BEA
Educating for Tomorrow's Media

Routledge
Taylor & Francis Group

Check for updates

Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies, 2003–2015

Joseph Turow, Michael Hennessy, and Nora Draper

This paper examines the persistence of Americans' misunderstanding of the function of privacy policies. We also identify groups that have misplaced confidence in the privacy policy label and address whether the groups' patterns of misperception have changed over time. The findings add a new dimension to the argument that the usefulness of privacy policies needs to be reassessed. As a remedy, we call for media literacy programs to address structural features of media systems that lead to broadly held misperceptions such as the one examined here.

Webs sites and apps contain a legal document—typically called a privacy policy—that describes the extent to which and the ways in which the proprietors will, in the words of the Federal Trade Commission's (FTC) own privacy policy, "collect, use, share, and protect your personal information" (FTC, 2014). Although the FTC strongly encourages privacy policies, no systematic research exists on how people's interpretation of the presence of a privacy policy relates to their confidence that their digital information is adequately protected. Studies do imply that understanding of privacy policies is important because individuals are more likely to share information about themselves with organizations when they are confident that the organization will protect them from unwanted use of that information (Brandimarte, Acquisti, & Loewenstein, 2013). A hypothesis stemming from this idea is that people who believe the presence of a privacy policy limits the extent to which a Web site will share their information will also express satisfaction with the ability of existing laws and organizational practices to protect online privacy.

Joseph Turow *(Ph.D., University of Pennsylvania) is the Robert Lewis Shayon professor of Communication at the University of Pennsylvania's Annenberg School for Communication. His research interests include media systems; the production of culture; and the intersection of marketing, digital media, and society.*

Michael Hennessy *(Ph.D., Northwestern University) is a researcher at the Annenberg School for Communication. His research interests are the combination of structural equation modeling and intervention program/behavioral theory, growth curve analysis of longitudinal data, and using factorial surveys to design effective behavioral intervention programs.*

Nora Draper *(Ph.D., University of Pennsylvania) is an assistant professor of Communication at the University of New Hampshire. Her research examines the influence of institutional forces on privacy, surveillance, reputation, and identity.*

Journal of Broadcasting & Electronic Media 62(3), 2018, pp. 461–478
DOI: https://doi.org/10.1080/08838151.2018.1451867 *ISSN: 0883-8151 print/1550-6878 online*

This paper evaluates that hypothesis by using the findings from the University of Pennsylvania's Annenberg School's national random surveys of Americans during 2009, 2012, and 2015. Each of these surveys presented respondents with a true-false question that asks: if a Web site has a privacy policy, does it mean the site will not share visitors' information with other sites without their permission. We analyze the relationship between 1) respondents' confidence that the presence of a privacy policy means they are protected from information sharing, and 2) the belief that regulations of privacy by government and other organizations need no change. We also examine the changes in Americans' understanding of *privacy policy* over time and test the extent to which socio-demographics such as gender, age, income, race, and education predict knowledge about the meaning of a privacy policy. The findings shed light on the misplaced confidence most Americans have in a label purportedly used to enlighten them. They also point to new initiatives the FTC might take under its mandate to redress deception in the marketplace—as well as indicating the need for literacy programs—that focus on digital media policy.

Background

The first mention of a Web site privacy policy in an FTC press release is dated 4 June 1998. Titled "FTC Releases Report on Consumers' Online Privacy," it describes a report about privacy online that the Commission had provided to Congress. After three years of study, the Commission concluded that "consumers have little privacy protection on the Internet" and that "industry's efforts to encourage voluntary adoption of the most basic fair information practices have fallen short of what is needed to protect consumers" (FTC, 1998). To this point, Congress had been relying on online advertisers, data brokers, and retailers to regulate their own collection and use of information collected about consumer behaviors. Based on a series of workshops and hearings, the Commission states, "studies have concluded" that there are four information practice principles that "are widely accepted as essential to ensuring that the collection, use, and dissemination of personal information are conducted fairly and in a manner consistent with consumer privacy interests" (FTC, 1998). These principles are notice, choice, access, and security. The FTC emphasized that at the time only 14% of 1,400 U.S. Web sites studied provided information allowing consumers to learn what they do with visitor data and what choices visitors have regarding those uses (FTC, 1998). The years after the release of the FTC report saw increased postings by Web sites of documents that detailed data disclosure practices. One study confirmed the mention of such practices rose from 1999 and 2000, from 66.8% to 86.1%, but the number decreased to 68.6% in 2001. The study found an increase from 48.3% in 1999 to 76.7% in 2001 in the adoption of privacy policy notices (Milne & Culnan, 2002, p. 352); these notices are typically placed in small letters associated with a link at the bottom of the home page.

The Privacy Policy and the Public

Despite the rise in the proportion of Web sites posting privacy policies, academic researchers have argued the public is largely unable to make sense of these documents. Culnan and Milne (2001), for example, found that while a majority of Americans read privacy policies, most found the documents long and the language confusing. Another survey (Turow, Feldman, & Meltzer, 2005) found that 70 percent of respondents disagreed with the statement "privacy policies are easy to understand." This lack of understanding is compounded by the fact that most people skip over the privacy policies or take too little time to read them in enough depth to extract their intended meaning (Obar & Oeldorf-Hirsch, 2016; also Barocas & Nissenbaum, 2009; Reidenberg et al., 2015). Indeed, McDonald and Cranor (2008) determined that if Internet users read every privacy policy they encountered online, they would spend 25 days a year engaged in this activity. Solove concludes that most people do not read privacy policies; that those who read them do not understand them; that those who read and understand them often lack enough background knowledge to make an informed choice; and that even those who can make an informed choice might have that choice skewed by various decision-making difficulties (2013, p. 1888).

But before attempting to read and make sense of privacy policies, Americans must have a reason for clicking on them. Past research has examined whether the public has reason to engage with these documents by presenting questions to see if Americans understand what the presence of a privacy policy signifies. For example, a 2005 Annenberg national survey asked American adults about the following statement: "When a web site has a privacy policy, I know that the site will not share my information with other Web sites or companies" (Turow et al., 2005). Similarly, in 2014 a Pew Research survey asked a representative sample of U.S. adults whether they agreed or disagreed with the following statement: "When a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users" (Smith, 2014). In both cases, results showed that the American public overestimates the protections afforded by the presence of these documents on a webpage.

Although certain results of these surveys received wide attention in the popular press, the findings about Americans' understanding of what "privacy policy" means did not. Nor have policymakers or academics taken note of what are consistent findings across the 12 years. One goal of this paper is to integrate the findings of these surveys to address a theoretically guided question regarding the relationship between people's confidence in the meaning of a regulatory label such as "privacy policy" and their satisfaction with existing privacy protections. At issue is whether the confidence in the privacy policy label predicts acceptance of the regulatory status quo.

Although available research doesn't speak directly to the connection between a sense of adequate privacy protection and satisfaction with existing privacy regulation, previous work does provide direction toward a hypothesis. Especially relevant is

literature about *meta-cognition*—the processes involved in knowing what we know (Metcalfe & Shimamura, 1996). An important aspect of this phenomenon is "the illusion of knowing." That is the circumstance when an individual's self-assessment of comprehension is high, while a factual assessment of the person's comprehension reveals it to be low. The consequences can hold important public policy implications. Brandimarte et al. (2013) conducted experiments showing that people are more likely to share data if they are confident that they have control over how their data are released and accessed. They also found that when people have misplaced confidence in controlling the release of their information, it can distract them from the possibility of unwanted uses of their data. Summarizing research on this topic in relation to privacy, Solove adds: "People are also more willing to share personal data whey they feel in control, regardless of whether that control is real or illusory" (Solove, 2013, p. 1887). More generally, he notes, "people are more willing to take risks, and judge those risks as less severe, when they feel in control" (2013, p. 1887).

These research streams lead to the hypothesis that people who hold misplaced confidence in the "privacy policy" label are more likely than those who correctly understand the label to state that existing laws and organizational practices for protecting online privacy are adequate. An obvious question is whether the extent of misplaced confidence in the label or opinion about government regulation varies based on sociodemographic differences. Brandimarte and colleagues (2013) imply their experimental results about sharing data in the face of privacy opinions will hold with people of all backgrounds. Yet research over the past couple of decades on people's understanding how to use computers (their "computer literacy") as well as their ability to navigate internet browsers and related tasks (their "online fluency") has sometimes found sociodemographic variables such as age, gender, education, and income significant for distinguishing among those who are successful and unsuccessful (see, for example, Freese, Rivas, & Hargittai, 2006; Hargittai, 2005; Hargittai & Hinnant, 2008; Mossberger, Tolbert, & Stansbury, 2003; Van Dijk, 2005).

Age and gender are the categories that stand out most, though with gender the findings are conflicting. Park (2013), for example, looked at the impact of income, education, age, and gender on two aspects of a national survey of American adults' personal information-control activities: their social skills (for example, giving a false email address or asking a site not to share personal information with other companies) and technical skills (for example, clearing the Web browser history or erasing some or all cookies on the computer). He found that being male and relatively young (lower than the median age 46) predicted technical skills, while relative youth alone predicted social skills (Park, 2013, pp. 225–228). Litt (2013) found a similar age pattern in studying the predictors of privacy tool use on social networks such as Facebook—but not education, income, and race—noting that older individuals were less likely to use technological strategies than younger individuals. Alternatively, Litt's study reported that women were more likely than men to use privacy tools. In research on Internet knowledge and activities, the nature of gender differences appear to be quite specific to the topic studied. Fogel and Nehmad (2009) found,

for example, that females used more privacy controls than males, while Hargittai and Hinnant (2008) observed that being female predicts lower self-reported understanding of Internet terms and actions.

Note that these studies tried to predict individuals' Internet activities rather than their policy position—the purpose of this study. Nevertheless, the available evidence does suggest a second hypothesis: that people's misplaced confidence in the privacy policy label and their related opinions about the need for more effective laws and organizational practices to protect privacy will vary, based on age and gender but not by education, income, and/or race.

Methods

We proceeded with our investigation in two steps. First, we gathered all questions about the meaning of "privacy policy" from a Pew Research survey (Smith, 2014) and the national telephone surveys carried out by the University of Pennsylvania's Annenberg School for Communication in 2003, 2005, 2009, 2012, and 2015. Several of the studies that tap the meaning of "privacy policy" have substantially different wording or choices, which impedes an exploration of the patterns in percentages of Americans who make incorrect choices about the meaning of the term "privacy policy." There are, however, three exceptions. The Annenberg School conducted national telephone surveys in 2009, 2012, and 2015 that presented virtually the same true/false statement: In 2009 and 2012 the statement was "If a website has a privacy policy, the site cannot share information about you with other companies, unless you give the website your permission." In 2015 it was "When a website has a privacy policy, it means the site will not share my information with other websites or companies without my permission."

After an overview of the general findings from all the surveys, we chose the 2009, 2012, and 2015 Annenberg surveys for close demographic analysis over time; data for all three surveys were collected by the Princeton Survey Research Associates. The surveys included: (1) 1,000 U.S. Internet users in 2009 (see Turow, King, Hoofnagle, & Hennessy, 2009), (2) 1,503 adult Internet users in 2012 (see Turow, Delli Carpini, Draper, & Howard-Williams, 2012), and (3) 1,506 Internet users in 2015 (Turow, Hennessy, & Draper, 2015). *Internet users* are defined as people who use the Internet or email "at least occasionally." Survey participants were contacted on both landline and wireless phones and the interviews averaged 20 minutes. When it came to asking the privacy-policy question, the response category of "not sure" was included as a choice rather than a volunteered answer. Since our hypotheses center on the "incorrect answers" to the privacy policy questions as indicators of misplaced confidence, we did not include the "unsure" answers in the analysis, which made up 13% of the responses across the three surveys.

The 2009 and 2012 Annenberg surveys both presented the following statement and asked those interviewed if they "agree," "agree strongly," "disagree," or "disagree strongly": "Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today." This question comes from an

attempt to replicate a standard set of questions used by the pioneering privacy theorist Alan Westin (Kumaraguru & Cranor, 2005). Here we used the answers to address our hypothesis that a relationship exists between not knowing the meaning of "privacy policy" and satisfaction with current regulation of the Internet industry's data sharing practices. Although the phrase "existing laws and organizational practices" combines two realms of action, it reflects a proxy for how the privacy issue is perceived by Internet users at large.

Statistical Analysis

All our analyses were conducted with Stata. We used probit regressions to predict the incorrect (that is, the "True") response and to identify the relationships between sociodemographic selection of incorrect answers during different years, adjusted for the other variables. Because the probit regression coefficients are Z scores and are nonlinearly related to the underlying probabilities of choosing the incorrect answer, we plot the marginal effects of time and the demographic variables using the Stata command "marginsplot". These plots are a completely deterministic function of the estimated regression; that is, they are simply a transformation of the estimated probit regression coefficients. To determine if the effects of demographic variables on the incorrect choice changed over time, we look for interaction effects (e.g., moderation) between year of the study, the demographic variables, and the outcome choice. Here plots of demographic effects by year are extremely informative.

Results

Table 1 presents the percentage of incorrect answers to the privacy policy questions asked in surveys of American adults who "use the internet" conducted from 2003 through 2015 (Smith, 2014; Turow, 2003; Turow, Feldman, & Meltzer, 2005; Turow, King, Hoofnagle, & Hennessy, 2009; Turow, Delli Carpini, Draper, & Howard-Williams, 2012; Turow, Hennessy, & Draper, 2015). The phrasings vary somewhat, and the 2003 question asked whether the respondent agreed or disagreed with the statement, as opposed to the true-false formulation of the other years. Nevertheless, over half of the respondents in every year said the statement is true when it is false (or, in the case of 2003, agreed with the statement when it was incorrect). In four of the years, the percentage of people choosing the wrong answer reached above 60%, and in two of those years it passed 70%. The years with relatively lower percentages involved the most unusual approaches to the question: the 2003 request for an agree/disagree answer, and the 2014 Pew statement that used an exceptionally strict formulation of the privacy policy's meaning via the phrase "ensures that the company keeps confidential all the information it collects" (Smith, 2014). The overall impression is clear, though: Despite differences in the

Table 1
Probit Regression Predicting that Existing Laws Provide Reasonable Protection

	Survey Creator & Sample Size*	Phrasing	% Incorrect Answer
2003	Annenberg (N=1,155)	When a web site has a privacy policy, I know that the site will not share my information with other websites or companies.	59% agree or agree strongly
2005	Annenberg (N=1,257)	When a website has a privacy policy, it means the site will not share my information with other websites or companies.	71% true
2009	Annenberg (N=842)	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.	73% true
2012	Annenberg (N=1,228)	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.	65% true
2014	Pew (N=1,034)	When a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users.	54% true
2015	Annenberg (N=1,399)	When a web site has a privacy policy, it means the site will not share my information with other websites or companies without my permission.	63% true

*Does not include Don't Know/Not Sure or No Response

expression of the meaning of a privacy policy, well over half of American adults in six surveys across thirteen years mistake the meaning of a privacy policy.

To get a deeper view of patterns over time and among different population segments, we turn to the three years when the questions and choices were almost the same: 2009, 2012, and 2015. Table 2 presents the true-false responses to the statements in each of the three years. It indicates that there is a statistically significant decrease across the years in the proportion of people who choose "true" over "false"—from 73.4% in 2009 to 65.2% in 2012 and 62.7% in 2015. Table 3 shows that the chances of being wrong were not distributed evenly across key categories of the population; negative coefficients reflect selecting the correct answer, "false." The table shows that men are statistically more likely than women to pick the correct answer; that people with higher education are more likely than those of lower levels (HS graduate or less) to select the correct answer; and that the people making

Table 2
Privacy Policy Responses: 2009–2015

If a Web site has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the Web site your permission.

	Year		
	2009	2012	2015
True	73.4%	65.2%	62.7%
False*	26.6%	34.8%	37.3%
* Correct answer			
N	842	1228	1399
Pearson χ^2: = 27.58, df = 2, p < .05			

The 2015 version was "When a web site has a privacy policy, it means the site will not share my information with other Web sites or companies without my permission."

$100,000 or more annually are statistically more likely to answer correctly than people making less than $100,000. White respondents are more likely than others to know the correct answer. Respondents who identify as neither Black nor White (for example, Asians and Native Americans) are likely to get the answer wrong. Black respondents are also likely to answer incorrectly; however, in the case of Black respondents, the relationship is not statistically significant. People of all age categories tend to get the answer wrong; differences between them are also not statistically significant. These relationships are displayed graphically in Figure 1.

To identify changes over time, we investigated the extent to which these five demographic variables interact with the year of the study. F tests show that none of these interactions approached statistical significance. In view of the large sample, this is convincing evidence that relationships among the responses of different demographic groups have not changed over time. Figure 2 displays the results shown in Table 3 by year. The charts show that differences between the demographic categories that we saw in Figure 1 persist in every year. Young adults, people with low income, people with less than a college education, women, Blacks, and ethnic non-whites go down in their misunderstanding (that is, a higher percentage get the answer correct) from 2009 to 2012 to 2015. Because there is no interaction, their improvement in knowledge does not catch up with the improvement that older, richer, male, White respondents, and more highly educated American adults show in their knowledge. Note that even with the general decline in selecting the incorrect answer, the adjusted predicted values for the incorrect answer is always greater than 50% in the samples. It's a reminder that despite the decline in incorrect answers, most Americans still have misplaced assurance about giving up their data when they see the privacy policy label.

Table 3
Probit Regression Predicting the Incorrect Privacy Policy Choice

	Coefficient	SE	T	P	95% Confidence Interval	
Male	−.137	.056	−2.45	.014	−.248	−.027
Age						
26–40	−.082	.094	−.87	.383	−.267	.103
41–55	−.043	.092	−.47	.638	−.224	.137
56–66	−.144	.102	−1.41	.159	−.344	.056
67+	−.023	.106	−.22	.824	−.231	.184
Income (Ks)						
20 to <30	−.085	.117	−.73	.467	−.314	.144
30 to <40	−.114	.117	−.97	.332	−.343	.116
40 to <50	.002	.122	0.18	.855	−.217	.262
50 to <75	−.165	.108	−1.53	.126	−.378	.046
75 to <100	−.141	.111	−1.26	.207	−.359	.078
100K+	−.207	.105	−1.97	.049	−.413	−.001
Education						
Some college	−.161	.076	−2.12	.034	−.310	−.012
College plus+	−.272	.076	−3.59	.001	−.421	−.123
Race						
Black	.110	.095	1.16	.247	−.076	.226
Non-Black / Non-White	.229	.081	2.82	.005	.071	.389
Year						
2012	−.182	.076	−2.41	.016	−.332	−.034
2015	−.255	.075	−3.41	.001	−.402	−.108
Intercept	.924	.116	7.96	-	.697	1.153

Note. N = 2,803. $F_{17,\ 2786} = 3.85$, $p < .05$, (McKelvey and Zavoina $R^2 = .055$). Negative coefficients indicate selecting the correct answer, positive coefficients the incorrect answer.

This general high level of misplaced comfort also associates with a belief that "Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today." As Table 4 indicates, about 60% in 2009 and 2012 who misunderstand the privacy policy label agree or agree strongly with that statement. In contrast, around 58% of those in both years who know the label's correct meaning disagree or disagree strongly with the statement. This consistent difference applies equally across the demographic categories presented earlier. Table 5 associates the demographics of people who got the label wrong with their belief that laws provide reasonable protection. This table shows that the only statistical difference we found related to age. Specifically, 18–24-year-olds who believe the privacy policy is protective are substantially more likely than other age groups to generalize that existing laws and organizational practices provide reasonable protection.

Figure 1
Probability of Incorrect Privacy Policy Answer by Year and Respondent Characteristics

Note: Dashed line is 50%. Brackets are 95% confidence intervals around the predicted value.

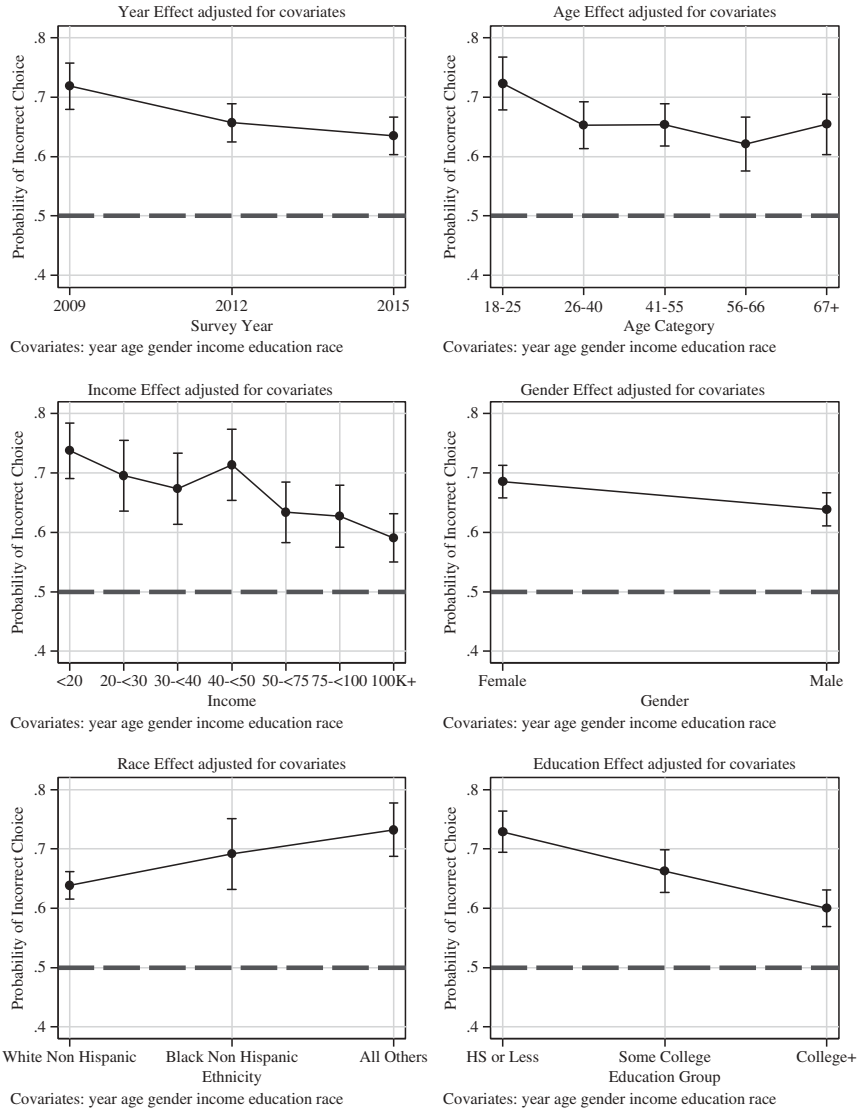

Figure 2
Probability of Incorrect Privacy Policy Answer Choice by Respondent Characteristic over Time

Note. Dashed line is 50%. Confidence intervals around predicted values not shown for clarity.

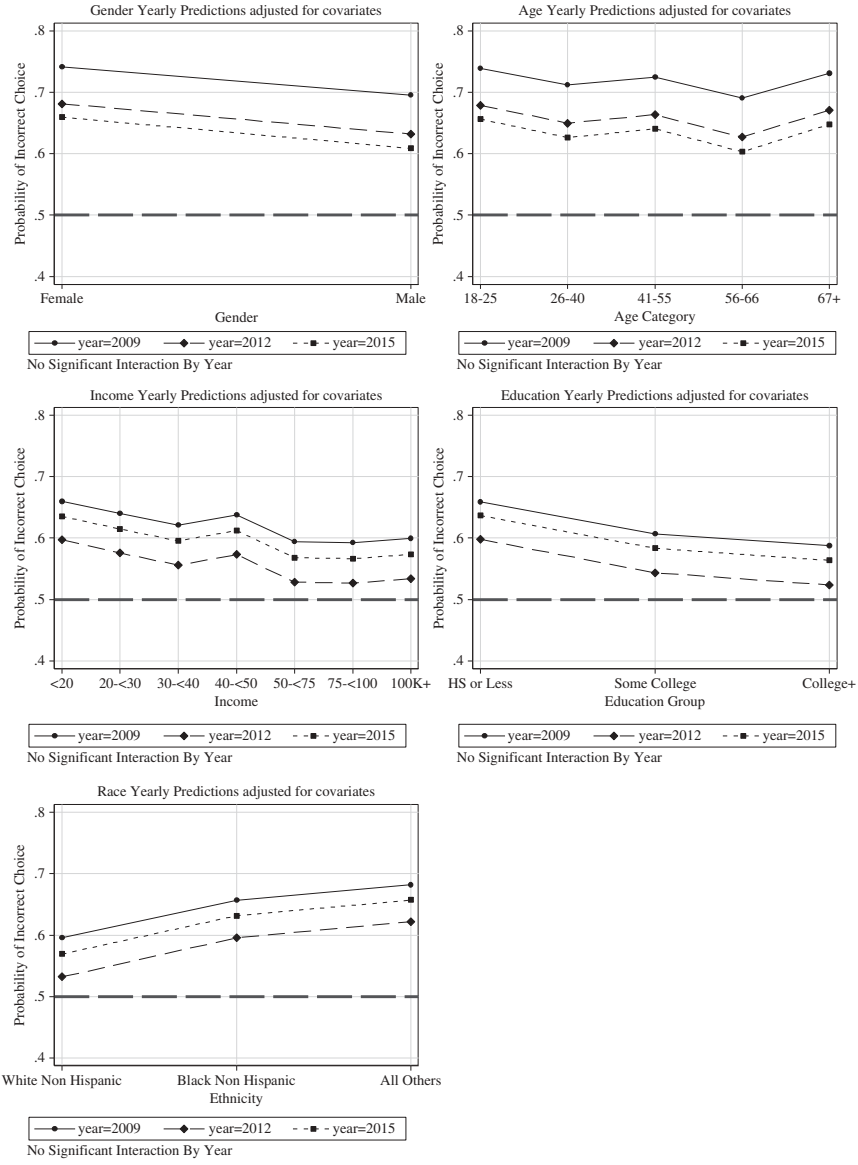

Table 4
Association of True/False Answers regarding Privacy Policy Statement with Agreeing or Disagreeing that "Existing Laws and Organizational Practices Provide a Reasonable Level of Protection for Consumer Privacy Today."

	Privacy policies protect personal data			
	2009		2012	
"Existing laws provide protection"	True (%)	False (%)	True (%)	False (%)
Agree or agree strongly	62	44	62	40
Disagree or disagree strongly	38	57	38	60
	N = 599	N = 222	N = 776	N = 424
Polychoric correlation	.28 ($p < .05$)		.34 ($p < .05$)	

Table 5
Probit Regression Predicting that Existing Laws Provide Reasonable Protection

	Coefficient	SE	T	P	[95% Confidence Interval]	
Male	.014	.091	0.15	0.877	−.164	.192
Age						
25–40	−.4219	.151	−2.78	0.005	−.719	−.124
41–55	−.469	.153	−3.06	0.002	−.770	−.168
56–66	−.592	.164	−3.61	0.000	−.914	−.270
67+	−.420	.188	−2.23	0.026	−.790	−.050
Income (Ks)						
20-<30	−.277	.177	−1.57	0.117	−.625	.069
30-<40	−.155	.178	−0.87	0.382	−.505	.194
40-<50	.068	.184	0.37	0.709	−.293	.431
50-<75	−.164	.172	−0.95	0.341	−.502	.173
75-<100	−.015	.182	−0.09	0.931	−.374	.342
100K+	−.229	.164	−1.39	0.165	−.552	.094
Education						
Some college	−.148	.117	−1.26	0.207	−.378	.082
College+	−.029	.116	−0.26	0.798	−.257	.198
Race						
Black	|-.064	.154	−0.42	0.677	−.367	.238
Non-Black / Non-White	.010	.124	0.08	0.935	−.233	.253
Year						
2012	−.003	.091	−0.04	0.967	−.182	.175
Intercept	.914	.175	5.21	0.000	.570	1.259

Note. N = 1075. $F_{16,1059} = 1.61$. p = 0.06, (McKelvey and Zavoina $R^2 = .055$). Negative coefficients indicate existing laws not reasonable, and positive coefficients indicate existing laws are reasonable.

Conclusion

That young adults who misunderstand the privacy policy label are more likely than their older adult counterparts to believe current data protection regulations are reasonable is noteworthy because of the great amount of public concern about young adults' willingness to give up too much private information online. It also contradicts the idea that those born in generations with widespread access to digital tools—sometimes called digital natives—have greater knowledge about how to control their online environment. Research has demonstrated that young people have deep concerns about their digital privacy (Turow et al., 2009) and have developed tools and strategies they feel provide them with some, often limited, protections (Berriman & Thomson, 2015; Boyd, 2014). Still, the results presented here suggest young adults share with the broader population a misplaced confidence in the presence of privacy policies as well as in the broader adequacy of regulations and organizational policies relating to them.

Our study has shown remarkable consistency with respect to misplaced understanding of the privacy policy label over a 12-year span. Across our 6-year comparison (2009–2015), it has also shown a consistent overlap between those who misunderstand privacy policies and have a belief that their personal information is adequately protected by existing laws and regulations. Earlier we introduced research that found people are more likely to behave in ways that open them to harm when they feel they are adequately protected rather than when they don't feel that way. The application of this general principle to online behaviors that can introduce risk into the privacy and security of one's personal information highlights the importance of the current study's findings. The substantial percentage of the population that feels it is protected by both privacy policies and existing laws may engage in riskier behaviors regarding their personal information. The fact that tech-conscious young adults are overrepresented in the group that feels privacy policies protect their information from being shared with third parties suggests that misunderstandings are not a function of a lack of familiarity with the technologies themselves, for, as we have seen, other studies associate younger age with higher technological knowledge and more skills than their older counterparts. The misplaced confidence may instead represent a misunderstanding about the ways digital firms manage the information world that underlies these technologies.

The finding that age is a predictor of the second of the two hypotheses resonates with the results of other studies that age is an important variable in understanding people's approaches to the Internet environment—though not necessarily in consistent ways. Gender, the other variable that Internet studies often emphasize as predictive, is also a significant factor in this research: men are more likely than women to know the correct answer about the meaning of the privacy-policy label. The finding meshes with some studies that see men as more knowledgeable or skillful than women on Internet topics, but it runs counter to others that note women as more proactive than men about using privacy controls. Our finding reinforces the observation, made earlier, that in research on Internet knowledge and activities, the

nature of gender differences appears to be quite specific to the topic studied. The current research reinforces the need to conceptualize dynamics of gender through a framework that explains these contrasting findings and suggests research to address their social implications. A conceptual framework of this sort would similarly be useful to understand the contrasting findings regarding age and the Internet.

Our study found other sociodemographic categories operating here that other studies don't note: people with higher education are more likely than those of lower levels (HS graduate or less) to select the correct answer; people making $100,000 or more annually are statistically more likely to answer correctly than people making less than $100,000; White respondents are more likely than others to know the correct answer; and respondents who identified as neither Black nor White (for example, Asians and Native Americans) are likely to get the answer wrong. An obvious commonality among many of these classifications is their relation to social status and power. More research is needed about the reasons for these differences. Another point of difference for future exploration relates to whether technological skills, social-environmental factors such as a person's access to multiple Internet devices, ability to use devices in many locations, and the availability of high-speed broadband predict correct understanding of the privacy-policy label. Prior studies (for example Hargittai & Hinnant, 2008; Litt, 2013; Park, 2013) suggest that these considerations might influence people's privacy-related activities and understandings. Although one or another of the Annenberg surveys gathered such information about respondents, the data weren't collected across all of the surveys and so could not be used for this study's analyses.

Consideration of sociodemographic, skill-related, and environmental factors should not, however, detract from the strongest finding of this research: large percentages of Americans irrespective of their backgrounds do not understand the most basic element of privacy notification. Moreover, this error associates with an unsubstantiated belief that "Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today." Improved education around various elements of digital life has been at the heart of calls from those invested in improving safety and security online (see for example Hobbs, 2010; Livingstone, Byrne, & Bulger, 2015). Our findings here suggest that such activities have to start with the most basic features—for example, the very meaning of the label "privacy policy".

The association we found between the misinterpretation of the label and a belief that existing privacy rules are adequate points to another aspect of public education about these issues. Academic researchers have sometimes critiqued digital literacy proponents for focusing on individual knowledge at the expense of encouraging changes to the structural and institutional systems that enable undesirable practices. Livingstone argues that approaches to literacy must incorporate an understanding of the social and institutional structures that encourage certain kinds of awareness of the media system but not others (2004, p. 11). Shade and Shepard (2013) push the point further. They argue that digital-policy literacy, which stresses understanding of

communication policy processes, the political economy of media, and technological infrastructures, is an essential but often overlooked part of digital-literacy campaigns.

Our study points to the importance of this approach. We found that people's misplaced confidence about an Internet feature as basic as a privacy-policy label not only has implications for their personal lives, but also may affect how they act as citizens in favor or against government or corporate activities. Digital literacy programs therefore should find ways to highlight the societal implications of this most basic aspect of the new-media landscape with the knowledge that many people need help understanding the mundane policy features of this new world.

Unfortunately, activities spreading either the individual or the societal orientation toward the meaning of privacy policy are so far rather scarce. Anecdotal evidence suggests that reviews of Web sites in the popular media almost never comment on privacy policies, and journalists who write about privacy issues rarely address privacy policies. The situation appears no better in formal educational settings. According to digital-literacy expert and professor Hobbs (personal communication, 2016), approaches to digital literacy in U.S. elementary, middle, and high schools (grades K through 12) are divided between schoolroom teachers and information-technology administrators. The former see developing students' basic computer and Internet skills as their mandate. The latter have additional concerns about implementing privacy and security in the classroom, especially as school districts choose among the many educational applications being offered to them. Hobbs notes that at recent educational technology conferences some K–12 teachers have shown up as "early adopters" who have aligned themselves with the concerns of the IT administrators and have begun thinking about digital citizenship and privacy as important classroom topics. They are, she emphasizes "a very special group, not typical classroom teachers." Moreover, when the early adopters get into dialog with the other teachers in their school systems, the basic skills perspective clashes with the larger societal one. "They literally cannot understand each other," Hobbs reports.

Activities to bridge the gaps between the early adopter and regular classroom teachers about the importance and meaning of privacy policies are clearly necessary. One possible way to spark an interest involves getting them engaged with the privacy policies of the educational apps their districts are evaluating for use in their classrooms. Critics of some of these apps have expressed concern that they can collect massive amounts of student "metadata"—including what students type and click that might include information about the type and times of classroom activities and homework—and resell the data for purposes teachers and administrators may not like (Herold, 2014). In association with a number of school districts, Common Sense Media has come up with a rating system to help administrators and teachers evaluate privacy policies (Common Sense Media, n.d.; Herold, 2014). Encouraging teachers in appropriate grades to explore the rating system and discuss its implications with their students can be a useful first step in sensitizing the younger generation to the varied meanings of the very term privacy policy.

One might think that engagement with such privacy policy ratings need not stop with teachers and their students. Yet attempts at ratings have been tried—P3P and Privacy Choice are two prominent ones—without (as this study indicates) wide

success in getting American adults tuned into the meaning and importance of even the meaning of the privacy policy label (Richmond, 2010; Zetter, 2012). A more successful tack might be for journalists and other media practitioners to make privacy policy evaluation part of their routine writing about new sites and apps. Praising and shaming firms might get the attention of audiences and sensitize them to what firms are doing with the information.

Although school-based and media-based privacy-education efforts are certainly important, there is a more direct step to addressing people's misunderstanding the correct meaning of the privacy policy label: Web sites and apps should change the label so that people don't have misplaced confidence in it. The FTC back in 1998 used the phrase "information practice statement" as a suggested title for the document. It didn't take hold, possibly because companies realized that "privacy policy" embodied the ambiguity they wanted. Thirteen years of research show consistently, though, that the label is deceptive. A strong majority of Americans thinks it means that firms will not use their information without their permission. One solution would be for the Federal Trade Commission, which is mandated to police deceptive corporate practices, to rule that only sites and apps that don't share people's information without their permission can use that phrase. Otherwise, they should use a label such as "what we do with your information," which is probably clearer than "information practice statement." Educators and advocates are likely to support this change. Companies are likely to object to it because they don't want the label to serve as a shorthand that alerts people to activities may not like. Yet it is a struggle worth pursuing in the interest of creating transparency around the name of a document that our research shows has been mistitled and misunderstood for over a decade.

References

Barocas, S., & Nissenbaum, H. (2009). On notice: The trouble with notice and consent. Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information. Retrieved from https://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf

Berriman, L., & Thomson, R. (2015). Spectacles of intimacy? Mapping the moral landscape of teenage social media. *Journal of Youth Studies*, *18*(5), 583–597. doi:10.1080/13676261.2014.992323

Boyd, D. (2014). *It's complicated: The social lives of networked teens*. New Haven, CT: Yale University Press.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. doi:10.1177/1948550612455931

Common Sense Media. (n.d.). *Privacy evaluation questions*. Retrieved from https://www.commonsense.org/education/privacy/questions/categories#data-sharing-how-do-third-parties-collect-access-and-use-data

Culnan, M. J., & Milne, G. R. (2001). *The Culnan–Milne survey of consumers and online privacy notices*. Retrieved from http://intra.som.umass.edu/georgemilne/PDF_Files/culnan-milne.pdf

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. doi:10.1016/j.chb.2008.08.006

Freese, J., Rivas, S., & Hargittai, E. (2006). Cognitive ability and Internet use among older adults. *Poetics*, *34*, 236–249.

FTC. (1998, June 4). *Federal trade commission*. Retrieved from https://www.ftc.gov/news-events/press-releases/1998/06/ftc-releases-report-consumers-online-privacy

FTC. (2014, March). *Federal trade commission*. Retrieved from https://www.ftc.gov/site-information/privacy-policy

Hargittai, E. (2005). Survey measures of Web-oriented digital literacy. *Social Science Computer Review*, *23*, 371–379.

Hargittai, E., & Hinnant, A. (2008). Digital inequality. *Communication Research*, *35*(5), 602–621.

Herold, B. (2014, April 16). Prominent ed-tech players' data-privacy policies attract scrutiny. *Education Week*. Retrieved from http://www.edweek.org/ew/articles/2014/04/16/28privacy_ep.h33.html

Hobbs, R. (2010). *Digital and media literacy: A plan of action* (White Paper). The Aspen Institute.

Kumaraguru, P., & Cranor, L. F. (2005). *Privacy indexes: A survey of Westin's studies* (No. Paper 856). Institute for Software Research. Retrieved from http://repository.cmu.edu/isr/856

Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior*, *29*, 1649–1656.

Livingstone, S. (2004). Media literacy and the challenge of new information and communication technologies. *The Communication Review*, *7*(1), 3–14. doi:10.1080/10714420490280152

Livingstone, S., Byrne, J., & Bulger, M. (2015). *Researching children's rights globally in the digital age* (Report of a Seminar Held February 12–14, 2015). London School of Economics and Political Science. Retrieved from http://eprints.lse.ac.uk/62248/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Livingstone,%20S_Researching%20children's%20rights_2015.pdf

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, *4*(3).

Metcalfe, J., & Shimamura, A. P. (1996). *Metacognition: Knowing about knowing* (1st MIT Press paperback ed.). Cambridge, MA: MIT Press.

Milne, G. R., & Culnan, M. J. (2002). Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 U.S. Web Surveys. *The Information Society*, *18*(5), 345–359. doi:10.1080/01972240290108168

Mossberger, K., Tolbert, C. J., & Stansbury, M. (2003). *Virtual inequality: Beyond the digital divide*. Washington, DC: Georgetown University Press.

Obar, J. A., & Oeldorf-Hirsch, A. (2016, July 7). *The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236. doi:10.1177/0093650211418338

Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., … Ramanath, R. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal*, *30*(1), 39–88.

Richmond, R. (2010, September 17). A loophole big enough for a cookie to fit through. *New York Times*. Retrieved from http://bits.blogs.nytimes.com/2010/09/17/a-loophole-big-enough-for-a-cookie-to-fit-through/?_r=0

Shade, L. R., & Shepherd, T. (2013). Viewing youth and mobile privacy through a digital policy literacy framework. *First Monday*, *18*(12). doi:10.5210/fm.v18i12.4807

Smith, A. (2014). *What Internet users know about technology and the Web*. Pew Research Center. Retrieved from http://www.pewinternet.org/files/2014/11/PI_Web-IQ_112514_PDF.pdf

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*(7), 1880–1903.

Turow, J. (2003). *Americans and online privacy: The system is broken* (Online). Philadelphia, PA: Annenberg Public Policy Center. Retrieved from http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/20030701_America_and_Online_Privacy/20030701_online_privacy_report.pdf

Turow, J., Delli Carpini, M. X., Draper, N., & Howard-Williams, R. (2012). *Americans roundly reject tailored political advertising*. Philadelphia, PA: Annenberg School of Communication.

Turow, J., Feldman, L., & Meltzer, K. (2005). *Open to exploitation: American shoppers online and offline*. Philadelphia, PA: University of Pennsylvania: Annenberg Public Policy Center.

Turow, J., Hennessy, M., & Draper, N. (2015). *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*. Philadelphia, PA: Annenberg School of Communication. Retrieved from https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and

Turow, J., King, J., Hoofnagle, C. J., & Hennessy, M. (2009). *Contrary to what marketers say Americans reject tailored advertising and three activities that enable it* (Online). Retrieved from SSRN.

Van Dijk, J. (2005). *The deepening divide: Inequality in the information society*. Thousand Oaks, CA: Sage Pub.

Zetter, K. (2012, February 13). Privacy tool lets users quickly rank Web sites on privacy policies. *Wired*. Retrieved from https://www.wired.com/2012/02/privacy-choice/