P., C. Jaeger, E. Rosa and T. Webler (2000) 'The Rational Actor Paradigm in Risk Theories: Analysis and Critique', in M. Cohen (ed.) *Risk in the Modern Age*, pp. 35–61. New York: St Martin's Press.
- Schwartz, J. (2003) 'Spyware Products: Crossing the Line; New Advances Alarm Privacy Experts', *International Herald Tribune*, 13 October, p. 1.
- Turow, J., J. Bracken and L. Nir (2000) *The Internet and the Family: the View from the Press*. Philadelphia, PA: Annenberg Public Policy Center
- Westin, A. (2003) 'Social and Political Dimensions of Privacy', *Journal of Social Issues* 59(2): 431–53.
- Wonnacott T. and R. Wonnacott (1986) *Regression: A Second Course in Statistics*. Malabar: Krieger Publishing.

JOSEPH TUROW is Robert Lewis Shayon Professor of Communication at the Annenberg School for Communication, University of Pennsylvania. His published research centers on internet privacy; new media, marketing and society and the internet and the family.

Address: Annenberg School for Communication, University of Pennsylvania, 3620 Walnut Street, Philadelphia, PA 19104, USA. [email: jturow@asc.upenn.edu]

MICHAEL HENNESSY is a senior statistician at the Annenberg Public Policy Center, University of Pennsylvania. His major interest is the integration of evaluation research and structural equation modeling.

Address: University of Pennsylvania, 3620 Walnut Street, Philadelphia, PA 19104, USA. [email: mhennessy@asc.upenn.edu]

BITS, BRIEFS AND APPLICATIONS

JOSEPH TUROW, MICHAEL HENNESSY, AND AMY BLEAKLEY

Consumers' Understanding of Privacy Rules in the Marketplace

Studies suggest the general structure of Web sites leads consumers away from demanding that online merchants take certain approaches to privacy as a condition for dealing with them. This article presents findings from a nationally representative survey showing that the absence of such a privacy marketplace can also be attributed to the public's incomplete knowledge of privacy regulations. Most respondents correctly understood that regulations regarding merchants' sharing information are domain specific. The respondents were only sporadically correct, however, regarding which domains have which rules. The study raises questions about the best approaches to education in the absence of a coherent national policy of privacy regulation.

While studies consistently show that individuals are apprehensive about companies learning personal information about them, people rarely, if ever, read privacy policies or take steps to protect personal information collected during online transactions (Graber, D'Allessandro, and Johnson-West 2002; Vila, Greenstadt, and Molnar 2003). As Nehf (2007) and Pitt and Watson (2007) note, consumers do not act as if there is an online market for privacy that leads them to choose privacy-enhancing Web sites over others. Nehf concludes that the problem lies in the structure of the online world. That is, the online marketplace is organized such that consumers drop their sensitivity toward protecting their information to "pursue other goals that render privacy less salient than other attributes" (Nehf 2007, 355).

The aim of this article is not to dispute that structural reasons play a role in explaining the failure of online consumers to inquire into sites' privacy

Joseph Turow is the Robert Lewis Shayon Professor of Communication at the Annenberg School for Communication, University of Pennsylvania, Philadelphia, PA (jturow@asc.upenn.edu). Michael Hennessy is a senior statistician at the Annenberg School for Communication, University of Pennsylvania, Philadelphia, PA (mhennessy@asc.upenn.edu). Amy Bleakley is a research scientist at the Annenberg School for Communication, University of Pennsylvania, Philadelphia, PA (ableakley@asc.upenn.edu).

Funds for this research were provided through the Annenberg Public Policy Center, University of Pennsylvania—Kathleen Hall Jamieson, Director.

The Journal of Consumer Affairs, Vol. 42, No. 3, 2008

ISSN 0022-0078

Copyright 2008 by The American Council on Consumer Interests

rules or to insist that sites not appropriate consumers' information. It is, rather, to present nationally representative survey findings suggesting that consumers' failure to protect their privacy online as well as offline can also be attributed to limited consumer's knowledge. Most respondents in the survey correctly understood that regulations regarding merchants' sharing information are domain specific. The respondents were only sporadically correct, however, regarding which domains have which rules. Our analysis highlights the dilemma of those who are looking for ways to encourage consumers to demand stronger privacy protections from marketers, and it suggests the importance of different levels of government involvement.

THE DILEMMA OF MARKETPLACE PRIVACY

In the United States, state and federal law generally leaves it up to individuals to learn the rules by which firms can use their personal information and to assess their privacy risks when dealing with merchants in the online and brick-and-mortar worlds. The lack of a cohesive regulatory scheme may be partly a result of inattention and neglect by regulators, partly a belief that the open market has historically been an American tradition, and partly because marketers and marketing advocacy groups have convinced regulators that important new businesses would be harmed by an aggressive stance on marketplace privacy (Turow 2006).

Within this regulatory context, Americans appear to have a contradictory approach to the issue. Some research shows that they are wary about the ways corporations use data about them. For example, a poll by the consultancy Privacy and American Business found that fifty-six percent of Americans in 2002 (vs. thirty-four percent in 1999) believed that most companies do not "handle personal information they collect in a proper and confidential way" (Westin 2003). At the same time, research shows that people behave in the online and offline marketplace as if they do not mind giving up information about themselves. Madden et al. (2007) at the Pew Internet and American Life Project found that "most internet users are not concerned about the amount of information available about them online, and most do not take steps to limit that information." Other research notes that people rarely read privacy policies or take steps to protect the information from marketers online—and that many are willing to give up information about themselves for gifts or other incentives (Hann et al. 2002; Jensen, Potts, and Jensen 2005; Jupiter Media Metrix 2002; Turow and Nir 2000).

One response to such findings has been to contend that "self-regulation works" and that government intervention on consumers' behalf could limit U.S. industries' competitiveness as well as the growth of the Internet.

Westin (2003) contends that despite their worries, consumers can correctly evaluate the costs and benefits of giving out personal information. Westin's argument suggests that consumers understand the privacy rules of the marketplace well enough to make informed decisions.

Some analysts disagree, arguing that the market in which consumers make choices is not an optimal one for information privacy. It is not a market where they can apply the skepticism they hold regarding collection of their information, learn the information they need to interact with merchants, and bargain with them about the data they want to give out. Pitt and Watson (2007) see the relationships between government data needs, corporate data needs, and technological change as making a privacy market impossible. Markets, they note, "require a certain level of stability to operate effectively" (374). While they take a broad view of forces militating against a unified privacy regime, Nehf (2007) focuses on the factors that lead people not to understand how to protect or negotiate their privacy. He notes that a variety of features companies build into Web sites discourage people from policing their online privacy. Among the factors he says discourage people from taking steps to protect their privacy are:

- obtuse and noncommittal privacy policies that make it difficult for people to know what information a site collects and how it will be used;
- voluntary privacy seals that do not properly signal strong privacy practices so that people will privilege those sites over others;
- lax accountability procedures on Web sites so that people have no idea when a privacy breach occurs; and
- companies falsely framing their Web sites as having strong privacy policies to take advantage of consumers' psychological predisposition to believe the claim to overcome the time constraints and high cognitive effort required to evaluate privacy policies.

Nehf's focus on Web sites resonates with literature not just in the area of online commerce but also in the areas of health and finance (e.g., Anton et al. 2003; Anton and Earp 2004; Goldman, Hudson, and Smith 2000). According to this perspective, consumers lack the knowledge or inclination to deal properly with privacy issues because of features of the online world and particularly aspects of Web sites. This structural view is persuasive, but partial. It emphasizes awareness of privacy rules as contingent on people's interactions with Web sites. In doing so, it neglects to consider that people encounter descriptions or implications of privacy rules through the general information and news environment. The press fairly frequently presents

stories about the stealing and accidental release of customer information. Credit card companies by law must regularly send privacy policy notices to their customers (The Gramm-Leach-Bliley Act of 1999—P.L. 106-102, §503, 113 Stat. 1439), and the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, §1173, 110 Stat. 2024-26) requires medical caregivers to tell patients the conditions under which they guard and/or share personal information. One view of these requirements is that they are difficult if not impossible to understand, a situation that might mislead consumers into thinking that their information is protected from cross-company sharing more than it really is (Turow 2003). Juxtaposed to these press stories, the very presence of the privacy notices and their comforting accompanying letters about the protection of consumer data may suggest an entirely different nature of privacy regime to their recipients.

Developing practical expertise regarding information privacy is not easy. Unlike regulators in other jurisdictions—those in the European Union, for example—lawmakers in the United States have not provided citizens with a coherent perspective through which they can understand how merchants must approach the privacy of their personal information (Langenderfer and Cook 2004). The consequence is a patchwork of regulations that reflects particular disconnected struggles over what information privacy should mean in certain areas of commerce—for example, the health and financial services industries—as well as in merchants' involvement with children younger than thirteen years. Apart from these exceptions, companies are generally *unconstrained* in their use of data for business purposes. They can take, use, and share personally identifiable data: information linked to individuals' names and addresses. They can also create, market, and sell detailed profiles of people whose names they do not know but whose interests and lifestyles they statistically infer from their activities online and offline (Pack 2000; Solove and Rotenberg 2003).

Despite the complexity of this regulatory environment, our findings based on a survey of adult Internet users suggest that Americans do have frameworks of knowledge regarding privacy in the marketplace. It is what they know, and especially what they believe they know, that is problematic.

METHODS AND MEASURE

Survey

We examined the nature of Americans' knowledge regarding privacy as part a larger study of Americans' knowledge of the laws regarding a company's right to collect information about them online or offline and to

charge them and others different prices for the same items at the same time. Because of our interest in people's relationships to both the online and the offline selling environments, we focused on U.S. adults who use the Internet. We included people aged eighteen years or older in our study if they said yes to the question, "Have you used the Internet in the past month at home, work, or anywhere else?"

ICR/International Communication Research of Media, Pennsylvania, collected the survey data from February 8 to March 14, 2005, using a nationally representative random digit dial sample to screen households for adults aged eighteen or older. The telephone interviews, which averaged twenty minutes, were completed with a nationally representative sample of 1,500 adults. The process involved computer-assisted telephone interviewing, which ensures that questions follow logical skip patterns and that attitude statements are automatically rotated, eliminating question position bias. Using the American Association of Public Opinion Research RR3 method, a standard for this type of survey, the overall response rate for this study was 58.4%. The margin of error for percentages was $\pm 2.5\%$ at the 95% confidence level, although the margin of error was higher for subgroups.

Measures

Table 1 shows the item set analyzed here. Items A–G refer to collecting and disclosing personal data. We analyzed these items in two different ways. First, we recoded the responses to reflect the correspondence between the correct answer and the respondent's answer. When coded this way, the items represent a knowledge index about information collection and disclosure by online and offline retailers. We also analyzed the respondent's unmodified true or false answers as reflecting a belief index about collection and disclosure behavior by online and offline retailers. Put another way, the first analysis of items A through G takes the "correctness" of the survey responses into account and treats the items as reflecting a potential knowledge structure, while the second analysis of items A through G ignores the correctness of the survey responses and treats the items as reflecting a belief index.

FINDINGS

Sample Characteristics

Table 2 provides a summary snapshot of the survey participants. Women slightly outnumbered men; seventy-three percent of participants

TABLE 1
Knowledge Items with Correct Answers and Survey Percentage Correct (N = 1500)

Knowledge Items on Collecting and Disclosing Personal Data	Correct Response	% Correct
A. Companies today have the ability to follow my activity across many sites on the Web.	True	83
B. A Web site is allowed to share information about me with affiliates without telling me the names of the affiliates.	True	51
C. When I subscribe to a magazine, by law that magazine cannot sell my name to another company unless I give it permission.	False	48
D. My supermarket is allowed to sell other companies information about what I buy.	True	36
E. When I give money to charity, by law that charity cannot sell my name to another charity unless I give it permission.	False	28
F. A video store is not allowed to sell information about the titles I have rented.	True	29
G. When a Web site has a privacy policy, it means the site will not share my information with other Web sites or companies.	False	25

designated themselves as non-Hispanic white and eight percent called themselves non-Hispanic blacks. Hispanics (white and black) comprised about ten percent of the sample, Asian Americans made up three percent, and Native Americans comprised about one percent. About sixty percent were younger than forty-five years, fifty-seven percent were married, and forty-four percent had children younger than 18 years. Most had at least some higher education, and while a substantial percentage said their household brought in more than \$75,000 annually, a firm claim about the sample's income distribution is difficult because seventeen percent of the population refused to reveal it. Other data collected included Internet use, self-reported computer and Internet skills, and shopping patterns; these variables are discussed below.

Understanding Merchants' Rights to Share Personal Information

The first analysis of items A through G in Table 1 treated them as measures of *knowledge* of data collecting and disclosing policies. Item A was the easiest to answer; eighty-three percent knew that companies have the ability to follow their activity across many sites on the Web. A far smaller percentage answered the other knowledge areas correctly. Around one-half correctly answered B and C—about Web sites and magazines sharing personal information. Only thirty-six percent knew the answer to the question about supermarkets and personal information; fewer than thirty percent correctly answered the questions about charities and video stores' policies.

TABLE 2
Characteristics of Survey Respondents (N = 1,500)

Respondent Characteristics	% ^a
<i>Gender</i>	
Male	48
Female	52
<i>Age (years)</i>	
18–34	37
35–44	22
45–54	18
55–64	10
65+	12
No answer	2
<i>Race and ethnicity</i>	
White non-Hispanic	73
White Hispanic	9
Black non-Hispanic	8
Black Hispanic	1
Asian American	3
Native American	1
Other	1
No answer	4
<i>Education</i>	
Less than high school graduate	8
High school/tech school graduate	31
Some college	27
College graduate or more	34
No answer	1
<i>Family income</i>	
Less than \$40K	26
\$40K but less than \$75K	29
\$75K but less than \$100K	13
\$100K+	14
Do not know/no answer	17
<i>Parental status</i>	
A parent of child younger than eighteen years	44
Not a parent of child younger than eighteen years	54
No answer	2

^aWhen the percentages fail to sum to 100%, it is because of rounding error.

Item G was the most difficult. Only twenty-five percent knew that the statement “When a Web site has a privacy policy, it means the site will not share my information with other Web sites or companies” was false.

To determine whether the items in the knowledge and belief indices were one dimensional, we used the KR20 statistic, a version of *alpha* appropriate for dichotomous data (Streiner 2003) and Mokken scaling. Mokken scaling assumes that unidimensionality of the items is defined by their ranking along an unobserved “difficulty” dimension such that all items after the

initial failure are also failed and all items before the initial failure are passed, a “Guttman pattern” of responses (Ringdal et al. 1999, 27). If the item scale using this definition, then the scale score implies that the respondent passed the items less than or equal to the observed score and failed all difficulty-ranked items greater than the value of the observed score.

Analysis of the relationships among the responses to the seven statements indicated a unidimensionality that conforms to a Guttman scale. The KR20 value was .73, which is high internal consistency, especially for test items as opposed to psychological ones. The Mokken scaling module in stata estimated a Loevinger's *H* (a measure of scalability) of .41 for the seven items, which is considered a “moderate” scale (Mokken, 1971). Overall, the average for the knowledge scale index was 3.22 items correct ($SD = 1.99$). Because the scale had a difficulty-ordering pattern, the correct items tended to be A, B, and C. Much smaller proportions of respondents knew the answers to D through G. Only 6.3% of all the respondents knew the correct answers to all seven questions. These results imply that moving from items A to G, if a respondent answered a question correctly, she/he was likely to know the correct answer to the easier questions before it. This scaled response pattern applied (e.g., showed the same ordering of items) even when background characteristics (e.g., gender, ethnicity, and age) were taken into account.

A plausible explanation for the respondent's knowledge can be linked to their education level: either they may have been taught the correct answers or their education may have provided them with the tools or skills to develop sophisticated knowledge frameworks. Education level was associated with the total knowledge score, $F(4, 1842) = 27.02, p < .05$. Those with graduate education had the highest knowledge score (mean = 3.85, $SD = 2.06, N = 306$), while those with less than a high school education had the lowest (mean = 1.81, $SD = 1.64, N = 31$).

In addition to differences by educational level, there were statistically significant differences in the average number of correct items by other respondent characteristics. When age was classified into four categories, the average knowledge score was significantly different between the age categories, $F(3, 1484) = 9.64, p < .05$. Average values on the knowledge scale were highest for the fifty- to sixty-four-year-old group (mean = 2.9, $SD = 1.95, N = 142$) and lowest for the eighteen- to twenty-nine-year-old group (mean = 2.67, $SD = 1.8, N = 238$). There was also a gender difference in knowledge; males' average score was 3.47 ($SD = 1.95$), while females averaged 3.01 ($SD = 2.02$), a statistically significant difference between means ($t = 4.35, p < .05$). Finally, the questionnaire collected data on the respondents' self-reported “abilities to go online or navigate

the Internet." The levels of assessment were "a beginner" ($N = 187$), "an intermediate user" ($N = 638$), "an advanced user" ($N = 506$), and "an expert user" ($N = 167$). Using these categories, we found that the knowledge score was significantly related to the respondent's self-assessment of skill, $F(3, 1497) = 25.5, p < .05$. The average values for the four skill groups (from least to most skilled) were 5.25 ($SD = 3.05$), 6.50 ($SD = 3.47$), 7.27 ($SD = 3.29$), and 8.04 ($SD = 3.60$).

The scaled array of the responses indicated a patterned set of responses; people who knew the right answers to certain statements about domains tended to be correct on statements regarding other domains. Yet the proportions of people who knew any of the statements below C were lower—often substantially lower—than 40%. People tended to state that companies in certain domains are allowed to share personal information but companies in other domains are not. So, for example, while fifty percent knew that the law does not protect the sharing of their personal information when it comes to the Web, only thirty-six percent also knew that this lack of protection applies to supermarkets and only twenty-eight percent knew that it applies to charities. If they believed that all domains fall under the same regulations, these percentages should be the same. Rather, such inconsistencies regarding firms' rights to share information across the range of domains indicate that most people believe that information-sharing rules are specific to particular merchant domains.

This conclusion was corroborated when we attempted to scale items A through G as a set of beliefs. Here, we ignore the correctness of the response and just analyze the intercorrelations between the items. As a set of beliefs, there was no pattern to the true or false responses at all: the KR20 was $-.19$. The items treated as beliefs were also not scaleable as to difficulty; Loevinger's H was $-.035$. Most strikingly, we found only a small (although significant) positive correlation between a respondent's score on the correct answer index and an index constructed from the summed belief items; the polychoric correlation between the two variables was $.08 (N = 1,500, p = .004)$. This small correlation highlights the respondents' lack of agreement about what domains are prohibited from sharing their private information and what domains are allowed to do so.

Our conclusion is that a small proportion of Internet-using American adults have a highly sophisticated knowledge framework regarding marketplace privacy. That segment has learned the regulations that allow it to correctly distinguish the circumstances in which merchants have the right to share information in different marketplace domains. A slightly larger proportion (the ones who knew all but the video-store answer) holds a less sophisticated, but nevertheless typically correct, framework. From our data,

we cannot tell whether this framework reflects actual knowledge of every specific marketplace domain except for video stores or whether it is based on a general assumption (wrong only in the video-store case) that the government always allows merchants to share people's private information. It is clear from the data that the large majority of Internet-using adults understand that regulations regarding merchants' sharing information are domain specific. At the same time, that majority was only sporadically correct regarding the true-false statements. The general picture of the population at large is one of the selective and limited knowledge about where in the marketplace one might find merchants who are legally allowed to share customers' personal information without their consent.

DISCUSSION

People who believe that banks send customers e-mails asking them to verify their accounts leave themselves open to "phishing," whereby thieves using e-mail persuade customers to give them private banking information and then steal their money. In our sample of Internet-using American adults, forty-nine percent did not know this fact about the online world. The misunderstanding helps explain the \$630 million that the Consumer Reports National Research Center estimates was stolen by this method through September 2006 (*Consumer Reports 2006*). Unfortunately, phishing is only one facet of Americans' ignorance of activities and rules relating to use of their private information. While a great majority of Americans know that companies have the ability to follow them across sites on the Web, far fewer know important facts about how merchants can take their information, about their recourse to complain if credit-related errors arise as a result of data collection, or that many types of merchants online and offline have the legal right to share information about them with other organizations even if they do not ask their permission.

These findings and others from this study broaden the concerns that observers such as Pitt and Watson (2007) and Nehf (2007) have regarding the structural impediments to privacy demands of Web sites by the public. The public's knowledge of the rules of privacy in the marketplace is clearly absent not just online but also offline and across a variety of for-profit and nonprofit entities. Our findings suggest that this ignorance goes beyond the failure to learn about specific privacy details at the point of individuals' interactions with merchants. It is rooted in a broader difficulty: the combination of a generally correct awareness of the fragmented nature of privacy regulation linked to frequent mistakes about actual facts of those regulations.

In the face of a misunderstanding of privacy regulations in the marketplace, a two-pronged approach of education and mandatory labeling may be required to make Americans aware of the data collection environment that surrounds them. Studies of the impact of the 1990 Nutrition Labeling and Education Act (e.g., Burton and Biswas, 1993; Burton, Creyer, and Huggins 2006; Burton, Garretson, and Velliquette, 1999) provide an interesting parallel. They suggest that education *and* mandatory labeling are both necessary in order to encourage consumer interest in, understanding of, and use of data that affect them but of which they have been unaware. Reflecting on a multimethod study of consumer responses to nutrition labeling, Balasubramanian and Cole (2002, 126) summarize that “Consumers care about nutrition information, but with two important nuances: First, they appear to rely on simple heuristics to collect nutrition information, that is, using the easy-to-digest information in descriptor terms or nutrition claims rather than the more comprehensive information in the Nutrition Facts panel Second, they appear to care more about certain types of nutrition information (negative types).” Balasubramanian and Cole (2002, 124) noted that “both nuances may yield suboptimal nutrition choices,” and this conclusion reinforces their suggestion that public policy officials should increase education about nutrition and nutrition labeling along with the required labeling.

Our findings regarding marketing and privacy suggest that, as with nutrition information, consumers rely on simple heuristics. That is why in the absence of a unified national philosophy about marketplace privacy to teach the rules in a logical manner, the best approach for educating Americans on the subject may well be to streamline the discussion of the regulations. Schools, community organizations, and media should describe privacy rules in ways that explicitly contradict the claims of customer choice implied by the corporate disclosures that people get in the mail and read on the Web. While there are some specific exceptions to merchant power over customer data, in most domains of U.S. commerce, merchants have the right to share customers’ personal information without their permission and the right to manipulate data to suit business aims without telling their customers. Encouraging a consumer orientation that emphasizes skepticism and assumes a lack of privacy protections may well lead them to be more correct than mistaken on this subject.

This sort of privacy education should, however, be accompanied by labeling requirements. The reason centers on the complexity, ambiguity, and lack of transparency that consumers confront in relation to privacy. Inaccurate knowledge frameworks may well be reinforced by structural features of the retail experience that Nehf (2007) clearly describes. In

supermarkets, for example, our finding that people's incorrect belief that the stores are not allowed to sell their information may be reinforced by the emphasis on speed at checkout counters. The fast-paced nature of the interaction at checkout counters makes it improbable that discussions will take place about the data collected with frequent shopper cards. The same type of structural reinforcement of inaccurate knowledge likely takes place with a Web site's link to its privacy policy. The very existence of the link may discourage people from reading the policy by exploiting their inaccurate knowledge regarding rules that govern merchants' use of information. Recall our finding that only twenty-five percent of respondents correctly said "false" to the statement "when a Web site has a privacy policy, it means the site will not share my information with other Web sites or companies." At the point of entry, then, individuals are inclined to believe that the law protects them and that the privacy policy merely states that. Our finding suggests that the label "privacy policy" is effectively even if not intentionally deceptive when used on a site that does not handle information in the way that a majority of Americans believe the label signifies. One response to this situation would be for the Federal Trade Commission to require a nondeceptive tag, such as "using your information," for areas of Web sites where rules for handling visitor information are described.

Businesses generally do not have sufficient incentive to implement this sort of transparency online or offline (Nehf 2007; Turow 2006). In the interest of encouraging a marketplace for privacy guidelines, it may therefore be up to the federal government to require posting of data collection policies that follow an orderly, predictable, and understandable template at the entry to all online and offline businesses. These two approaches—educating people in privacy frameworks that are accurate and requiring merchants to post information where they shop in ways that will allow them to use those frameworks—may go a long way toward establishing a beneficial marketplace for information privacy.

REFERENCES

- Anton, Annie and Julie B. Earp. 2004. A Requirements Taxonomy for Reducing Web Site Privacy Vulnerabilities. *Requirements Engineering*, 9 (3): 169–185.
- Anton, Annie, Julie B. Earp, Davide Bolchini, Qingeng He, Carlos Jensen, and William Stufflebeam. 2003. The Lack of Clarity in Financial Privacy Policies and the Need for Standardization. North Carolina State University Technical Report #TR-2. http://66.102.1.104/scholar?hl=en&lr=&q=cache:7Y0Lck1RWWIJ:www.theprivacyplace.net/papers/glb_secPriv_tr.pdf+. (Accessed July 8, 2008).
- Balasubramanian, Siva K. and Catherine Cole. 2002. Consumers' Search and Use of Nutritional Information: The Challenge and Promise of the Nutrition Labeling and Education Act. *Journal of Marketing*, 66 (3): 112–127.

- Burton, Scot and Abhijit Biswas. 1993. Preliminary Assessment of Changes in Labels Required by the Nutrition Labeling and Education Act of 1990. *Journal of Consumer Affairs*, 27 (1): 127–144.
- Burton, Scot, Elizabeth Creyer, and Kyle Huggins. 2006. Attacking the Obesity Epidemic: The Potential Health Benefits of Providing Nutrition Information in Restaurants. *American Journal of Public Health*, 96 (9): 1669–1675.
- Burton, Scot, Judith A. Garretson, and Anne M. Velliquette. 1999. Implications of Accurate Usage of Nutrition Facts Panel Information for Food Product Evaluations and Purchase Intentions. *Journal of the Academy of Marketing Science*, 27 (4): 470–480.
- Consumer Reports*. 2006. State of the Net, 2006. September. http://www.consumerreports.org/cro/electronics-comp-utters/online-protection-9-06/state-of-the-net/0609_online-prot_state.htm. (Accessed November 13, 2007)
- Goldman, Janlori, Zoe Hudson, and Richard Smith. 2000. *Privacy: Report on the Privacy Policies and Practices of Health Web Sites*. Oakland, CA: California HealthCare Foundation. Accessed <http://www.chcf.org/topics/view.cfm?itemID=12497>. (Accessed November 11, 2007)
- Graber, Mark, Dona M. D'Allessandro, and Jill Johnson-West. 2002. Reading Level of Privacy Policies on Internet Health Web Sites. *Journal of Family Practice*, 51 (7): 642–645.
- Hann, Il-Horn, Tom Lee, Kai-Lung Hui, and I.P. Pug. 2002. Online Information Privacy: Measuring the Cost-Benefit Trade-Off. *Proceedings of the Twenty-Third International Conference on Information Systems*. http://www.comp.nus.edu.sg/~ipng/research/privacy_icis.pdf. (Accessed July 8, 2008)
- The Health Insurance Portability and Accountability Act of 1996, Public Law No. 104–191, §1173, 110 Stat. 2024–26.
- Jensen, Carlos, Colin Potts, and Christian Jensen. 2005. Privacy Practices of Internet Users: Self-Reports versus Observed Behavior. *International Journal of Human-Computer Studies*, 63: 203–227.
- Jupiter Media Metrix. 2002. *Seventy Percent of US Consumers Worry About Online Privacy, But Few Take Protective Action*. Press Release, June 3.
- Langenderfer, Jeff and Don Cook. 2004. Oh, What a Tangled Web We Weave: The State of Privacy Protection in the Information Economy and Recommendations for Governance. *Journal of Business Research*, 57 (7): 734–747.
- Madden, Mary, Susannah Fox, Aaron Smith, and Jessica Vitak. 2007. *Digital Footprints: Online Identity Management in the Age of Transparency*. Washington, D.C.: Pew Internet and American Life Project, 2007. <http://www.pewinternet.org/>. (Accessed July 8, 2008)
- Mokken, Robert. 1971. *A Theory and Procedure of Scale Analysis*. The Hague, The Netherlands: Mouton.
- Nehf, James P. 2007. Shopping for Privacy on the Internet. *Journal of Consumer Affairs*, 41 (2): 351–365.
- Pack, Todd. 2000. Law Too Weak to Help Much; Some Statutes Attempt to Protect Your Privacy, but Advocates Say They Are Filled with Loopholes. *Orlando Sentinel*, September 24, A13.
- Pitt, Leyland F. and Richard T. Watson. 2007. An Ecosystem Perspective on Privacy. *Journal of Consumer Affairs*, 41 (2): 365–375.
- Ringdal, Kristen, Gerd Ringdal, Stein Kaasa, Klaus Bjordal, Marcus Wisløff, Ian Sundstrøm, and Marianne Hjermstad. 1999. Assessing the Consistency of Psychometric Properties of the HRQoL Scales within the EORTC QLQ-C30 across Populations by Means of the Mokken Scaling Model. *Quality of Life Research*, 8 (4): 25–43.
- Solove, Daniel and Marc Rotenberg. 2003. *Information Privacy Law*. New York: Aspen Publishers.
- Steiner, David. 2003. Starting at the Beginning: An Introduction to Coefficient Alpha and Internal Consistency. *Journal of Personality Assessment*, 80 (1): 99–103.
- Turow, Joseph. 2003. *Americans and Online Privacy: The System is Broken*. Philadelphia, PA Annenberg Public Policy Center. http://www.annenbergpublicpolicycenter.org/04_info_society/2003_online_privacy_version_09.pdf. (Accessed July 8, 2008)
- . 2006. *Niche Envy: Marketing Discrimination in the Digital Age*. Cambridge, MA: MIT Press.
- Turow, Joseph and Lilach Nir. 2000. *The Internet and the Family 2000: The View from Parents, the View From Kids*. Philadelphia, PA: Annenberg Public Policy Center.

- Vila, Tony, Rachel Greenstadt, and David Molnar. 2003. Why We Can't Be Bothered to Read Privacy Policies. In *ACM International Conference Proceeding Series*, edited by Norman Sadeh, Vol. 50, pp. 403–407. New York: ACM Press.
- Westin, Allen. 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59 (3): 431–453.

