

Research Report: What Californians Understand About Privacy Online

By Chris Jay Hoofnagle & Jennifer King¹

September 3, 2008

Abstract	2
Introduction	3
<i>Privacy Policies and Privacy Practices</i>	3
<i>California Consumers and Privacy Policies</i>	4
Methods	5
<i>Our Research Standards</i>	6
<i>Alan Westin's Privacy Segmentation</i>	6
Results & Discussion	10
<i>How Often Did Respondents Shop Online</i>	10
<i>Third Party Information Sharing</i>	11
<i>Affiliate Sharing</i>	13
<i>Disclosure of Information Sharing Partners</i>	14
<i>Analysis of Online Activities</i>	15
<i>Enhancement</i>	17
<i>Retention of Personal Information</i>	18
<i>Access and Correction</i>	19
<i>Right to Delete</i>	20
<i>Government Access</i>	21
<i>Assistance in the Event of Identity Theft</i>	22
<i>Notification of Security Breaches</i>	23
<i>Right to Sue for Damages</i>	24
Conclusion	25
Appendix I: Question Data	27
Appendix II: Westin Segmentation	30
Appendix III: Related Reports	33

¹ Respectively, Senior Staff Attorney and Research Specialist, Samuelson Law, Technology & Public Policy Clinic, University of California, Berkeley, School of Law.

Abstract

The volume of online commerce grows every year, in absence of a federal law setting baseline protections for the collection, use, and disclosure of personal information. Instead, information collected by websites are governed by individual privacy policies.

In order to gauge Californians' understanding of privacy policies and default rules in the online environment, we commissioned a representative survey of adults in the State (N=991). The telephonic survey of Spanish and English speakers was conducted by the Survey Research Center of University of California, Berkeley.

A gulf exists between California consumers' understanding of online rules and common business practices. For instance, Californians who shop online believe that privacy policies prohibit third-party information sharing. A majority of Californians believes that privacy policies create the right to require a website to delete personal information upon request, a general right to sue for damages, a right to be informed of security breaches, a right to assistance if identity theft occurs, and a right to access and correct data.

These findings show that California consumers overvalue the mere fact that a website has a privacy policy, and assume that websites carrying the label have strong, default rules to protect personal data. In a way, consumers interpret "privacy policy" as a quality seal that denotes adherence to some set of standards. Website operators have little incentive to correct this misperception, thus limiting the ability of the market to produce outcomes consistent with consumers' expectations. Drawing upon earlier work, we conclude that because the term "privacy policy" has taken on a specific meaning in the minds of consumers, its use should be limited to contexts where businesses provide a set of protections that meet consumers' expectations.

Introduction

Privacy Policies and Privacy Practices

“Privacy is about trust.”

“We take your privacy seriously, which is why we developed this privacy policy to explain our online information collection and use practices.”

“We are committed to protecting your privacy.”

“Your privacy is important to us.”

These statements are drawn from the privacy policies of popular e-commerce websites. But what do they mean? If privacy is *important*, so *serious* that companies have made a *commitment* to it, what business uses of personal information are permissible?

The law does little to conform business practices to representations about privacy’s importance. California state law requires that privacy policies address certain topics, and that companies comply with representations made.² However, the law does not specify baseline standards for the collection, use, and disclosure of information. Accordingly, privacy policies do not guarantee individuals specific rights; they are more akin to a statement of company policy. Among other practices, companies are free to adopt opt-out policies that allow sale of personal information unless the customer objects, or to refuse to allow individuals to opt-out unless they meet arbitrary requirements.³

In an earlier report, *What Californians Understand About Privacy Offline*, we found that Californians thought that legal rules protected personal information from sale to third parties. We asked Californians about privacy in nine offline contexts. In six of those contexts (pizza delivery, donations to charities, product warranties, product rebates, phone numbers collected at the register, and catalog sales), a majority either didn’t know or falsely believed that opt-in rules protected their personal information from

² Cal. Bus. & Prof. Code § 22575-22579.

³ “LexisNexis voluntarily offers individuals the opportunity to request that records about themselves be removed, under certain terms and conditions, from its non-public information databases. The policy governing the LexisNexis Opt-Out Program is not legally mandated by any state or federal law.” Opt Out Requests, LexisNexis, available at <http://www.lexisnexis.com/privacy/for-consumers/opt-out-of-lexisnexis.aspx>.

being sold to others. Only in two contexts—newspaper and magazine subscriptions and sweepstakes competitions—did our sample of Californians understand that personal information collected by a company could be sold to others.⁴

Also in earlier work, to learn more about information selling practices we used a California privacy law to make requests to 86 companies for a disclosure of their information sharing policies. We found that while many companies have voluntarily adopted a policy of not sharing personal information with third parties, many still operate under an opt-out model, and others simply did not respond to the request.⁵

California Consumers and Privacy Policies

In this report, we assess Californians' understanding of privacy policies and information privacy rights online. This paper builds upon the work of Professor Joseph Turow, who in 2003 and 2005, asked national representative samples of Americans about their privacy knowledge.⁶ In 2003, Turow focused on a range of online transactions, and in 2005, he added questions concerning offline privacy, online behavioral profiling and price discrimination. From these surveys, Turow concluded that consumers misinterpreted the "privacy policy" label, and thought that websites with privacy policies were barred from selling personal information.⁷

Drawing upon these surveys, in 2006 our clinical team wrote a paper with Professor Turow arguing, "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

⁴ Chris Jay Hoofnagle & Jennifer King, *What Californians Understand About Privacy Offline*, May 15, 2008, available at <http://www.law.berkeley.edu/samuelsclinic/privacy/274>.

⁵ Chris Jay Hoofnagle & Jennifer King, *Consumer Information Sharing: Where the Sun Still Don't Shine*, Dec. 17, 2007, available at <http://www.law.berkeley.edu/samuelsclinic/privacy/219>.

⁶ Joseph Turow, *Americans & Online Privacy, The System is Broken*, Annenberg Public Policy Center (June 2003), available at [http://www.annenbergpublicpolicycenter.org/Downloads/Information And Society/20030701 America and Online Privacy/20030701_online_privacy_report.pdf](http://www.annenbergpublicpolicycenter.org/Downloads/Information%20And%20Society/20030701_America_and_Online_Privacy/20030701_online_privacy_report.pdf); Joseph Turow, Lauren Feldman, & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, Annenberg Public Policy Center of the University of Pennsylvania, Jun, 1, 2005, available at <http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31>.

⁷ *Id.*

make disclosures, they should not be allowed to refer to such disclosures as ‘privacy policies.’”⁸

We wished to further explore the knowledge gap among consumers illuminated by Turow’s research, and test the extent to which consumers believe privacy policies limit business practices. We thus asked Californians whether privacy policies gave them rights to control personal information in twelve different ways.

We also analyzed responses under Professor Alan Westin’s popular segmentation of privacy attitudes.

Methods

Our survey questions were asked as part of the 2007 Golden Bear Omnibus Survey, a telephone-based survey of a representative sample of California residents conducted by the Survey Research Center of University of California, Berkeley. The Samuelson Law, Technology & Public Policy Clinic funded the privacy portion of the Golden Bear survey from general operating funds; no outside organization sponsored the survey.

The dual frame sample used random digit dialing of both cell phones and residential landline telephones, with one respondent per household selected.⁹ English and Spanish speakers over the age of 18 were eligible. 1,186 respondents completed the telephone interview, conducted from April 30th to September 2nd, 2007, for a response rate of 15.9%. However, in order to include more questions in the survey than could be administered to all respondents in a reasonable period of time, the sample was divided into six randomized parts or units. All respondents were asked certain basic demographic and background questions, but most questions were administered only to 5/6th of the complete sample. This reduced the number of respondents who answered our questions to 991. Weights were applied to compensate for probabilities of selection

⁸ Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good & Jens Grossklags, The Federal Trade Commission and Consumer Privacy in the Coming Decade, 3 ISJLP 723 (Winter 2007), available at <http://www.is-journal.org/V03I03/Turow.pdf>.

⁹ For details on the construction of the sample, please see <http://sda.berkeley.edu/src/GB0/2007/Doc/hcbka01.htm>.

and to match certain demographic distributions.¹⁰ This weighting ensures that the results reflect a representative sample of Californians by age, education, ethnicity, and gender, and compensates for differences in probabilities of selection based on use of landline versus cell phones.

Additionally, each of our privacy questions were administered to approximately one-third of the total sample of 991 subjects. Exact respondent totals for each question can be found in Appendix I.

Our Research Standards

We hold ourselves to high standards in conducting public polls. We encourage the reader to compare our methods to the best practices articulated in *20 Questions A Journalist Should Ask About Poll Results*, published by the National Council on Public Polls.¹¹ Furthermore, we go beyond these standards by, first, guaranteeing that we publish all the questions asked and responses received; and second, sharing our results so that others can inspect them (see Appendix I). The Survey Research Office will post the raw data file associated with the Golden Bear Omnibus Survey online in late 2008.

Alan Westin's Privacy Segmentation

Professor Alan Westin has pioneered a popular "segmentation" of privacy attitudes among the American public.¹² In it, Americans are divided into three groups: "Privacy Fundamentalists,"¹³ who place a high value on privacy and favor passage of

¹⁰ For a detailed overview of sampling methods, please see: <http://sda.berkeley.edu/src/GB0/2007/Doc/hcbka02.htm>.

¹¹ Available at <http://www.ncpp.org/?q=node/4>.

¹² Ponnurangam Kumaraguru & Lorrie Faith Cranor, *Privacy Indexes: A Survey of Westin's Studies*, Dec. 2005, available at <http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf>.

¹³ "Privacy Fundamentalists (about 25%). This group sees privacy as an especially high value, rejects the claims of many organizations to need or be entitled to get personal information for their business or governmental programs, thinks more individuals should simply refuse to give out information they are asked for, and favors enactment of strong federal and state laws to secure privacy rights and control organizational discretion." *Opinion Surveys: What Consumers Have To Say About Information Privacy, before the House Commerce Subcommittee on Commerce, Trade, and Consumer Protection*, May 8, 2001 (testimony of Alan K. Westin, Professor Emeritus, Columbia University), available at <http://energycommerce.house.gov/reparchives/107/hearings/05082001Hearing209/Westin309.htm>.

strong privacy laws; “Privacy Pragmatists,”¹⁴ who see the relative benefits of information collection and favor voluntary standards for privacy protection; and the “Privacy Unconcerned,”¹⁵ those who have low privacy concern and have little objection to giving government or businesses personal information. The Westin segmentation has been influential politically and is often used to frame Americans’ privacy attitudes.

We were interested to see how our sample of California residents fit into the Westin segmentation. We included the three questions (Appendix II) Westin has used to divide respondents into these segments in our survey instrument.

Westin’s own figures for the three segments are as follows:

Table 1: Westin’s Figures for Privacy Segments in U.S., 1995¹⁶ – 2001¹⁷

Year of Study	Privacy Fundamentalists	Privacy Pragmatists	Privacy Unconcerned
1995-1999	25%	55%	20%
2001	25%	63%	12%

¹⁴ "Privacy Pragmatists (about 55%). This group weighs the value to them and society of various business or government programs calling for personal information, examines the relevance and social propriety of the information sought, looks to see whether fair information practices are being widely enough observed, and then decides whether they will agree or disagree with specific information activities -- with their trust in the particular industry or company involved a critical decisional factor. The Pragmatists favor voluntary standards over legislation and government enforcement, but they will back legislation when they think not enough is being done -- or meaningfully done -- by voluntary means." *Id.*

¹⁵ "Privacy Unconcerned (about 20%) This group doesn't know what the “privacy fuss” is all about, supports the benefits of most organizational programs over warnings about privacy abuse, has little problem with supplying their personal information to government authorities or businesses, and sees no need for creating another government bureaucracy to protect someone's privacy." *Id.*

¹⁶ Figures from 1995-1999 are approximate. EQUIFAX-HARRIS MID DECADE CONSUMER PRIVACY SURVEY (1995), EQUIFAX-HARRIS CONSUMER PRIVACY SURVEY (1996), IBM-HARRIS MULTI-NATIONAL CONSUMER PRIVACY STUDY (1999).

¹⁷ 2001 data is found in: Ponnurangam Kumaraguru & Lorrie Faith Cranor, *Privacy Indexes: A Survey of Westin’s Studies*, Dec. 2005, available at <http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf>.

Segmentation of our population is shown in Table 2:

Table 2: Westin Segments Applied to This Survey of Californians¹⁸

	Privacy Fundamentalists	Privacy Pragmatists	Privacy Unconcerned	Unclassified	Total
Count	208	665	30	88	991
Percentage of all respondents	21%	67%	3%	9%	100%
Percentage of those who could be classified	23%	74%	3%	N/A	100%

Westin notes that since he began conducting consumer privacy surveys, he has observed “a well-documented transformation in consumer privacy attitudes over the past decade, moving concerns from a modest matter for a minority of consumers in the 1980s to an issue of high intensity expressed by more than three-fourths of American consumers in 2001.”¹⁹ The changes in Pragmatists and the Unconcerned between 1999 to 2001 (the year for which most recent data is available), according to Westin, further reflects the rising popularity of the internet (and its attendant privacy risks), as well as heightened awareness of identity theft. In comparing our California-specific population to Westin’s general population numbers, it is clear that Californians have even stronger privacy concerns; while Fundamentalists are slightly lower than Westin’s 2001 numbers (23% in CA compared to 25% nationally), Pragmatists are over 10 points higher (74% in CA compared to 63% nationally), and the Unconcerned nine points lower (3% in CA compared to 12% nationally).²⁰ Considering the change in Westin’s numbers in only two

¹⁸ In order to be included in a segment, a respondent had to provide a valid answer to all three questions. Respondents who provided one or more invalid answers are unclassified.

¹⁹ Ponnuram Kumaraguru & Lorrie Faith Cranor, *Privacy Indexes: A Survey of Westin’s Studies*, Dec. 2005, available at <http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf>.

²⁰ Due to the presentation of the privacy policy questions to only one-third of the subjects (as described in the previous section), the number of subjects classified as Privacy Unconcerned is quite small when additionally filtering for subjects who shop online. Due to these restrictions, we did not attempt to measure whether differences in responses between the three Westin groups were statistically significant.

years, and the prominence that privacy and security issues have had in the public consciousness after the September 11, 2001 terrorist attacks, it is probable that a national survey conducted in 2008 would produce numbers more in line with our California findings.

Table 3: Westin Segments Applied to Respondents Who Shop Online

	Privacy Fundamentalists	Privacy Pragmatists	Privacy Unconcerned	Unclassified	Total
Count	108	402	17	30	557
Percentage of all respondents	19.40%	72.20%	3.10%	5.30%	100%
Percentage of those who could be classified	20.50%	76.30%	3.30%	N/A	100%

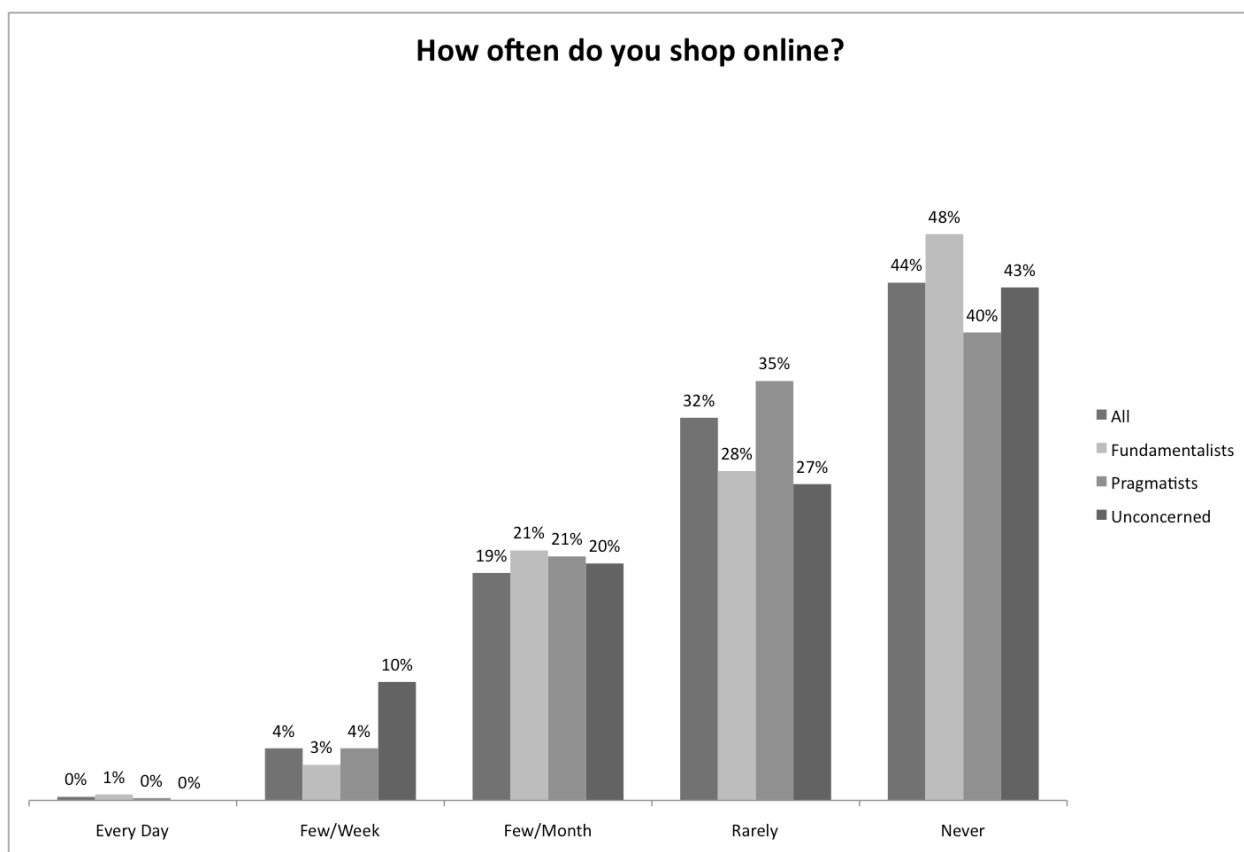
Finally, it is important to note that for each of the privacy questions we ask, numbers presented for Westin segmentations are for online shoppers only, and not for the entire subject pool.

Results & Discussion

How Often Did Respondents Shop Online

Respondents were first asked whether they shopped online in order to divide the sample into subgroups based on their level of experience with e-commerce. A large percentage of the sample does not shop online. This does not mean that they do not use the internet, because there are a significant group of individuals who have access to the internet for information and news gathering, but who refuse to purchase items online.

Since our survey gauges Californians' knowledge of privacy rights in twelve different contexts, this question offers the opportunity to compare how often Privacy Fundamentalists, Pragmatists, and the Unconcerned shop online, and whether they can correctly identify privacy rights.



Third Party Information Sharing

Third party information sharing is strongly opposed by the public. As Joanne McNabb, Chief of California's Office of Privacy Protection, explains, "Consumers are increasingly very unhappy with sharing of their information for marketing purposes."²¹ When given the opportunity to vote on the issue, North Dakotans strongly rejected an opt-out standard for third party information sharing in financial services context. In June 2002, 73% voted to reestablish an affirmative consent standard for banks that wished to sell personal information to third party companies.²²

When asked in opinion polls, large majorities of Americans indicate that they support requiring businesses to obtain affirmative consent before selling personal information to third parties. The Pew Internet & American Life Project found that 86% support opt-in consent before companies sell personal information.²³ Similarly, *BusinessWeek* found that 88% want websites to gain affirmative opt-in consent before sharing personal information with others.²⁴ However, no state or federal law limits the sale of personal information of adults collected on websites to third parties.

Survey research has also shown that consumers are not aware of information flow and sale. In 2003, Turow wrote:

*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.*²⁵

²¹ Louis Trager, *Cal.'s Unique, Broad New Info-Sharing Law Largely Under the Radar, Says State Privacy Chief*, WASH. INTERNET DAILY, Oct. 7, 2005.

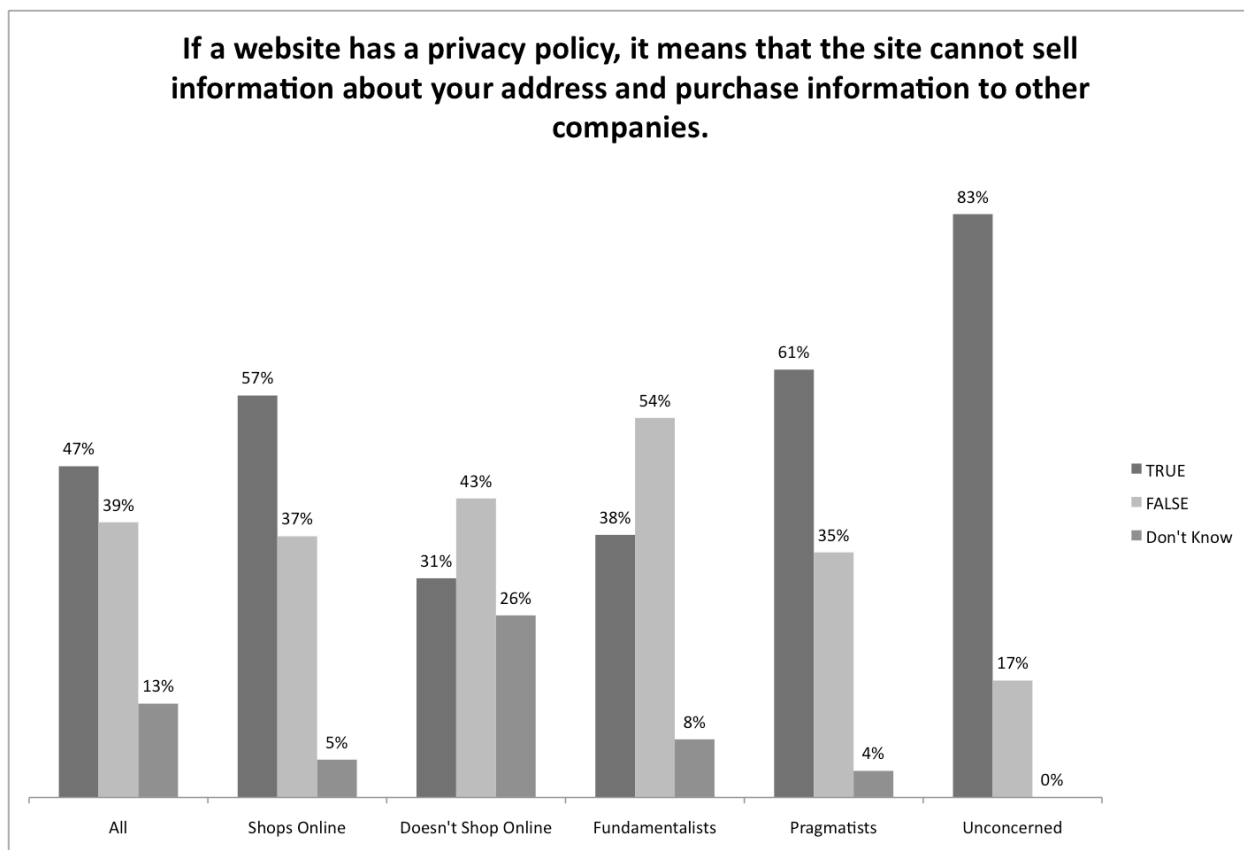
²² North Dakota Secretary of State, Statewide Election Results, Jun. 11, 2002.

²³ PEW INTERNET & AMERICAN LIFE PROJECT, TRUST AND PRIVACY ONLINE: WHY AMERICANS WANT TO REWRITE THE RULES, Aug. 20, 2000, available at http://www.pewinternet.org/report_display.asp?r=19

²⁴ *A Growing Threat*, BUSINESSWEEK MAGAZINE, Mar. 2000, available at http://www.businessweek.com/2000/00_12/b3673010.htm.

²⁵ Joseph Turow, *Americans & Online Privacy, The System is Broken*, Annenberg Public Policy Center (June 2003), available at [http://www.annenbergpublicpolicycenter.org/Downloads/Information And Society/20030701_America_and_Online_Privacy/20030701_online_privacy_report.pdf](http://www.annenbergpublicpolicycenter.org/Downloads/Information%20And%20Society/20030701_America_and_Online_Privacy/20030701_online_privacy_report.pdf).

Turow et al., in their 2005 national sample of internet users, found that 59% agreed with the incorrect statement, “When a website has a privacy policy, it means the site will not share my information with other websites or companies.” Of the remaining respondents, 25% answered false, and 16% didn’t know.²⁶



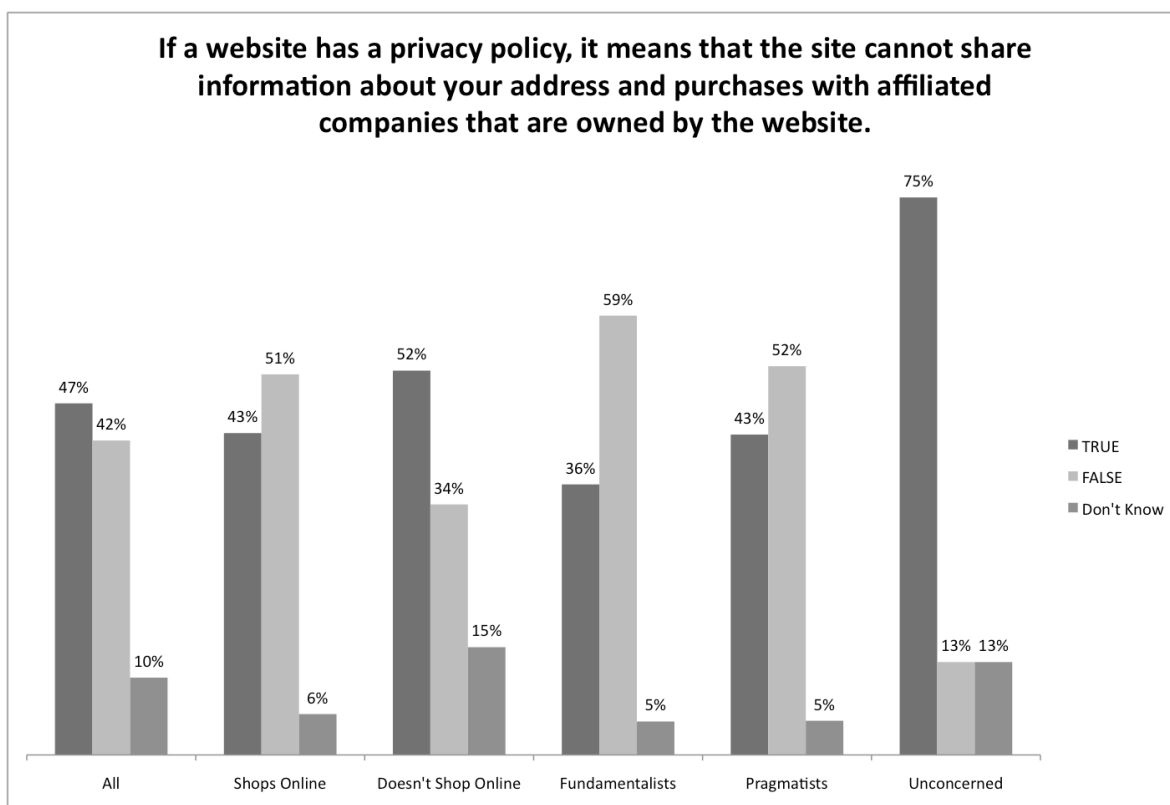
We asked Californians whether privacy policies prohibit third-party information sharing. When asked of all respondents, 47.3% thought that privacy policies prohibited such sale, and 13.4% didn’t know. Our results tracked Turow’s when asked of online shoppers: 57.4% believed that their personal information could not be sold, and 5.4% said that they didn’t know. Those who do not shop online and Privacy Fundamentalists were more likely to answer the question correctly than online shoppers, the Pragmatists, and the Unconcerned.

²⁶ Joseph Turow, Lauren Feldman, & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, Annenberg Public Policy Center of the University of Pennsylvania, Jun, 1, 2005, available at <http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31>

Affiliate Sharing

Privacy law frequently makes a distinction between transferring personal information to third parties and similar transfers among “affiliates,” companies that are related to each other by having common corporate control or ownership. Generally, privacy laws give consumers more control over third party information sharing. Consumers may also expect that a large entity would leverage economies of scale to perform more efficiently, thus requiring some level of affiliate sharing. As with third party information sharing, no federal or state law limits the sharing of adults’ personal information collected on websites with affiliates.

Turow et al. found in their 2005 study of internet-using adults that 51% correctly answered true to the statement, “A website is allowed to share information about me with affiliates without telling me the names of the affiliates.” Of the remaining respondents, 29% answered false and 20% didn’t know.²⁷

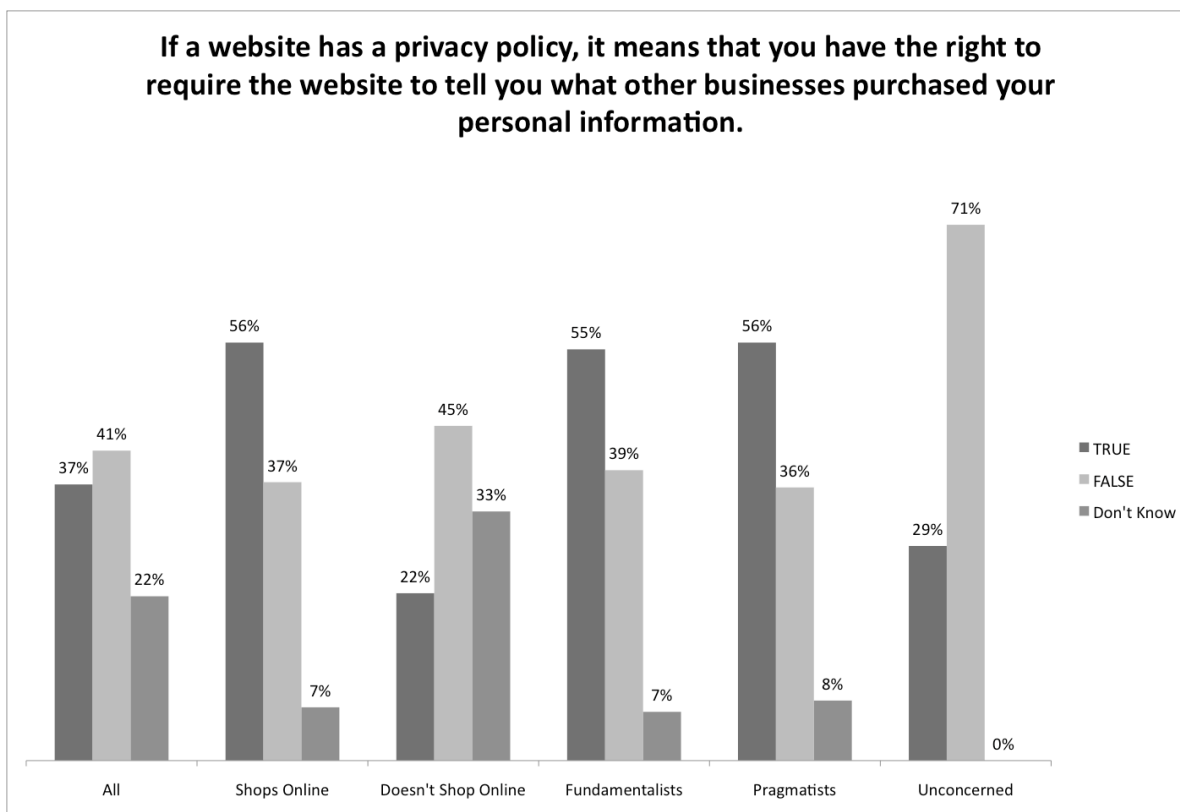


²⁷ Joseph Turow, Lauren Feldman, & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, Annenberg Public Policy Center of the University of Pennsylvania, Jun, 1, 2005, available at <http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31>.

We asked Californians whether privacy policies prohibit information sharing with affiliates. When asked of all respondents, 47.3% thought such sharing was prohibited by privacy policies and 10.4% didn't know. Online shoppers were more in tune with the actual rules--51.2% correctly answered false. Again, Privacy Fundamentalists were more likely to answer correctly than Privacy Pragmatists or the Unconcerned.

Disclosure of Information Sharing Partners

Privacy policies often specify that a company will share personal information with others, but the law does not require a website to disclose the identity of its information sharing partners. California law simply requires that privacy policies disclose the “categories” of third party information sharing partners. Also, a relatively obscure California law, SB 27, the “Shine the Light Law,” allows residents to request that businesses, online or off, disclose their information sharing partners.²⁸ Businesses can also comply with this law by allowing consumer to opt out. This right is not tied to the



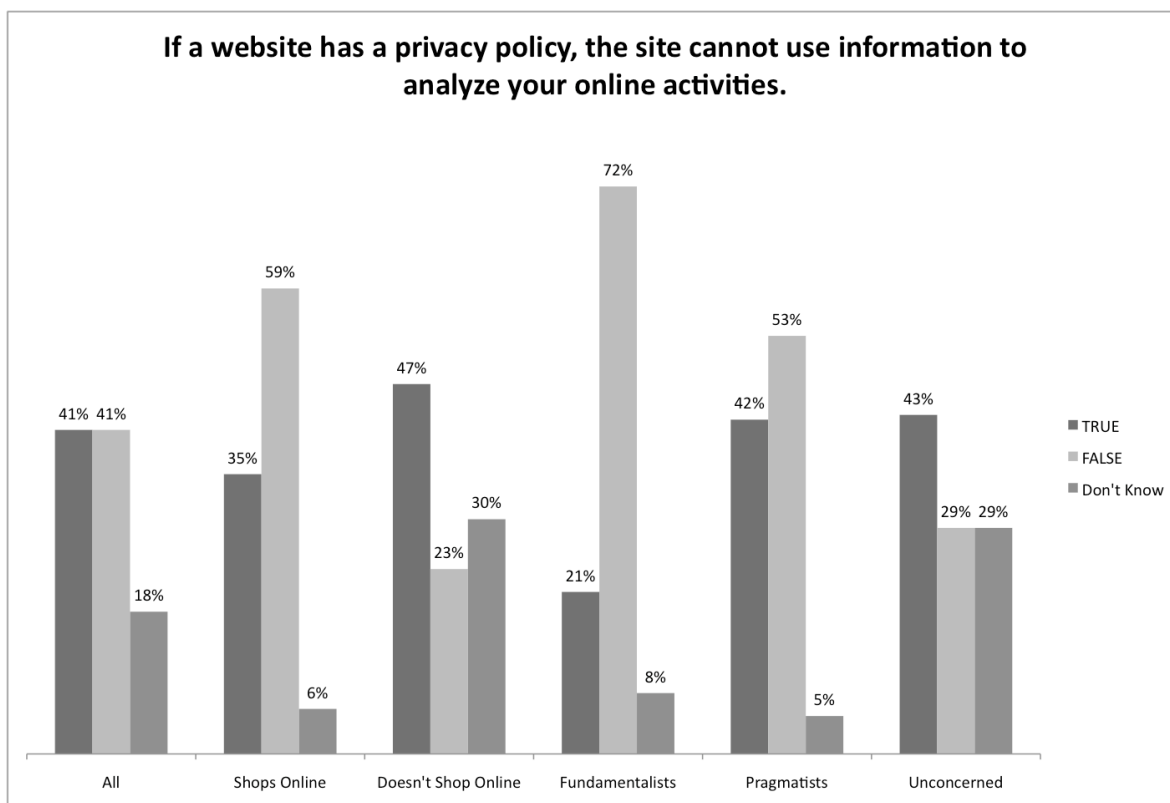
²⁸ Chris Jay Hoofnagle & Jennifer King, *Consumer Information Sharing: Where the Sun Still Don't Shine*, Dec. 17, 2007, available at <http://www.law.berkeley.edu/samuelsclinic/privacy/219>.

presence of a privacy policy.

We asked Californians whether privacy policies required disclosure of the names of businesses that purchased their personal information. Among all respondents, 41.3% answered that such a disclosure was not required, but 36.8% thought that privacy policies required websites to reveal to whom personal information was sold, and 21.9% didn't know. A majority of online shoppers believed that privacy policies required disclosure of the identity of information sharing partners, and 7.4% didn't know.

Analysis of Online Activities

We next attempted to assess whether Californians understood that websites can analyze online activities using personal information. Turow found in his 2003 survey that 59% agreed or strongly agreed with the statement, "When I go to a website it collects information about me even if I don't register."²⁹ That collection of information can be used for analysis of behavior on websites and for targeted advertising.

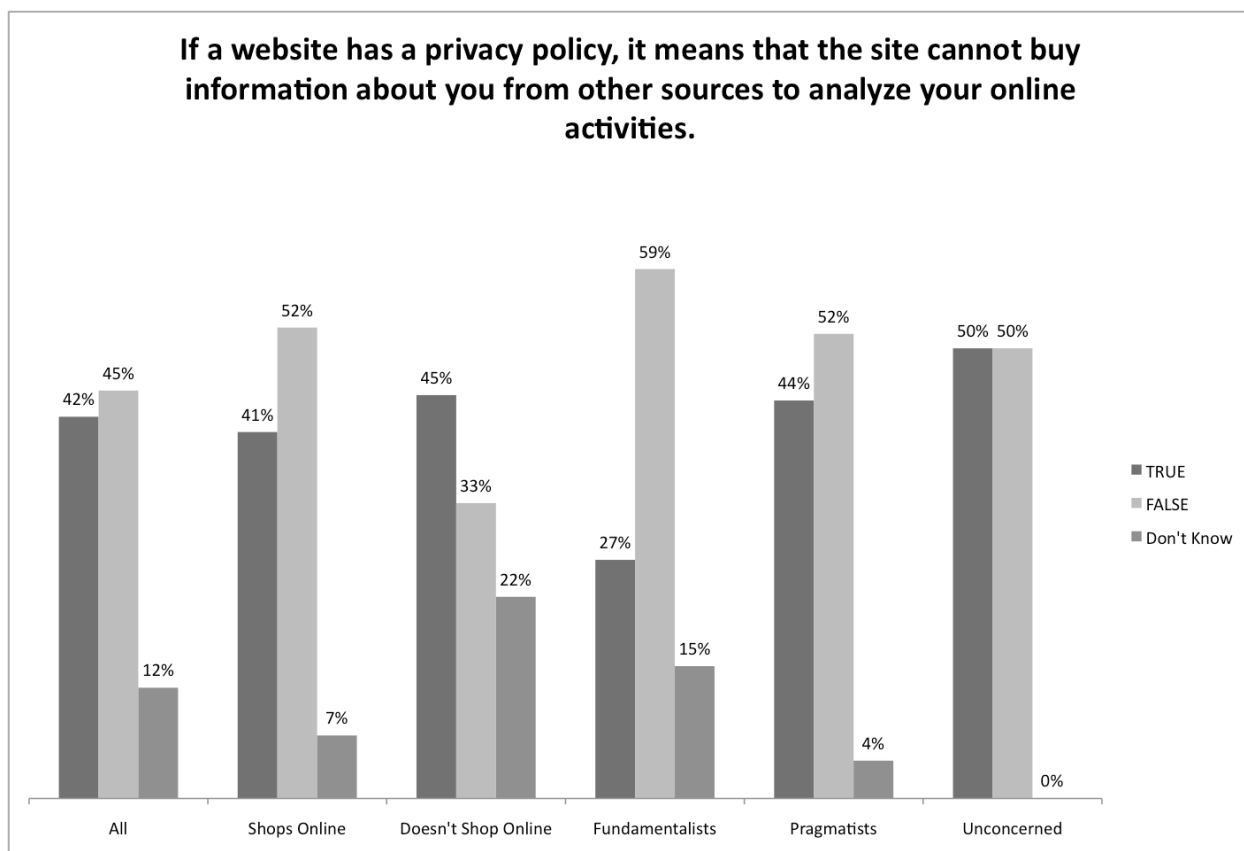


²⁹ Joseph Turow, *Americans & Online Privacy, The System is Broken*, Annenberg Public Policy Center (June 2003), available at, <http://www.annenbergpublicpolicycenter.org/Downloads/Information And Society/20030701 America and Online Privacy/20030701 online privacy report.pdf>.

A clear majority of online shoppers understand this; we found that 58.9% correctly answered false to the statement, “If a website has a privacy policy, it means that the site cannot use information to analyze your online activities.” Among those who do not shop online, 46.8% incorrectly answered true, and 29.7% said they didn’t know. This means that the knowledge gap among non-shoppers is substantial and that consumer education efforts should specifically include this subgroup. Since personal information is often collected outside the context of purchasing (for instance, internet searches), this group is using the internet while profoundly misunderstanding the rules of the road. Privacy Fundamentalists were more likely to answer correctly than Pragmatists or the Unconcerned.

Enhancement

Enhancement, often referred to as a data “append,” is the practice of adding personal information from other sources to an existing database. For instance, if an individual shares a name and email address with a website, that website could use the information to buy the individual’s home address and phone number. Turow et al. found in their 2005 survey of internet-using Americans that there was strong resistance to enhancement. When read the statement, “If I trust an online store, I don’t mind if it buys information about me from database companies without asking me,” 90% disagreed or disagreed strongly.³⁰



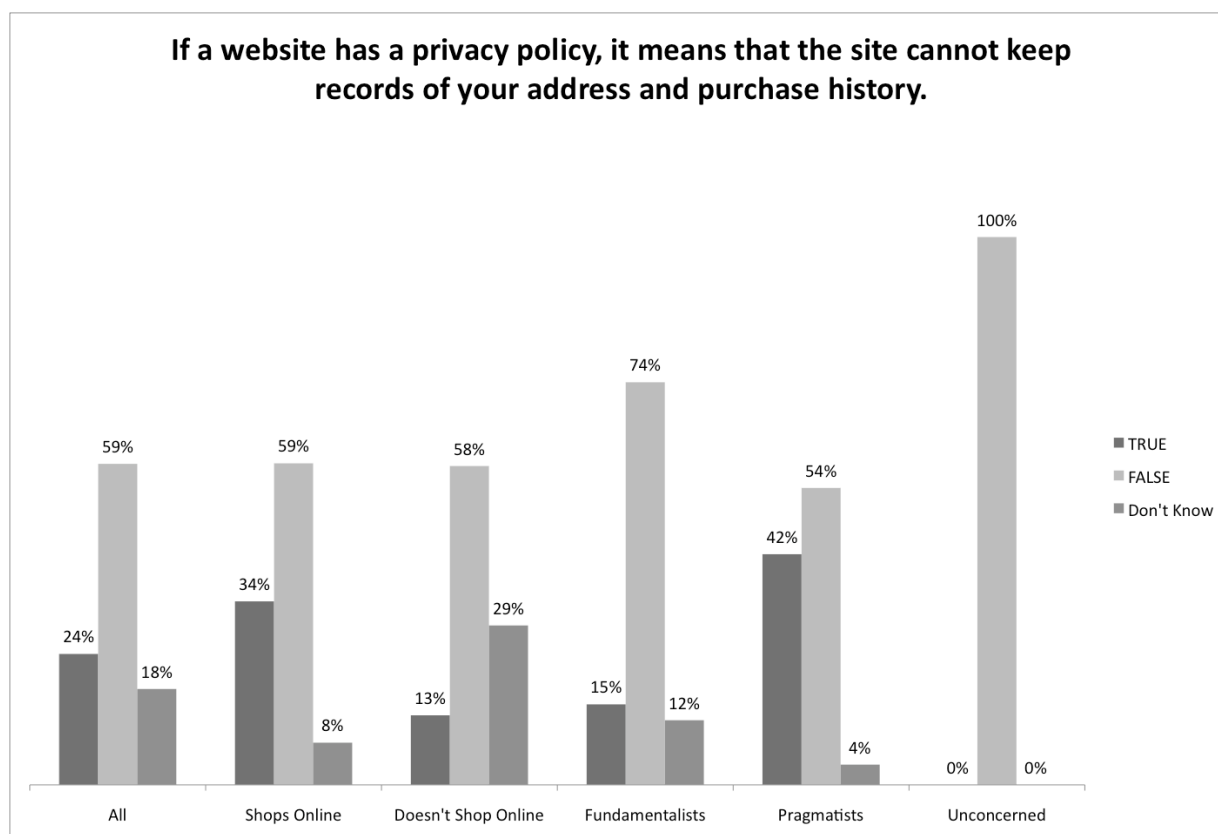
We asked Californians whether privacy policies prohibited the purchase of personal information from other sources. When asked of all respondents, 42.4% thought privacy policies prohibited enhancement activities, and 12.3% didn't know.

³⁰ Joseph Turow, Lauren Feldman, & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, Annenberg Public Policy Center of the University of Pennsylvania, Jun, 1, 2005, available at <http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31>

Respondents who shopped online were more likely to understand that privacy policies do not prohibit enhancement--52.3% correctly responded false to the question.

Retention of Personal Information

Websites are free to maintain personal information collected from individuals indefinitely. Merely having a privacy policy does not limit the period that data can be retained. Turow et al. found in their 2005 study of internet-using adults that many object to retention of purchase records. They found that 57% agreed or agreed strongly with the statement, "It would bother me if websites I shop at keep detailed records of my buying behavior."³¹



Our group of Californians across all categories were more likely than not to understand that websites can keep records of address and purchase history despite the presence of a privacy policy. Among all respondents, 58.6% correctly answered false,

³¹ Joseph Turow, Lauren Feldman, & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, Annenberg Public Policy Center of the University of Pennsylvania, Jun, 1, 2005, available at <http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31>

and 58.7 of online shoppers answered false. Our small group of Privacy Unconcerned answered false unanimously, as did a high percentage of Privacy Fundamentalists.

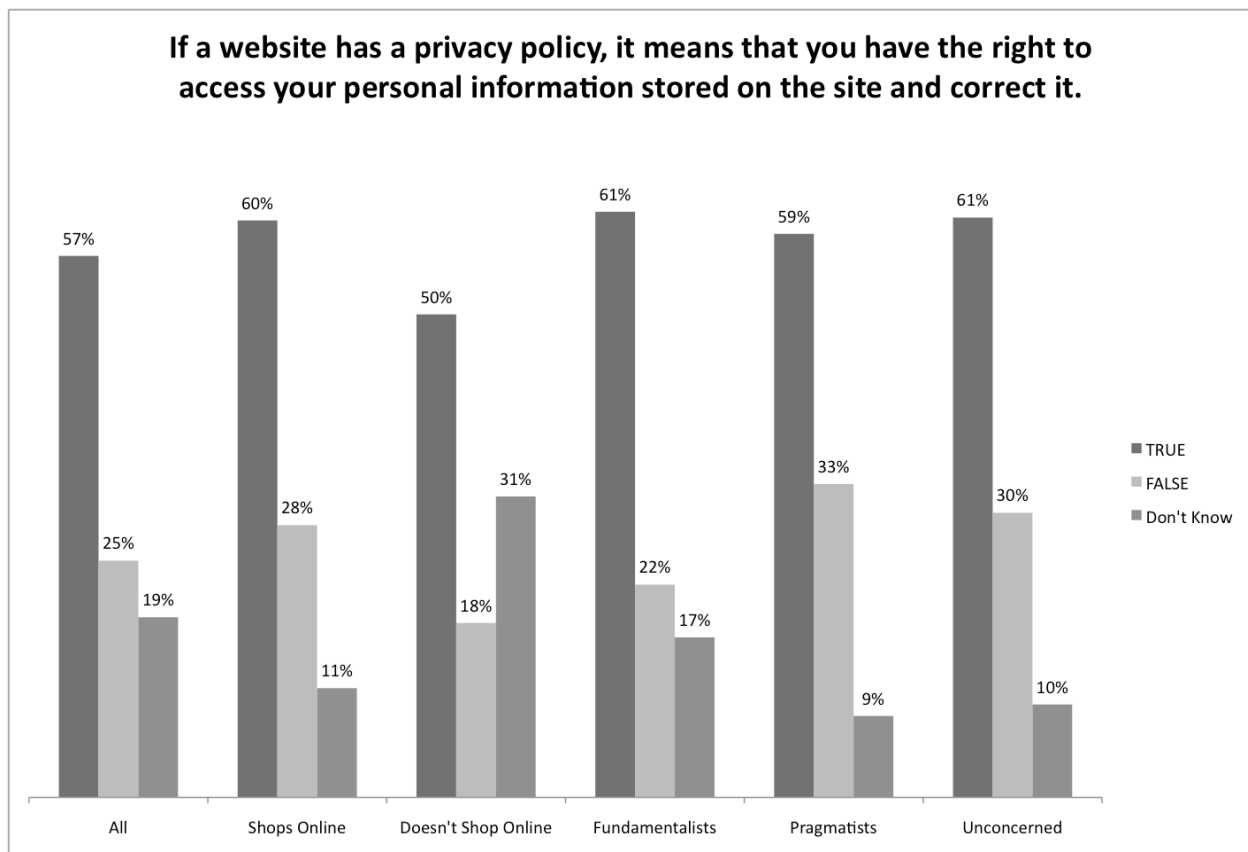
Access and Correction

Merely having a privacy policy does not give users a right to access and correct their data, although many e-commerce and other sites do allow some ability to review and change personal information. In 2003, Turow found that 94% of his sample of 1,200 American adults agreed or agreed strongly with the statement, “I should have a legal right to know everything that a website knows about me.”³² In 2005, Turow et al. found in their national sample of internet-using adults that 23% answered true to the statement, “Most online merchants give me the opportunity to see the information they gather about me.” Of the remaining respondents, 53% answered false and 25% said they didn’t know.³³

The majority of all of our respondents falsely believe that a privacy policy conveys access rights. Among all our respondents, 56.5% thought that privacy policies conveyed the right to access and correct personal information, and 18.8% did not know. Among online shoppers, 60.2% thought that such a right was guaranteed.

³² Joseph Turow, *Americans & Online Privacy, The System is Broken*, Annenberg Public Policy Center (June 2003), available at, [http://www.annenbergpublicpolicycenter.org/Downloads/Information And Society/20030701 America and Online Privacy/20030701 online privacy report.pdf](http://www.annenbergpublicpolicycenter.org/Downloads/Information%20And%20Society/20030701%20America%20and%20Online%20Privacy/20030701%20online%20privacy%20report.pdf).

³³ Joseph Turow, Lauren Feldman, & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, Annenberg Public Policy Center of the University of Pennsylvania, Jun, 1, 2005, available at <http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31>

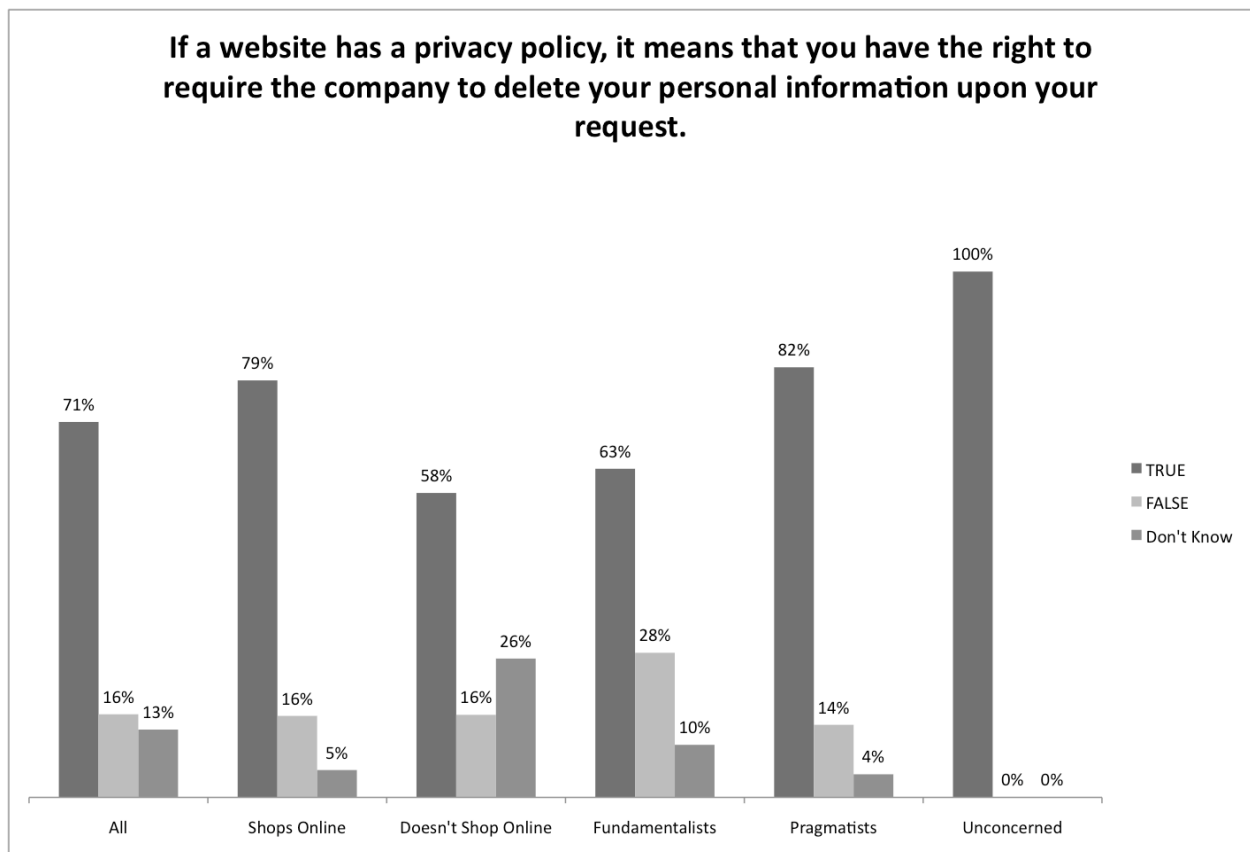


Right to Delete

In 2005, Turow et. al. found in their survey of internet-using adults that 19% incorrectly answered true to the statement, “Most online merchants allow me the opportunity to erase information they have gathered about me.” Of the remaining respondents, 50% answered false, and 30% said they didn’t know.³⁴

We asked Californians whether privacy policies guaranteed a right to delete personal information. Again, the majority of all respondents across all categories falsely believe that privacy policies convey a right to delete. Among all respondents, 71.4% incorrectly thought privacy policies guaranteed a deletion right. Online shoppers were more misinformed that such a right exists--79.3% answered true. Fundamentalists were far more likely to answer correctly (false) to this question than either Pragmatists or the Unconcerned.

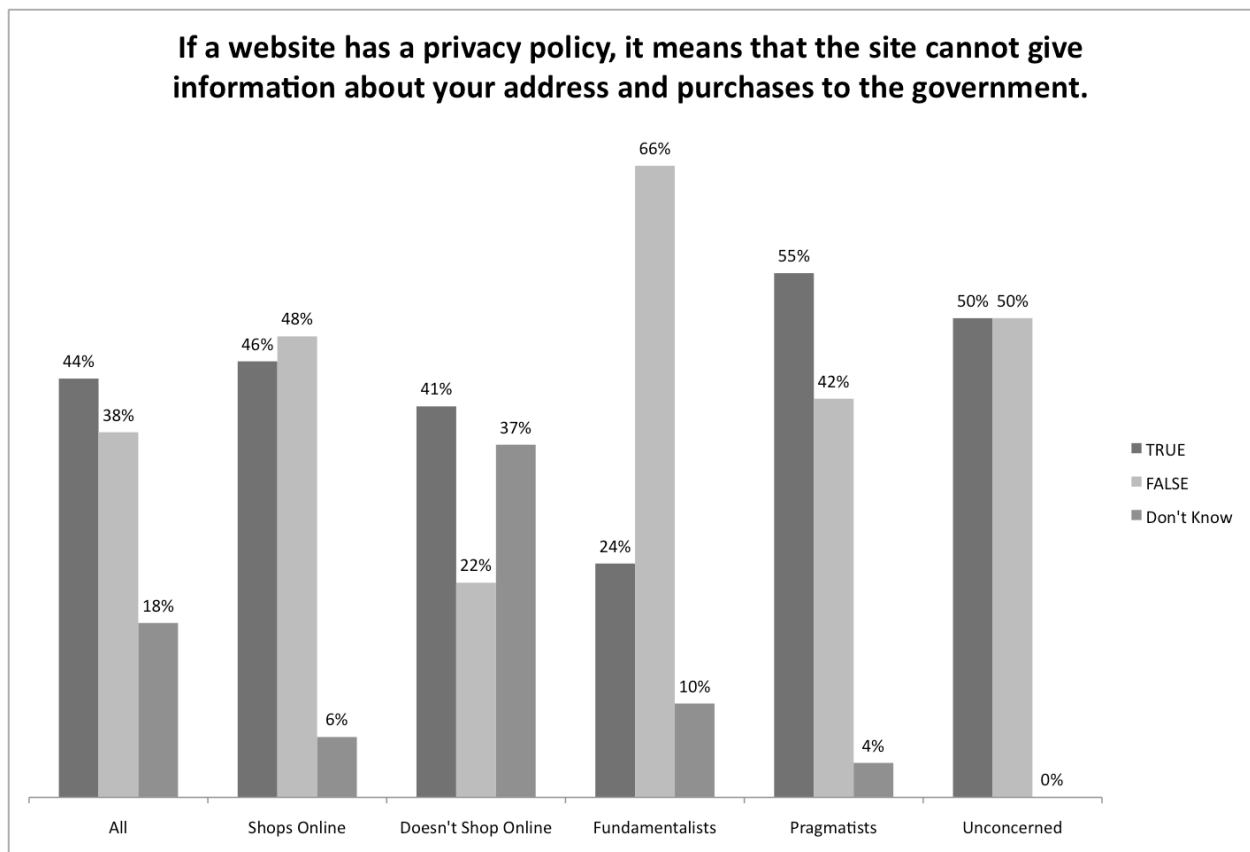
³⁴ Joseph Turow, Lauren Feldman, & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, Annenberg Public Policy Center of the University of Pennsylvania, Jun, 1, 2005, available at <http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31>



Government Access

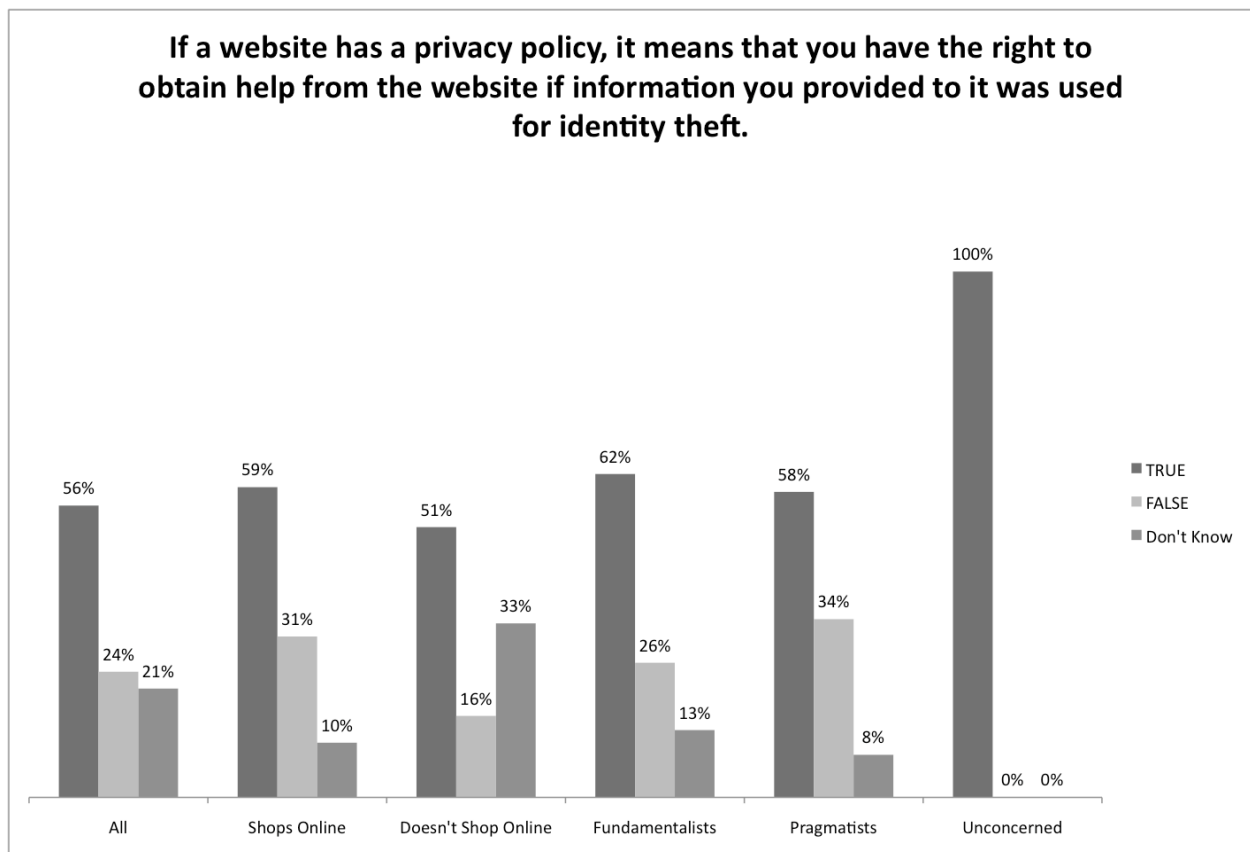
Websites with privacy policies often assert the right to provide personal information and transactional history in response to government requests. Depending on the status of the business involved, a sectoral privacy law may require law enforcement or other government requesters to obtain a court order before disclosure. In most cases, however, websites are free to voluntarily disclose details about customers without notification.

Many Californians, however, believe that privacy policies limit this practice. When asked of all respondents, 43.7% believed that privacy policies prohibited disclosure of personal information to the government, and 18.2% didn't know. Online shoppers were similarly ill-informed--45.5% thought that policies prohibited disclosure, and 6.3% didn't know. Privacy Fundamentalists strongly understood this practice was not prohibited by privacy policies, 66%, compared to only 42% of Pragmatists and 50% of the Unconcerned.



Assistance in the Event of Identity Theft

Providers of web services are under no legal obligation to help users who suffer from identity theft from security breaches or rogue employees who sell personal information. We asked Californians whether they thought privacy policies created such an obligation. The majority of respondents across all categories falsely believed that privacy policies obligated such assistance. When asked of all respondents, 55.5% thought that privacy policies obligated websites to help victims of identity theft, and 20.7% didn't know. Notably, 100% of our small sample of the Unconcerned falsely believed this was the case.



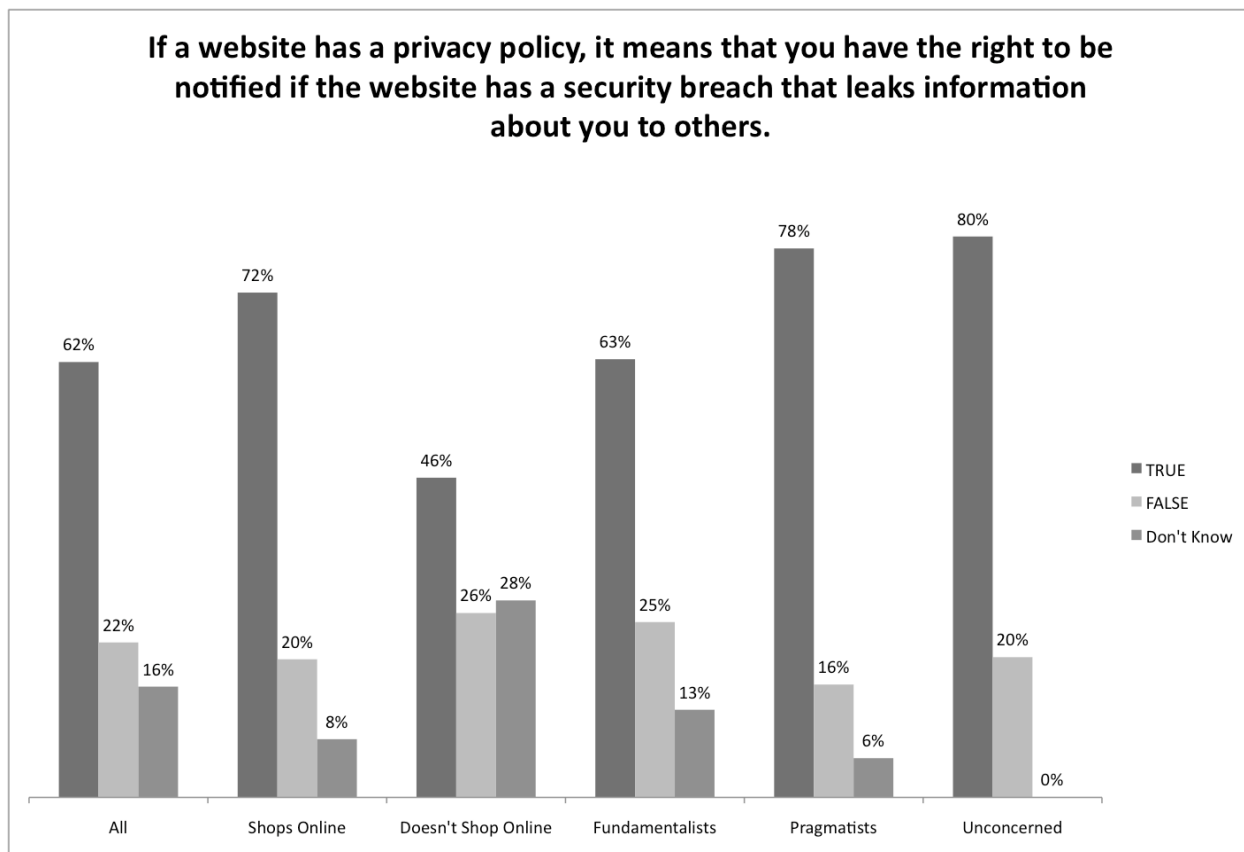
Notification of Security Breaches

Under California law, any entity that suffers an information security breach involving Social Security numbers, drivers license numbers, credit card numbers, or medical information must disclose to affected individuals that the breach occurred. This obligation is designed to give individuals warning of the risk of possible identity theft.

Privacy policies do not confer this right, and a website that does not possess these types of personal data need not disclose breaches of information security. We asked Californians whether they thought that privacy policies created such an obligation generally.

When asked of all respondents, 62.1% thought that privacy policies established an obligation to give notice of security breaches and 15.8% didn't know. Those who shopped online were more likely to think this obligation was present. Across all categories, Californians appeared to falsely believe a privacy policy conferred this right,

though among Westin segments Privacy Fundamentalists were more likely to answer correctly than Pragmatists or the Unconcerned.

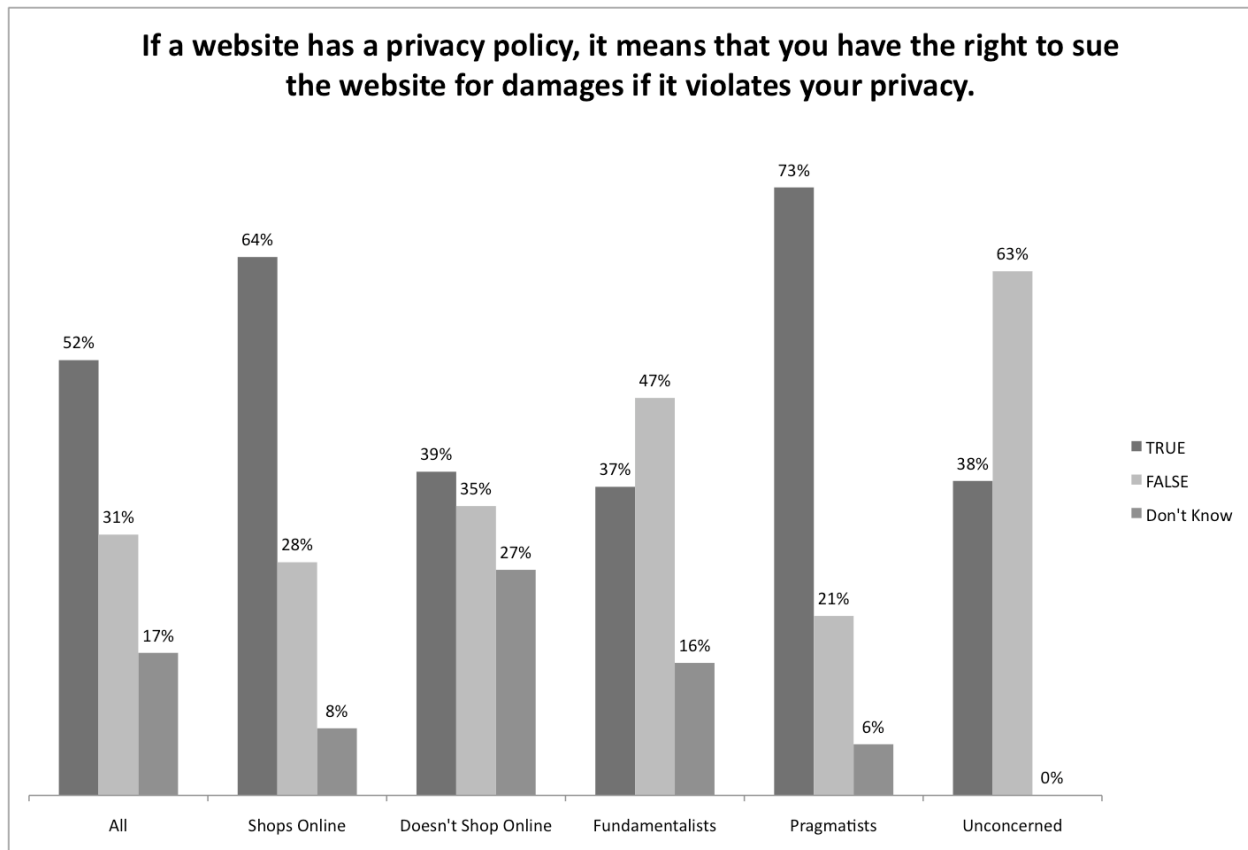


Right to Sue for Damages

Multiple actions brought by the Federal Trade Commission have firmly established that violation of a privacy policy could be both an unfair and deceptive trade practice. In California, a 2003 law required websites doing business in the State to post a privacy policy and to abide by promises made in it. Website operators who violate promises made in a privacy policy are subject to suit under the statute.

We asked Californians whether privacy policies conferred a right to sue for damages in the event of a privacy violation. When asked of all respondents, 51.9% thought privacy policies created a right to sue, and 17% didn't know. Online shoppers were more likely to believe they could sue for privacy violations.

Both Privacy Fundamentalists and the Unconcerned were skeptical that privacy policies created such a right, while the majority of Pragmatists answered "true."



Conclusion

In earlier work,³⁵ we argued that the Federal Trade Commission should police the term “privacy policy,” because consumers believed it conveys a baseline level of information practices. We drew an analogy to the regulations that govern use of the term “free.” Just as “free” means to the consumer that she has to pay nothing for a product or service,³⁶ “privacy policy” means that personal data about the consumer will not be sold to third parties.

This survey explores the meaning and misunderstandings of the term “privacy policy” among consumers. We found that many California consumers believe that privacy policies guarantee strong privacy rights. The term “privacy policy” is functioning

³⁵ Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good & Jens Grossklags, The Federal Trade Commission and Consumer Privacy in the Coming Decade, 3 ISJLP 723 (Winter 2007), available at <http://www.is-journal.org/V03I03/Turow.pdf>.

³⁶ Federal Trade Commission, FTC Guide Concerning Use of the Word ‘Free’ and Similar Representations, available at <http://www.ftc.gov/bcp/guides/free.htm>.

in consumers' minds as a privacy seal. A majority of Californians believe that privacy policies guarantee the right to require a website to delete personal information upon request, a general right to sue for damages, a right to be informed of security breaches, a right to assistance if identity theft occurs, and a right to access and correct data. In other cases, a majority believes that privacy policies prohibit common business practices, or simply doesn't know the answer to the question. For instance, a majority either doesn't know or believes that privacy policies prohibit third party information sale, affiliate sharing, government access to personal information, and enhancement.

It is unlikely that the Federal Trade Commission's self-regulatory posture will ever produce these rights, because it relies upon the assumptions that consumers read privacy policies, understand them, and then use privacy practices as a sorting mechanism to choose among competitors. This and other surveys provide an explanation as to why the Commission's approach is unlikely to work: consumers already think they enjoy these rights. They do not read privacy policies because they believe that they do not have to; to consumers, the mere presence of a privacy policy implies some level of often false privacy protection.

It is long past time to revisit this self-regulatory posture. It has resulted in wasted time and effort among companies that strive to formulate legally accurate and comprehensible privacy policies (that go unread and misunderstood by consumers). It positions consumers as unwitting participants in the sale of personal information, under the pretense of informed consumer choice. Consumers would benefit if the Commission explored better alternatives to the existing model.

Appendix I: Question Data

Note: All Westin segments are for online shoppers only except for Question 1.

Q1: How often do you shop online?						
	All	Fundamentalists	Pragmatists	Unconcerned		
Every Day	0.30%	0.50%	0.20%	0%		
Few/Week	4.40%	3%	4.40%	10%		
Few/Month	19.20%	21.10%	20.60%	20%		
Rarely	32.30%	27.80%	35.40%	26.70%		
Never	43.70%	47.80%	39.50%	43.30%		
	99.9%	100.2%	100.1%	100%		
	N=990	N=903				
Q2: If a website has a privacy policy, it means that the site cannot sell information about your address and purchase information to other companies.						
	All	Shops Online	Doesn't Shop Online	Fundamentalists	Pragmatists	Unconcerned
TRUE	47.30%	57.40%	31.30%	37.50%	61.10%	83.30%
FALSE	39.30%	37.30%	42.70%	54.20%	35%	16.70%
Don't Know	13.40%	5.40%	26%	8.30%	3.80%	0%
	100%	100.1%	100%	100%	99.9%	100%
	N=336	N=335		N=187		
Q3: 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.						
	All	Shops Online	Doesn't Shop Online	Fundamentalists	Pragmatists	Unconcerned
TRUE	47.30%	43.30%	51.70%	36.40%	43.10%	75%
FALSE	42.30%	51.20%	33.70%	59.10%	52.30%	12.50%
Don't Know	10.40%	5.50%	14.50%	4.50%	4.60%	12.50%
	100%	100%	99.9%	100%	100%	100%
	N=337	N=336		N=161		
Q4: 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.						
	All	Shops Online	Doesn't Shop Online	Fundamentalists	Pragmatists	Unconcerned
TRUE	36.80%	55.70%	22.30%	54.80%	55.70%	28.60%
FALSE	41.30%	37.10%	44.60%	38.70%	36.40%	71.40%
Don't Know	21.90%	7.10%	33.20%	6.50%	8%	0%
	100%	99.9%	100.1%	100%	100.1%	100%
	N=325	N=324		N=126		

Q5: If a website has a privacy policy, the site cannot use information to analyze your online activities.

	All	Shops Online	Doesn't Shop Online	Fundamentalists	Pragmatists	Unconcerned
TRUE	41%	35.40%	46.80%	20.50%	42.30%	42.90%
FALSE	41%	58.90%	23.40%	71.80%	52.90%	28.60%
Don't Know	18%	5.70%	29.70%	7.70%	4.80%	28.60%
	100%	100%	99.9%	100%	100%	100.1%
	N=317	N=316		N=150		

Q6: 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.

	All	Shops Online	Doesn't Shop Online	Fundamentalists	Pragmatists	Unconcerned
TRUE	42.40%	40.70%	44.80%	26.50%	44.20%	50%
FALSE	45.30%	52.30%	32.80%	58.80%	51.60%	50%
Don't Know	12.30%	7%	22.40%	14.70%	4.20%	0%
	100%	100%	100%	100%	100%	100%
	N=377	N= 377		N=228		

Q7: If a website has a privacy policy, it means that the site cannot keep records of your address and purchase history.

	All	Shops Online	Doesn't Shop Online	Fundamentalists	Pragmatists	Unconcerned
TRUE	23.90%	33.50%	12.70%	14.70%	42.10%	0%
FALSE	58.60%	58.70%	58.20%	73.50%	54.20%	100%
Don't Know	17.50%	7.70%	29.10%	11.80%	3.70%	0%
	100%	99.9%	100%	100%	100%	100%
	N=289	N=289		N=147		

Q8: 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.

	All	Shops Online	Doesn't Shop Online	Fundamentalists	Pragmatists	Unconcerned
TRUE	56.50%	60.20%	50.40%	61.10%	58.80%	60.50%
FALSE	24.70%	28.40%	18.20%	22.20%	32.70%	29.70%
Don't Know	18.80%	11.40%	31.40%	16.70%	8.50%	9.70%
	100%	100%	100%	100%	100%	99.9%
	N=323	N=332		N=195		

Q9: 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.

	All	Shops Online	Doesn't Shop Online	Fundamentalists	Pragmatists	Unconcerned
TRUE	71.40%	79.30%	57.90%	62.50%	81.80%	100%
FALSE	15.80%	15.50%	15.70%	27.50%	13.80%	0%
Don't Know	12.90%	5.20%	26.40%	10%	4.40%	0%
	100.1%	100%	100%	100%	100%	100%
	N=335	N=334		N=203		

Q10: If a website has a privacy policy, it means that the site cannot give information about your address and purchases to the government.

	All	Shops Online	Doesn't Shop Online	Fundamentalists	Pragmatists	Unconcerned
TRUE	43.70%	45.50%	40.80%	24.40%	54.70%	50%
FALSE	38.10%	48.10%	22.40%	65.90%	41.60%	50%
Don't Know	18.20%	6.30%	36.80%	9.80%	3.60%	0%
	100%	99.9%	100%	100.1%	99.9%	100%
	N=314	N=314		N=182		

Q11: 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.

	All	Shops Online	Doesn't Shop Online	Fundamentalists	Pragmatists	Unconcerned
TRUE	55.50%	59%	51.40%	61.50%	58.10%	100%
FALSE	23.90%	30.60%	15.50%	25.60%	33.90%	0%
Don't Know	20.70%	10.40%	33.10%	12.80%	8.10%	0%
	100.1%	100%	100%	99.9%	100.1%	100%
	N=315	N=315		N=167		

Q12: 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.

	All	Shops Online	Doesn't Shop Online	Fundamentalists	Pragmatists	Unconcerned
TRUE	62.10%	72%	45.60%	62.50%	78.30%	80%
FALSE	22.10%	19.70%	26.30%	25%	16.10%	20%
Don't Know	15.80%	8.30%	28.10%	12.50%	5.60%	0%
	100%	100%	100%	100%	100%	100%
	N=307	N=307		N=180		

Q13: 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.

	All	Shops Online	Doesn't Shop Online	Fundamentalists	Pragmatists	Unconcerned
TRUE	51.90%	64.20%	38.60%	36.80%	72.50%	37.50%
FALSE	31.10%	27.80%	34.50%	47.40%	21.40%	62.50%
Don't Know	17%	8%	26.90%	15.80%	6.10%	0%
	100%	100%	100%	100%	100%	100%
	N=359	N=358		N=177		

Appendix II: Westin Segmentation

In order to calculate membership in one of Westin's three privacy segments, we categorized respondents based on their answers to the following three questions, using Westin's rationale: "Privacy Fundamentalists are respondents who agreed (strongly or somewhat) with [Question 1] and disagreed (strongly or somewhat) with [Question 2 and Question 3]. Privacy Unconcerned are those respondents who disagreed with [Question 1] and agreed with [Question 2 and Question 3]. Privacy Pragmatists are all other respondents." Respondents who did not provide a valid answer for all three of these questions were considered invalid for the purposes of this categorization.

Westin Question 1: For each of the following statements, how strongly do you agree or disagree? First...

"Consumers have lost all control over how personal information is collected and used by companies."

Do you Strongly agree, agree, disagree, or strongly disagree?

Valid %	%	N	Value	Label
39.8	38.1	377	1	Strongly Agree
33.1	31.7	314	2	Agree
13.5	12.9	128	3	Disagree
13.7	13.1	130	4	Strongly Disagree
	4.1	41	8	Don't Know
		1	9	Refused/ Missing Data
100%		949/991 Valid Cases		

Mean: 2.01 Median: 2.0 Mode: 1 Std. Deviation: 1.039

Westin Question 2: How about...

"Most businesses handle the personal information they collect about consumers in a proper and confidential way."

Do you Strongly agree, agree, disagree, or strongly disagree?

Valid %	%	N	Value	Label
12.9	12.2	121	1	Strongly Agree
40.3	38.3	380	2	Agree
25.2	24	238	3	Disagree
21.6	20.5	204	4	Strongly Disagree
	4.8	48	8	Don't Know
		1	9	Missing Data
100%		942/991 Valid Cases		

Mean: 2.56 Median: 2.0 Mode: 2 Std. Deviation: .968

Westin Question 3: How about...

"Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today."

Do you Strongly agree, agree, disagree, or strongly disagree?

Valid %	%	N	Value	Label
10.9	10.2	101	1	Strongly Agree
46.8	43.7	433	2	Agree
26.4	24.7	244	3	Disagree
15.9	14.9	148	4	Strongly Disagree
	6.1	61	8	Don't Know
		4	9	Refused/ Missing Data
100%		926/991 Valid Cases		

Mean: 2.47 Median: 2.0 Mode: 2 Std. Deviation: .887

Appendix III: Related Reports

- *The FTC and Consumer Privacy In the Coming Decade*, Nov. 8, 2006, available at <http://www.law.berkeley.edu/samuelsclinic/privacy/48>, reprinted in Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good, & Jens Grossklags, *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 ISJLP 723 (2007).
- Joseph Turow, Deirdre K. Mulligan & Chris Jay Hoofnagle, *Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace*, Oct. 31, 2007, available at <http://www.law.berkeley.edu/samuelsclinic/privacy/216>.
- Chris Jay Hoofnagle & Jennifer King, *Consumer Information Sharing: Where the Sun Still Don't Shine*, Dec. 17, 2007, available at <http://www.law.berkeley.edu/samuelsclinic/privacy/219>.
- Jennifer King and Chris Jay Hoofnagle, *Research Report: A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information*, Apr. 18, 2008, available at <http://www.law.berkeley.edu/samuelsclinic/privacy/259>.
- Jennifer King and Chris Jay Hoofnagle, *Research Report: What Californians Understand About Privacy Offline*, May 15, 2008, available at <http://www.law.berkeley.edu/samuelsclinic/privacy/274>.