2010 Privacy Trust Study of the United States Government

Independently conducted by Ponemon Institute LLC

Publication Date: June 30, 2010

2010 Privacy Trust Study of the United States Government

Ponemon Institute, June 30, 2010

1. Executive Summary

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?

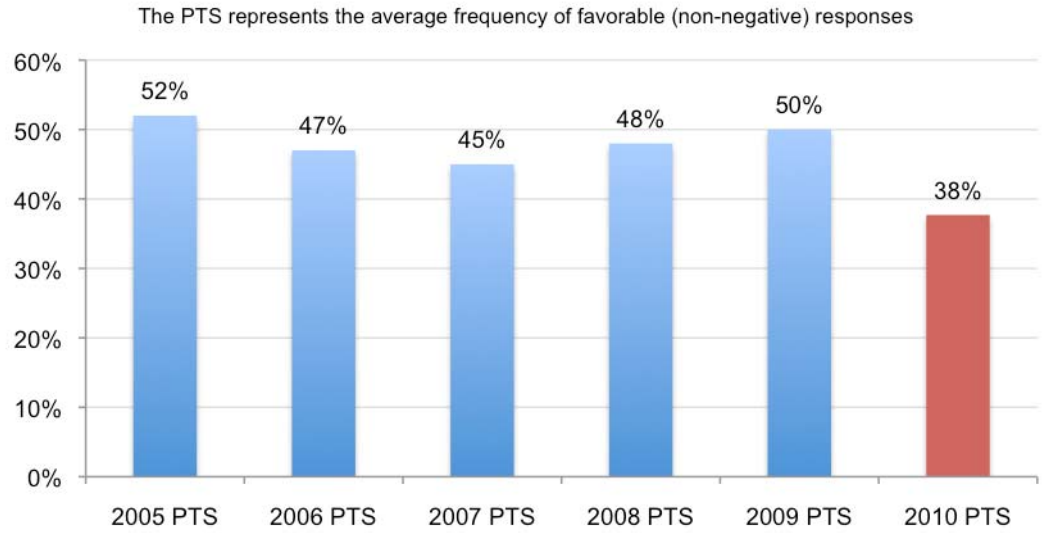
To answer these and other normatively important questions, we surveyed more than 9,000 adult-aged citizens who rated 75 different federal government organizations according to their opinions or beliefs about how well these entities protect privacy.

The objective of this research is to study Americans' trust in federal government organizations that acquire and use the public's personal information for a wide array of legitimate and important purposes. These include delivering mail, processing tax returns, providing veterans' benefits, conducting the census, and many other activities. Three guiding questions for this study are:

- Do we believe the privacy commitments of federal governmental departments, agencies and commissions vary in discernable ways?
- 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 six years ago?[1]

Since we conducted the first privacy trust study of the U.S. government in 2004, results suggest that a majority of respondents **do not trust** the privacy commitments of the federal government. While not a steady downward trend over six years, Bar Chart 1 does reveal that privacy trust in the U.S. government declined from a high of 52 percent in 2005 to a low of 38 percent in the present study.

Bar Chart 1: Average privacy trust scores for U.S. government entities rated



[1]The 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.

Our list of top performing government organizations remains relatively consistent from 2009 with one notable exception – that is, the U.S. Census Bureau dropped from an average PTS of 78 percent last year to 39 percent in 2010.[2] The U.S. Postal Service once again earns top honors with a PTS of 87 percent. Albeit small declines from 2009, the Federal Trade Commission and the Internal Revenue Service earn second and third place, respectively. [3]

Bar Chart 2: 2009 and 2010 PTS scores for top rated U.S. government entities

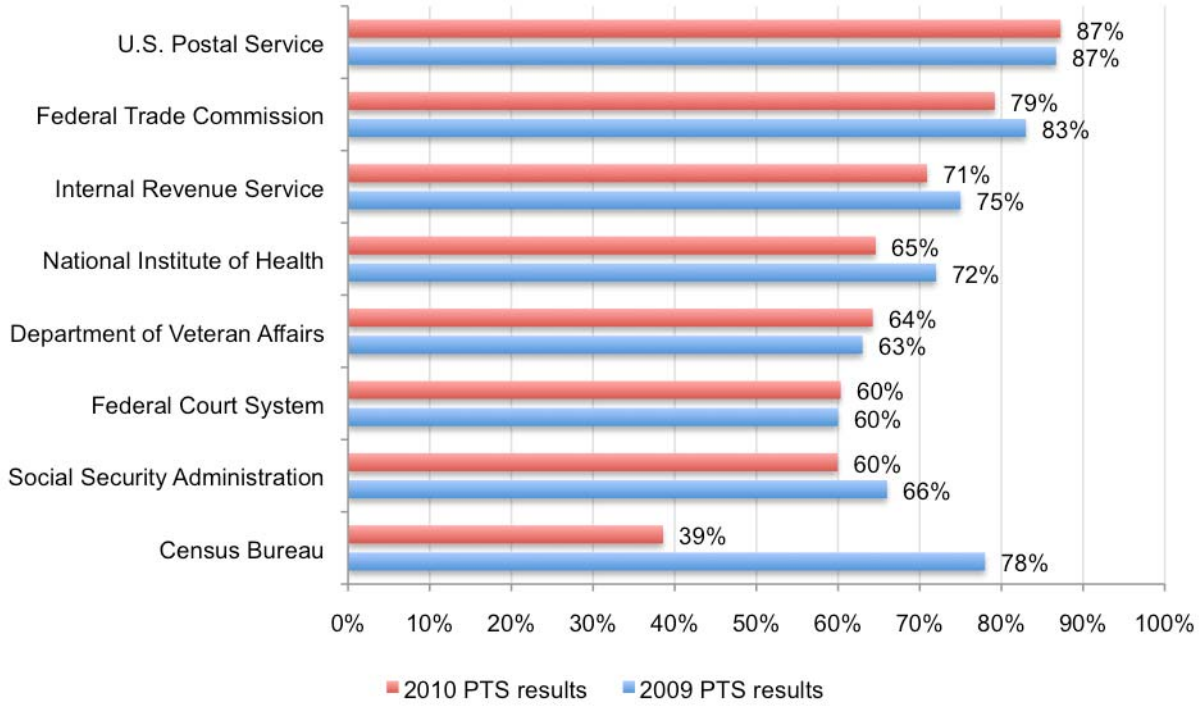


Table 1 reports the top performing U.S. government organizations with respect to privacy trust scores over six consecutive years. Despite the drop in PTS scores for the Census Bureau, it still remains among the top five.

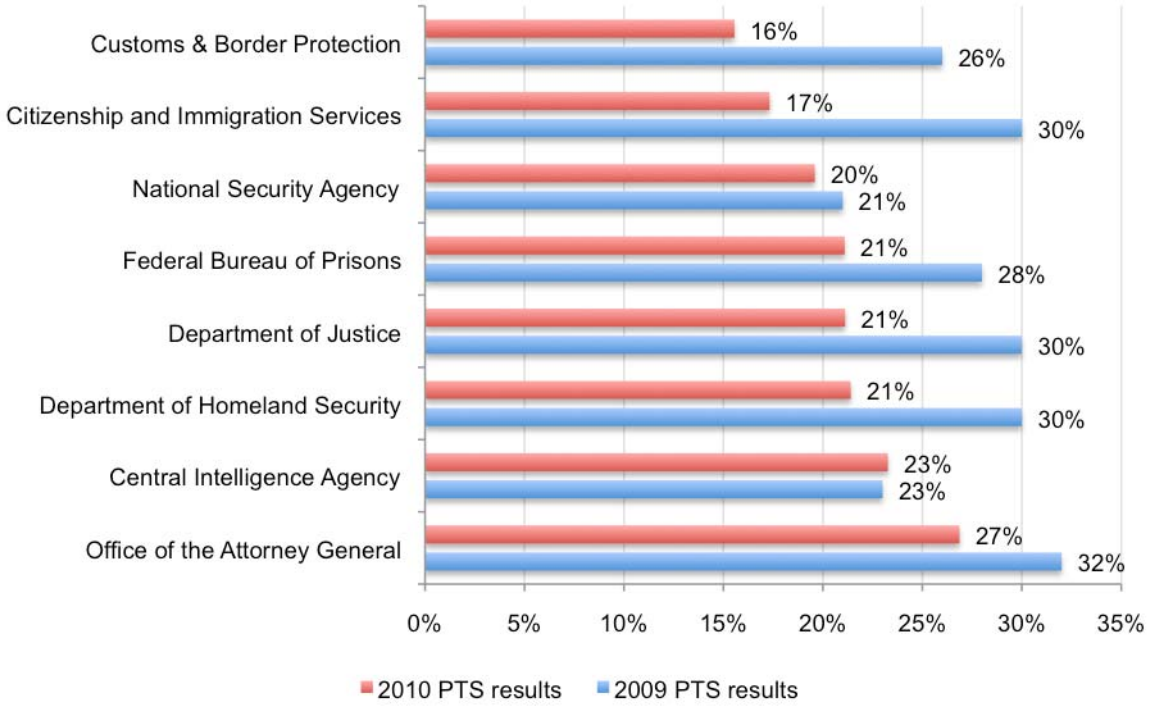
Table 1 Top five entities over six years	U.S. Postal Service	Federal Trade Commission	Internal Revenue Service	National Institutes of Health	Census Bureau
Six year rank	1	2	3	4	5
Six year average	84%	79%	72%	70%	66%
2005 PTS	78%	70%	75%	68%	66%
2006 PTS	82%	78%	74%	69%	72%
2007 PTS	83%	80%	67%	71%	68%
2008 PTS	86%	82%	70%	73%	75%
2009 PTS	87%	83%	72%	72%	75%
2010 PTS	87%	79%	71%	65%	39%

[2]It is important to note that privacy trust ratings may be influenced by current events. During the fielding of this year's research, the Census Bureau was conducting the U.S. national census. We acknowledge that this activity influenced respondents' ratings. Similarly, in prior years, the Veteran Affairs suffered a significant decline in PTS after it disclosed a data breach involving the loss or theft of veterans' personal information. In the case of the VA, privacy trust ratings recovered about one year after the incident, thus placing it in the top privacy trust category as shown in Bar Chart 2.

[3] The Bureau of Consumer Protection, which was listed separately in the 2009 study, is consolidated within the 2010 FTC results.

Bar Chart 3 reports the U.S. government organizations that have the lowest privacy trust ratings based on responses. Customs & Border Protection (CBP) has the lowest overall privacy trust score among all rated organizations. Citizen and Immigration Services (CIS) and the National Security Agency (NSA) have tne second and third lowest scores, respectively.

Bar Chart 3: 2009 and 2010 PTS scores for bottom rated U.S. government entities



Other poor performers for privacy trust include the Federal Bureau of Prisons, Department of Justice, Department of Homeland Security, Central Intelligence Agency and Office of the Attorney General. With the exception of the CIA, all bottom performing companies experienced a decline in privacy trust scores from 2009 to 2010.

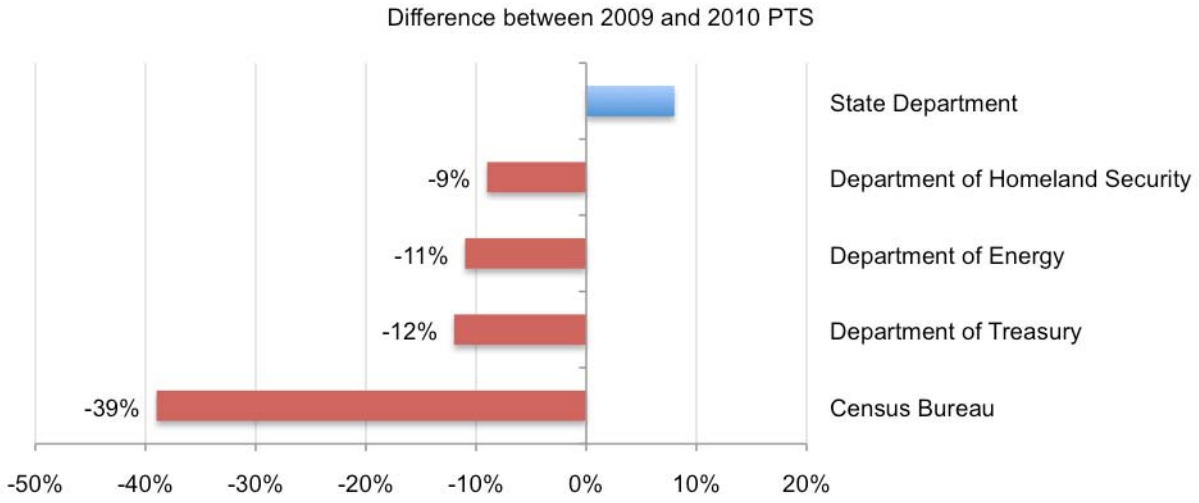
Table 2 reports the bottom performing organizations over the past six years. It shows general consistency in scores over this time period. For purposes of consistency, CBP and CIS are consolidated under its parent, the Department of Homeland Security.

Table 2 Bottom five performing U.S government entities	Central Intelligence Agency	National Security Agency	Department of Homeland Security	Department of Justice	Office of Attorney General
Six year rank	74	74	73	72	71
Six year average	23%	23%	25%	26%	27%
2005 PTS	27%	29%	27%	24%	22%
2006 PTS	21%	28%	17%	25%	26%
2007 PTS	21%	19%	22%	29%	23%
2008 PTS	23%	21%	30%	24%	29%
2009 PTS	23%	21%	30%	30%	32%
2010 PTS	23%	20%	21%	21%	27%

Bar Chart 4 reports the government organizations that exhibited the largest net change between the 2009 and 2010 studies. The Census Bureau experienced a 39-point decrease from 78 to 39 percent over the past year. The Departments of Energy, Treasury and Homeland Security

experienced significant declines in privacy trust ratings of 12, 11 and nine percent, respectively. On a positive note, the State Department experienced an eight percent increase from the prior year's study.

Bar Chart 4: Federal government entities with the largest net change in PTS



II. Privacy Trust Score

Our survey required individuals to record their beliefs about 75 U.S. government organizations that are known to collect and use personal information about the public. The list of government organizations presented in the survey is a subset of entities identified in prior research and was validated by a panel of experts. Table 3 reports the 75 government organizations incorporated in the final survey instrument.

Table 3: U.S. Governmental organizations in the survey

1	Administration for Children & Families	39	Federal Bureau of Prisons
2	Administration on Aging	40	Federal Citizen Information Center
3	AMTRAK	41	Federal Communications Commission (FCC)
4	Branches of the Military	42	Federal Court System
5	Bureau of Alcohol, Tobacco and Firearms (ATF)	43	Federal Elections Commission
6	Bureau of Citizenship & Immigration	44	Federal Emergency Management Agency
7	Bureau of Consumer Protection	45	Federal Maritime Commission
8	Bureau of Engraving & Printing (Mint)	46	Federal Trade Commission (FTC)
9	Bureau of Labor Statistics	47	First Gov
10	Bureau of Land Management	48	Fish & Wildlife Service
11	Census Bureau	49	Food & Drug Administration (FDA)
12	Center for Disease Control & Prevention	50	Forest Service
13	Central Intelligence Agency (CIA)	51	General Services Administration (GSA)
14	Coast Guard	52	Government Accountability Organization (GAO)
15	Consumer Product Safety Board	53	Housing & Urban Development (HUD)
16	Criminal Records Database (NCIC)	54	Immigration and Customs Services
17	Customs & Border Protection	55	Internal Revenue Service
18	Defense Intelligence Agency	56	Library of Congress
19	Department of Agriculture	57	National Aeronautic & Space Admin (NASA)
20	Department of Commerce	58	National Archives and Records Admin
21	Department of Defense	59	National Institute of Corrections
22	Department of Education	60	National Institute of Science & Technology
23	Department of Energy	61	National Institutes of Health
24	Department of Health & Human Services	62	National Security Agency (NSA)
25	Department of Homeland Security	63	Occupational Safety and Health Admin (OSHA)
26	Department of Justice	64	Office of Management & Budget
27	Department of Labor	65	Office of Personnel Management
28	Department of State	66	Office of Refugee Resettlement
29	Department of the Interior	67	Office of Student Financial Assistance Program
30	Department of the Treasury	68	Office of the Attorney General
31	Department of Transportation	69	Passport Services & Information
32	Department of Veteran Affairs (VA)	70	Postal Service (USPS)
33	Director of National Intelligence (DNI)	71	Secret Service
34	Drug Enforcement Agency (DEA)	72	Selective Services
35	Environmental Protection Agency (EPA)	73	Small Business Administration
36	Equal Employment Opportunities Commission	74	Social Security Administration
37	Federal Aviation Administration (FAA)	75	Transportation Security Administration
38	Federal Bureau of Investigation (FBI)		

Many of the above-mentioned organizations in our survey are subsidiaries of a federal agency or department. For example, the Transportation Security Administration (TSA) and the 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 independent entities in terms of privacy commitments to the public.

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

- **Yes** – I am confident the U.S. government organization is committed to protecting the privacy of my personal information (a.k.a. favorable rating).
- **No** – I am not confident the U.S. government organization is committed to protecting the privacy of my personal information (a.k.a. unfavorable rating).
- **Unsure** – I am not sure the U.S. government organization is committed to protecting the privacy of my personal information.

For purposes of analysis, our primary variable is the Privacy Trust Score (PTS) calculated for each one of the federal organizations listed on the survey instrument. The PTS is defined as a percentage net favorable response as:

$$PTS_{[\text{federal organization}]} = \sum (\text{Yes response}) / \sum (\text{Yes + No response})$$

By design, the theoretical maximum PTS score is 100 percent 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 and unsure responses were omitted from the privacy trust tabulations for a given organization. Federal organizations that did not achieve at least 20 Yes or No responses were eliminated from the total ranking process.

Eight government organizations were omitted in the analysis because of high blank or unsure responses. The remaining organizations were ranked in ascending order according to their PTS score. Seven organizations achieved a tied score.

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

III. 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 to avoid demand effects and survey fatigue. Traditionally, a concise survey results in a higher response rate and better quality of responses. We used Web and paper-based collection channels 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 more than 130 named federal organizations or institutions of which 61 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 75 entities were selected for inclusion in the instrument.

A final instrument with 75 government entities was finalized in February 2010. As in prior years, the present survey utilized a framing technique to ensure that individual responses were aligned on 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, Internet activities 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 Americans – citizens and legal residents in all U.S. states and territories – based on a scientific sampling plan. A few days before the survey link and form were sent out, we mailed an announcement to more than 176,000 adult-aged individuals requesting their participation.[4] The letter or email announcement requested subjects to complete the instrument within four weeks after receipt.

Upon completion of the survey, each returned instrument was measured against specific tests for validity and reliability. In total, 868 returned surveys were rejected because of incomplete or inconsistent responses. Table 4 provides the sample response over a four-week period. The final

[4] Email invitations were staggered over a five-day period to avoid black or gray anti-spam lists.

net response rate was 5.3 percent. More than 94 percent of respondents utilized the web-based collection channel rather than complete and return a paper copy.

Table 4: Sample Statistics	Freq.	Pct%
Sampling frame	176,009	100.0%
Bounce back	29,482	16.8%
Total response	10,180	5.8%
Rejected surveys	868	0.5%
Final sample	9,312	5.3%

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 significant 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 other category includes U.S. territories including Puerto Rico.

The Northeast region had the largest number of responses (19 percent) and the Southwest had the fewest number of responses (13 percent). All major regions of the United States are represented in this study, with respondents residing in 47 states.

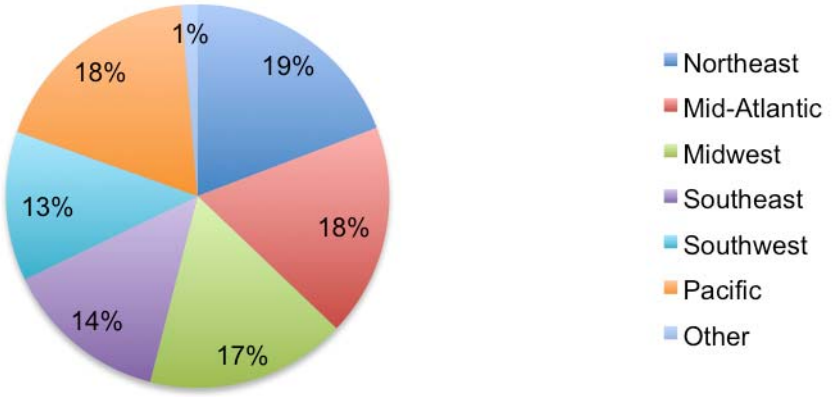


Table 5 lists 10 factors considered important for defining a governmental organization's privacy commitment to the American public. The importance of each factor was determined based on the percentage frequency of responses. Respondents were asked to check as many of these factors that they believe were relevant to their perceptions about privacy. Results for three years are summarized below.

Table 5 Ten factors for raising trust in privacy commitments	Five year average	Five year rank	PTS 2006	PTS 2007	PTS 2008	PTS 2009	PTS 2010
Sense of security protection	59%	1	58%	57%	61%	59%	61%
One-to-one contact	52%	2	51%	53%	49%	55%	52%
Limited collection of personal data	50%	3	53%	51%	51%	51%	46%
Secure website	39%	4	35%	39%	40%	40%	40%
Overall positive experience	37%	5	38%	38%	37%	37%	36%
Media coverage of issues	32%	6	30%	39%	32%	27%	34%
Education and outreach	20%	7	17%	20%	22%	21%	19%
Fast response to questions	13%	8	10%	14%	11%	16%	12%
Access to personal information	11%	9	11%	11%	14%	9%	11%
Privacy policies	8%	10	12%	12%	7%	5%	2%

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

The most important factor over five years is the, "sense of confidentiality and data security protections when providing personal information." The second most important factor 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 over five years 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 over five years. 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	Five year average	Five year rank	PTS 2006	PTS 2007	PTS 2008	PTS 2009	PTS 2010
Surveillance into personal life	60%	1	63%	63%	56%	53%	63%
Loss of civil liberties	59%	2	69%	67%	57%	51%	53%
Monitoring of emails & Web	48%	3	51%	48%	47%	45%	49%
Identity theft	35%	4	23%	29%	40%	41%	42%
Sharing data with commercial organizations	30%	5	34%	33%	30%	28%	26%
Sharing data with state & local government	28%	6	31%	29%	29%	26%	25%
Seizure of personal assets	17%	7	15%	19%	15%	14%	24%

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

The above table shows 63 percent of Americans in the 2010 study are most concerned about government's surveillance in their personal lives (which is a 10 percent increase from the 2009 study). At 53 percent, the "loss of civil liberties and privacy rights" is their number two privacy concern for respondents in 2010. The third most significant issue is the "monitoring of email and web activities" for 49 percent of respondents in 2010. It is also interesting to note that concerns about identity theft have significantly increased by 19 percent from 23 percent in 2006 to over 42 percent in 2010.

IV. Caveats

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 as a primary collection channel, it is possible that allowing respondents to furnish only non-Web responses (mail 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.

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

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.