

Independently Conducted by



Presents

**2008 Privacy Trust Study of the
United States Government®**

Published by Ponemon Institute LLC

March 31, 2008

Private & Confidential Document: Please Do Not Quote Without Express Permission.

2008 Privacy Trust Study of the United States Government[®]

By Dr. Larry Ponemon, March 31, 2008

Synopsis

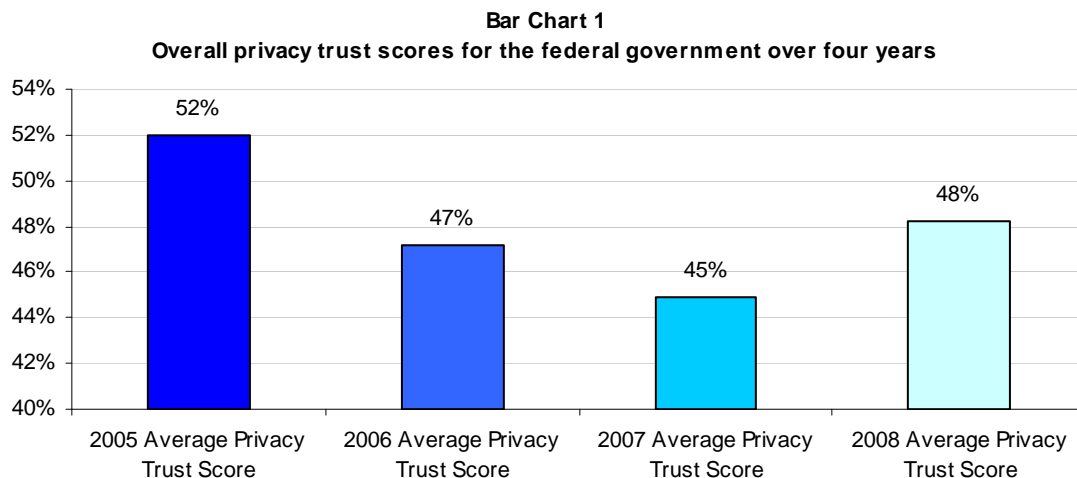
Do Americans believe the federal government takes appropriate steps to safeguard their personal information? Do we believe our government is committed to protecting the privacy rights of its citizens?

To answer these and other normatively important questions, we surveyed more than 9,000 adult-aged citizens who rated 74 different federal government organizations according to their perceptions about how well they protect their privacy.

The objective of this research is to study citizens' trust in federal government organizations that routinely use the public's personal information for various reasons. These include delivering mail, paying taxes, receiving Social Security benefits, performing the census, or registering individuals on the Do Not Call list. The four guiding research questions for this study are:

- Do we believe that the privacy commitments of federal governmental departments, agencies and commissions vary in discernable ways?
- Do our beliefs about the current presidential administration influence what we think about the privacy commitments made by federal organizations?
- What factors do we consider most important when judging the privacy of a particular governmental organization?
- Have perceptions changed since our inaugural study was conducted more than four years ago?¹

Since Ponemon Institute conducted the first privacy trust study of the U.S. government in 2004, the results suggest that a large proportion of Americans do not trust of the federal government's privacy commitments. As shown in Bar Chart 1, overall trust scores declined from a high of 52% in 2005 to a low of 45% in 2007. The 2008 study reports an increase to 48% as shown below.

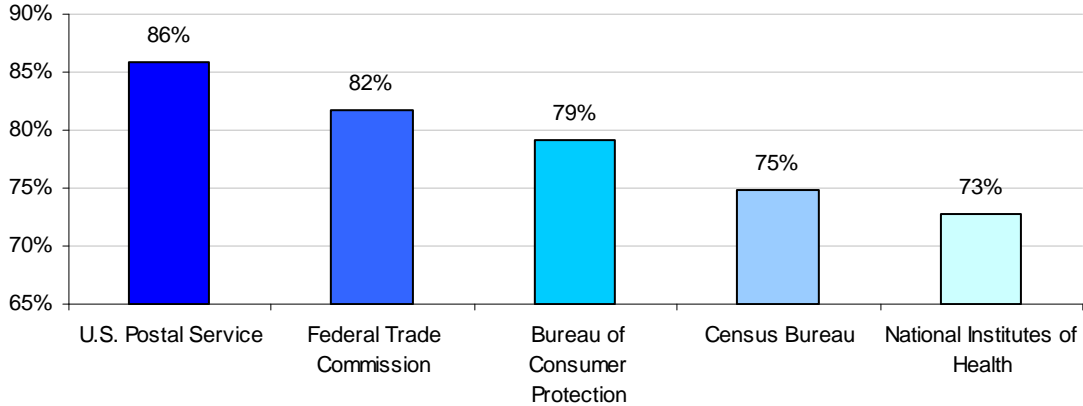


In general, our list of top and bottom performing government organizations remains consistent with prior years. The U.S. Postal Service rose once again from 83% to 86%, and has maintained the top position as the most trusted organization for privacy over all four years of study. The

¹The first Privacy Trust Survey of the United States Government was completed in 2004 and officially released in January 2005 as a joint publication of Ponemon Institute and Carnegie Mellon University.

Federal Trade Commission also experienced a 1% increase from 80% to 81%, earning them the second place for the most trusted governmental organization for privacy.

Bar Chart 2
2008 Privacy trust scores for the top five US government organizations



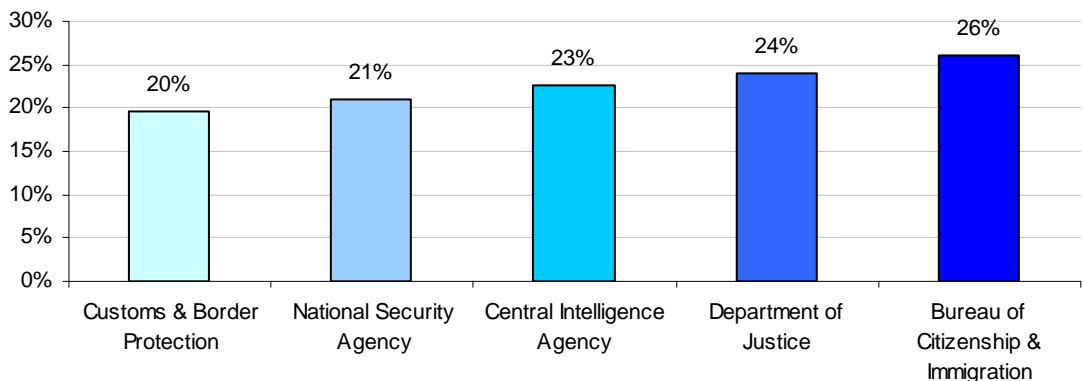
As shown above in Bar Chart 2, other top performers in this year's study include the Bureau of Consumer Protection, the U.S. Census Bureau, and the National Institutes of Health. Table 1 reports the top performing organizations for privacy trust over the past four years.

Table 1: Four year view of top performing US government organizations	Four Year Forced Rank	Four Year Average	2005 Privacy Trust Score	2006 Privacy Trust Score	2007 Privacy Trust Score	2008 Privacy Trust Score	2008 to 2007 Net Change
U.S. Postal Service	1	82%	78%	82%	83%	86%	3%
Federal Trade Commission	2	78%	70%	78%	80%	82%	1%
Bureau of Consumer Protection*	3	74%	68%	72%	79%	79%	0%
Internal Revenue Service	4	72%	75%	74%	67%	70%	2%
National Institutes of Health	5	70%	68%	69%	71%	73%	2%
Census Bureau	5	70%	66%	72%	68%	75%	7%

*The Bureau of Consumer Protection is located within the Federal Trade Commission.

Bar Chart 3 reports the government organizations least trusted for privacy. Customs & Border Protection (CBP) received the lowest privacy trust score among all rated federal organizations.

Bar Chart 3
2008 Privacy trust scores for the bottom five US government organizations



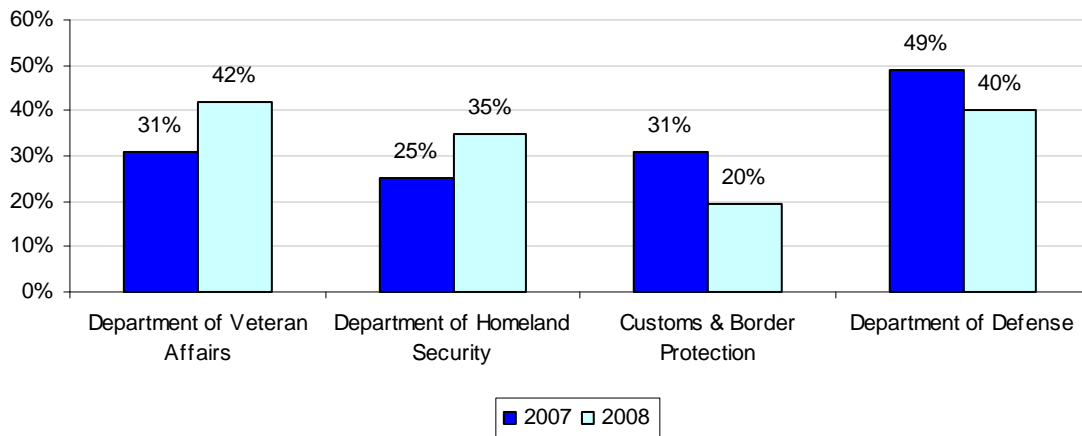
Other poor performers for privacy trust include the National Security Agency, the Central Intelligence Agency, the Department of Justice, and the Bureau of Citizenship & Immigration. Table 2 reports the bottom performing organizations over the past four years.

Table 2: Four year view of bottom performing US government organizations	Four Year Forced Rank	Four Year Average	2004 Privacy Trust Score	2006 Privacy Trust Score	2007 Privacy Trust Score	2008 Privacy Trust Score	2008 to 2007 Net Change
Department of Homeland Security	74	22%	27%	17%	22%	30%	8%
Central Intelligence Agency	73	23%	27%	21%	21%	23%	2%
Office of Attorney General	72	24%	22%	26%	23%	29%	6%
Transportation Security Administration*	71	25%	30%	19%	25%	35%	10%
National Security Agency	70	25%	29%	28%	19%	21%	2%
Department of Justice	69	26%	24%	25%	29%	24%	-5%
Federal Bureau of Prisons	68	33%	38%	31%	31%	28%	-3%
Bureau of Citizenship & Immigration	67	33%	39%	29%	32%	26%	-6%
Customs & Border Protection*	66	35%	38%	35%	31%	20%	-11%

*TSA and CBP are part of the Department of Homeland Security.

Bar Chart 4 reports the government organization that exhibited the largest net change between the 2007 and 2008 studies. The Veterans Administration (VA) experienced an 11% point increase from 31% to 42% over the past year. As noted in last year's report, the VA experienced the largest PTS decline due to a data breach involving the loss of sensitive data about veterans. The Department of Homeland Security (DHS) experienced a 10% point increase from 25% to 35%.

Bar Chart 4
Net change between 2007 and 2008
 Two most positive and negative governmental organizations



In contrast, Custom & Border Protection and the Department of Defense experienced the most significant decrease in privacy trust scores between 2007 and 2008.

Survey

The survey asked individuals to record their beliefs about 74 U.S. government organizations that are known to collect and use personal information about the public. The set of government organizations presented in the survey was a subset of entities identified in field tests with the assistance of expert panels.

Many of the organizations listed in our survey are a subsidiary operation within a larger agency, bureau or department. For example, the Transportation Security Administration and Department of Homeland Security (DHS) are listed as separate entities, even though the TSA reports through DHS. Separate ratings were required because our preliminary test revealed that respondents viewed TSA and DHS as separate governmental entities for purposes of judging their privacy commitments.

Table 3 reports the 74 government organizations listed in our final survey instrument based on field research, and input from an expert panel.

Table 3: List of Governmental Organizations on Survey

1	Administration for Children & Families	38	Federal Bureau of Prisons
2	Administration on Aging	39	Federal Citizen Information Center
3	AMTRAK	40	Federal Communications Commission (FCC)
4	Branches of the Military	41	Federal Court System
5	Bureau of Alcohol, Tobacco and Firearms (ATF)	42	Federal Elections Commission
6	Bureau of Citizenship & Immigration	43	Federal Emergency Management Agency
7	Bureau of Consumer Protection	44	Federal Maritime Commission
8	Bureau of Engraving & Printing (Mint)	45	Federal Trade Commission (FTC)
9	Bureau of Labor Statistics	46	First Gov
10	Bureau of Land Management	47	Fish & Wildlife Service
11	Census Bureau	48	Food & Drug Administration (FDA)
12	Center for Disease Control & Prevention	49	Forest Service
13	Central Intelligence Agency (CIA)	50	General Services Administration (GSA)
14	Coast Guard	51	Government Accountability Organization (GAO)
15	Consumer Product Safety Board	52	Housing & Urban Development (HUD)
16	Criminal records database (NCIC)	53	Immigration and Customs Enforcement
17	Customs & Border Protection	54	Internal Revenue Service
18	Defense Intelligence Agency	55	Library of Congress
19	Department of Agriculture	56	National Aeronautic & Space Admin (NASA)
20	Department of Commerce	57	National Archives and Records Admin
21	Department of Defense	58	National Institute of Corrections
22	Department of Education	59	National Institute of Science & Technology
23	Department of Energy	60	National Institutes of Health
24	Department of Health & Human Services	61	National Security Agency (NSA)
25	Department of Homeland Security	62	Occupational Safety and Health Admin (OSHA)
26	Department of Justice	63	Office of Management & Budget
27	Department of Labor	64	Office of Personnel Management
28	Department of State	65	Office of Refugee Resettlement
29	Department of the Interior	66	Office of Student Financial Assistance Program
30	Department of the Treasury	67	Office of the Attorney General
31	Department of Transportation	68	Passport Services & Information
32	Department of Veteran Affairs (VA)	69	Postal Service
33	Drug Enforcement Agency (DEA)	70	Secret Service
34	Environmental Protection Agency (EPA)	71	Selective Services
35	Equal Employment Opportunities Commission	72	Small Business Administration
36	Federal Aviation Administration (FAA)	73	Social Security Administration
37	Federal Bureau of Investigation (FBI)	74	Transportation Security Administration

The instrument provided three possible responses for each federal entity presented, which are:

- **Yes** – I am confident that the U.S. government organization is committed to protecting the privacy of my personal information.
- **No** – I am not confident that the U.S. government organization is committed to protecting the privacy of my personal information.
- **Unsure** – I am not sure if the U.S. government organization is committed to protecting the privacy of my personal information.

The primary variable of interest is the Privacy Trust Score (PTS) for each one of the organizations or institutions listed on the survey instrument. The PTS is a calculated construct defined in percentage terms as Total Yes response divided by total number of yes and no responses (or sample size minus unsure or blanks). By design, the theoretical maximum PTS score is 100% and the theoretical minimum PTS score is zero.

Because several federal organizations are not known or recognized by the public, we also permitted individuals to leave entries blank. Blank responses were omitted from the privacy trust tabulations for a given organization. Also, organizations that had more than a 25% blank response rate were eliminated from the total ranking process.

Nine government organizations were omitted in the analysis because of a high number of blank responses. The remaining 65 organizations were ranked in ascending order according to their PTS score. Eleven organizations achieved a tied score.

In addition to the primary research question, the survey included descriptive items designed to capture opinions about how government can do a better job in advancing privacy and data protection efforts.

The remainder of this paper summarizes our research method and limitations. Despite limitations of our survey instrument and sampling method, we believe that our study sheds light on the public's trust in different U.S. government entities that are responsible for safeguarding our private information.

Caveats on the PTS Findings

There are inherent limitations to survey research that need to be carefully considered before making conclusions from sample findings. The following items are specific limitations that are germane to most perception-capture studies.

Non-Response Bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. While tests of late responses were performed to assess non-response bias, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-Frame Bias: Because our sampling frame is a pre-selected email list, the quality of results is influenced by the accuracy of contact information and the degree to which the list is representative of individuals who are informed about privacy. We also acknowledge that the results may be biased by media coverage of public events at the time of the study.

While compensation was held to a nominal amount, we acknowledge potential bias caused by compensating subjects to complete this research within a pre-defined holdout period. In addition, because we used a Web-based collection method, it is possible that allowing respondents to furnish non-Web responses (form survey or telephone) would have resulted in significantly different results.

Extrapolated Behavioral Data: The current instrument allowed individuals to use a fixed response variable to disclose current beliefs or perceptions. Our analyses relied on self-assessed results. While there was no indication that this procedure created bias or error, the extrapolation behavioral data from a fixed response variable needs to be considered as a potential limitation when interpreting results.

Unmeasured Demographics: To keep the survey concise and focused, we decided to omit other normatively important demographic variables from our analyses. The extent to which omitted variables might explain survey findings cannot be estimated at this time.

Self-Reported Results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that subjects did not provide truthful responses.

Survey Methods

The survey was developed with the goal of collecting opinion-based information from a representative cross-section of individuals who reside in the United States. We limited the number of survey items so that it took a short timeframe to complete. Traditionally, a concise survey results in a higher response rate and better quality of responses. We used Web and paper-based surveys to make completion of the survey as convenient as possible.

To keep the survey form short, only those items crucial to our research objectives were included. Hence, key items focused on individual perceptions about governmental organizations or institutions that collect and use personal information. Other descriptive items were selected to explore key relationships between privacy trust perceptions (PTS) and key demographic variables.

The original survey instrument was developed with the guidance of experts who were asked to list the most relevant federal government entities to include in our instrument. The main criterion for inclusion was the expert's belief that the listed organization collects and uses sensitive or non-public personal information about individuals or households. In total, the aggregated list contained 128 unique federal organizations or institutions of which 64 were not overlapping entities.

Two opinion criteria were used to prioritize organizations for the survey, including: (1) level of privacy concern about the organization's use of personal information and (2) belief that the organization collects and uses personal information about them or their families. From these criteria, organizations were ranked from highest to lowest in priority, and the top 74 entities were selected for inclusion in the instrument.

A final instrument with 74 government entities was finalized in January 2008. As in prior years, the 2008 survey utilized a framing technique to ensure that individual responses were aligned according to the same definitions for personal information and privacy commitment. The actual framing used within the survey instrument is described as follows:

- Personal information – information about yourself and your family. This information includes name, address, telephone numbers, email address, Social Security number, other personal identification numbers, access codes, age, gender, income and tax information, travel information, account activity and many other pieces of data about you.
- Privacy commitment – an obligation by the specified government organization to keep your personal information safe and secure. This includes the commitment not to share your personal information without a just cause or without obtaining your consent to do so.

The survey contained several items including one dependent variable that asked subjects to rate organizations by title, using a fixed-format design. No personally identifiable information was collected about the participants.

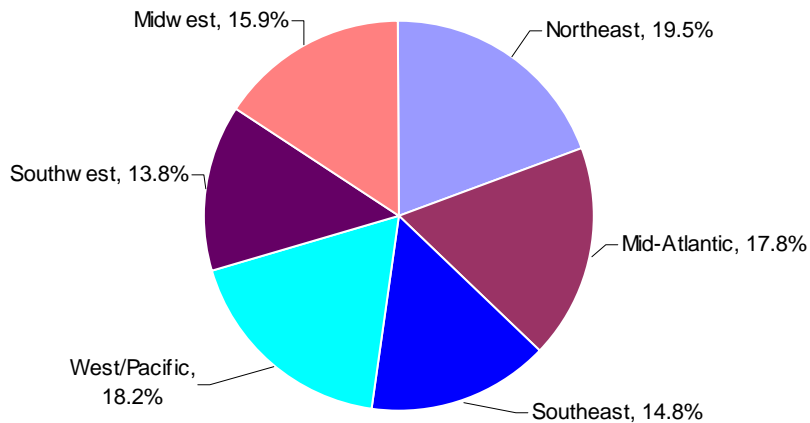
Once completed, the survey was administered to a national list of targeted participants based on a random sampling plan. A few days before the actual email invitations were sent, we sent an announcement to all targeted participants requesting their participation in an important study for nominal compensation. The letter or email announcement requested subjects to complete the instrument within three weeks after receipt.

Upon completion of the survey, each returned instrument was measured against specific tests for validity and reliability. In total, 510 returned surveys were rejected because of incomplete or inconsistent responses. Table 3 provides the sample response over a four-week holdout period. The final net response rate was 9.27%.

Table 3: Sample Statistics	Sample plan	Pct% Response
Total Number in Sample Frame	97,802	100.00%
Total Number of Responses	9,683	9.90%
Unusable or Rejected Surveys	613	0.63%
Final Sample Size	9,070	9.27%

To assess non-response bias, we employed a late response testing method using the mail clearing date stamp or email internal run time. The results of this test show no differences in the pattern of survey information provided by subjects over time. Pie Chart 1 shows the distribution of our final sample across six major regions across the nation. The Midwest region had the largest number of responses and the Southwest had the smallest number of responses. All major regions of the United States are represented in this study, with respondents residing in 48 states.

Pie Chart 1: Geographic distribution



Following our procedures from prior annual studies, governmental organizations were removed from the rating evaluation process if these organizations had a high blank response (indicating that subjects did not recognize the named organization). Governmental organizations with a total blank percentage rate above 25% were removed from the ranking procedure.

Table 5 lists 10 factors considered important for defining a governmental organization's privacy commitment to the American public. The importance of each factor was determined based on the percentage frequency of responses. Respondents were asked to check as many of these factors

that they believe were relevant to their perceptions about privacy. Results for three years are summarized below.

Table 5 Factors most important to creating trust in the government's privacy commitments	Pct% 2006	Pct% 2007	Pct% 2008
Sense of confidentiality and data security protections when providing personal information	58%	57%	61%
Personal relationships or one-to-one contact with someone inside the organization	51%	53%	49%
Limits over the collection of personal information	53%	51%	51%
Media or press coverage of issues or problems	30%	39%	32%
Secure Web site	35%	39%	40%
Overall positive experiences in dealing with the organization	38%	38%	37%
Education and outreach	17%	20%	22%
Fast response to questions	10%	14%	11%
Privacy policies	12%	12%	7%
Access to my personal information	11%	11%	14%

*Table does not sum to 100% because more than one item could be selected.

The most important factor over three years is the, "sense of confidentiality and data security protections when providing personal information." The second most important factor in 2007 and 2008 is, "having personal relationships or one-to-one contact with someone inside the organization." For instance, in the case of the USPS, the "someone" may be the local mail carrier.

The third most important factor in 2008 is, "limits over the collection of personal information." Factors that are considered less important include, "fast response to questions," "the right of access to personal information," and "privacy policies."

What worries respondents most about the government's use of the public's personal information? Table 6 provides percentage results in descending order by the frequency of responses. Here again, respondents were required to check as many of these factors that they believe are relevant to their beliefs about the privacy commitment of the federal government to its citizenry.

Table 6 The most salient privacy concerns of respondents	Pct% 2005	Pct% 2006	Pct% 2007	Pct% 2008
Loss of civil liberties and privacy rights	64%	69%	67%	57%
Surveillance into personal life	63%	63%	63%	56%
Monitoring of email and Web activities	47%	51%	48%	47%
Theft of your identity	19%	23%	29%	40%
Sharing with business and other commercial organizations	34%	34%	33%	30%
Sharing with state and local government including police	31%	31%	29%	29%
Theft or seizure of your personal assets	16%	15%	19%	15%

*Table does not sum to 100% because more than one item could be selected.

Despite a decrease of 10% from 67% in 2007, the above table shows 57% of Americans believe the "loss of civil liberties and privacy rights" as their number one privacy concern. The second most frequently selected issue is "surveillance into personal life" for 56% respondents, which is a 7% decrease in percentage terms from past years. The third most significant issue is the

“monitoring of email and Web activities” for 47% of respondents. It is also interesting to note that concerns about identity theft have significantly increased by 11% from 29% in 2007 to over 40% in 2008.

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote from or reuse this report), please contact by letter, phone call or email:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49689
1.800.887.3118
research@ponemon.org

Ponemon Institute LLC

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.