

Sponsored by



Independently Conducted by



Presents

# **2008 U.S. Study on Email Marketing Practices and Privacy**

**Published by Ponemon Institute LLC**

**June 23, 2008**

## 2008 U.S. Study on Email Marketing Practices & Privacy

Prepared by Dr. Larry Ponemon, June 23, 2008

### I. Introduction

Are U.S. marketers and privacy and data protection practitioners<sup>1</sup> miles apart in their beliefs about how their organizations should and do protect consumers' information in email marketing campaigns? If so, does such a gap in their beliefs indicate that organizations are putting personal information at risk?

The study entitled, *2008 U.S. Study on Email Marketing Practices & Privacy* was conducted by Ponemon Institute and sponsored by StrongMail. The findings reveal gaps in perceptions between marketers and privacy professionals about how email marketing practices affect consumers' privacy rights and risks to personal information. While both groups believe that it is important for consumers and customers to trust the privacy commitments of organizations, marketers worry that complying with privacy regulations could hinder their ability to attract new customers. This ability is core to their role in their organizations and is how their success is measured. The role of the privacy professional is to focus on compliance with regulations and to ensure that steps are taken to secure personal data.

According to the study, more than one-third of marketers do not limit the data they distribute to third parties, whereas 75% of privacy professionals believe that their organizations limit the data it shares. Marketers will share such personal information as credit card number (45%), debit card number (39%), Social Security number (29%), and bank account/routing number (17%).

Further, there is the tendency to outsource marketing campaigns to third parties. Fifty-nine percent of marketers and 53% of privacy professionals indicate that their organizations outsource to reduce costs and improve efficiency. However, our study finds that almost half of the organizations that experienced a data breach pinpointed the loss of data to a third party, such as a vendor, business partner or contractor. Not only are potential breaches an issue, but organizations also need to safeguard consumer data to ensure that it is not used for other unintended purposes, such as unsolicited spam or phishing attempts.

Consider the data breach case involving a third-party email service provider for nonprofit organizations. The third-party provider experienced a data breach when a hacker accessed subscriber email addresses and passwords from 92 of its clients. While the number of individuals affected by the breach is unknown, it could possibly be in the hundreds of thousands. Even though financial data was not breached, the data could be used for other unintended purposes, such as unsolicited spam or phishing attempts. In addition, the nonprofits that outsourced their fund raising campaign experienced a number of negative affects including damaged reputation, a loss of newsletter subscribers and the possibility reduced donations.

We surveyed 498 privacy and data protection professionals and 713 marketers with an average overall experience of nine years. Our survey asked both groups to respond to the same questions about the following issues:

- How confident are they that their organizations' marketing programs and practices are compliant with data protection regulations?

---

<sup>1</sup> For purposes of simplicity, privacy and data protection professionals will be referred to as privacy professionals in this document.

- Have data breaches occurred in their organizations? If so, what was the impact?
- What personal data is being shared when companies outsource their marketing programs?
- Could a company gain a competitive advantage by implementing superior privacy practices? If so, what would the benefit be?
- Can companies better protect their data by keeping marketing programs in-house?

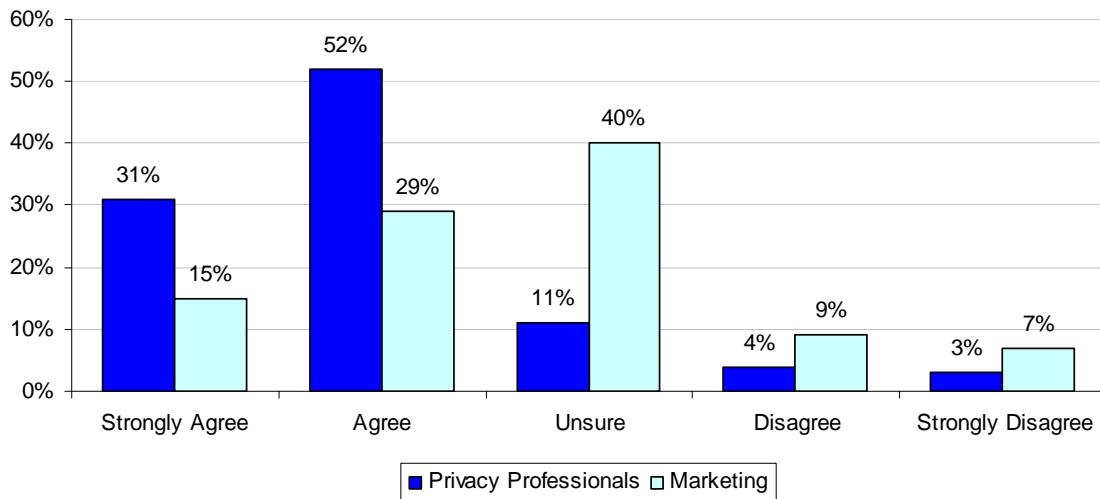
**II. Key findings**

Following are the most salient findings of this survey research. Please note that most of the results—not all—are displayed in bar chart format.

**Marketers are less confident than privacy professionals that their organizations are compliant with privacy laws and regulations such as the CAN-SPAM Act.**

The CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act) establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask emailers to stop spamming them. As shown in Bar Chart 1, only 44% of marketers strongly agree or agree that their organizations are compliant with privacy regulations while 83% of privacy professionals feel the same. A substantial percentage of marketers (40%) are uncertain if their companies are in compliance with these regulations.

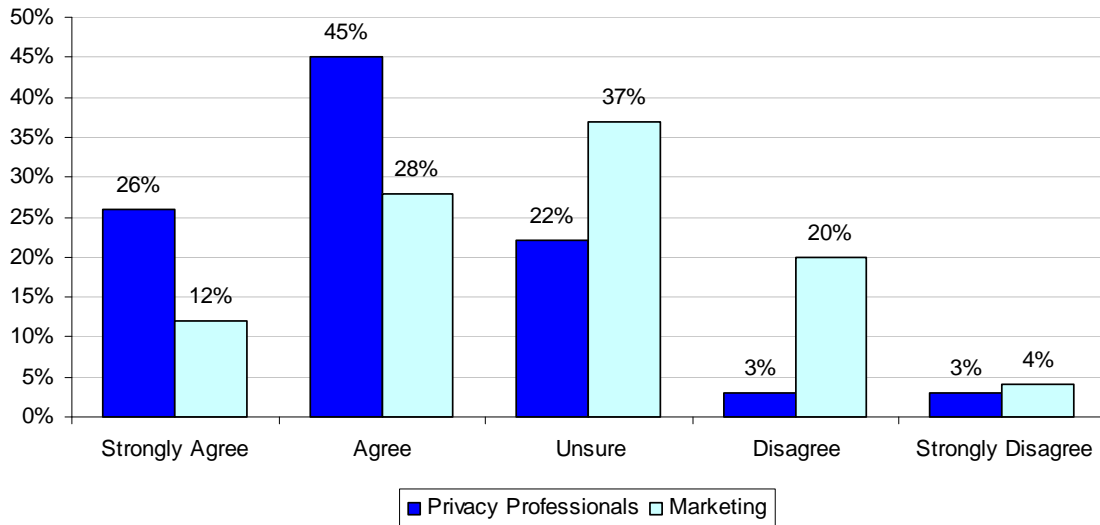
Bar Chart 1  
Our organization is compliant with privacy laws and regulations such as the CAN-SPAM Act.



**Marketers are less likely to believe their organizations are protective and respectful of consumers' privacy and personal information.**

Seventy-one percent of privacy professionals believe their organizations are respectful of consumers' privacy rights while only 40% of marketers agree. As seen in Bar Chart 2, there is notable uncertainty among marketers in our study.

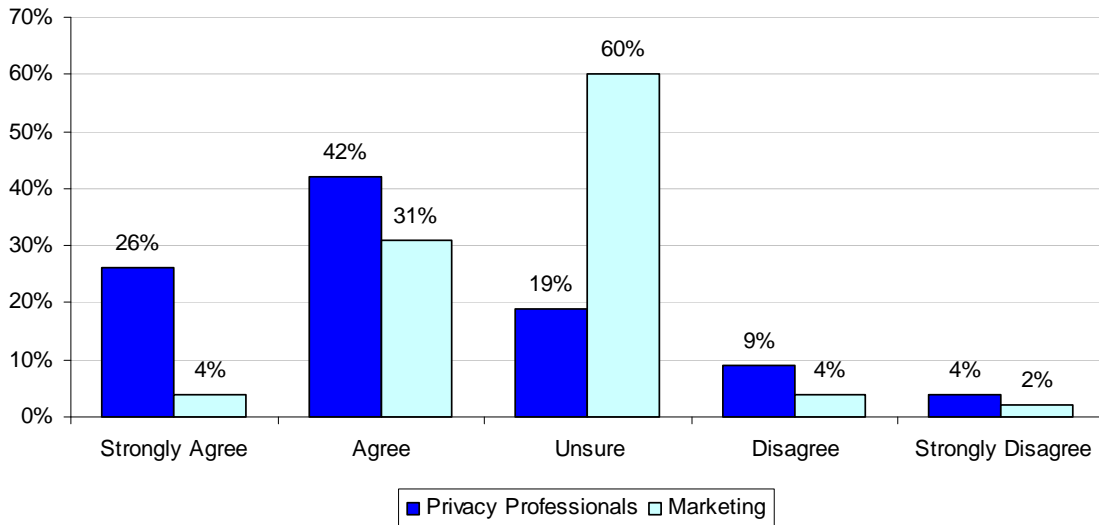
Bar Chart 2  
Our organization respects consumers' privacy rights.



**Marketers who should be most aware about their email marketing campaigns are dubious whether their organizations' marketing practices violate an individual's privacy rights or put personal data at risk.**

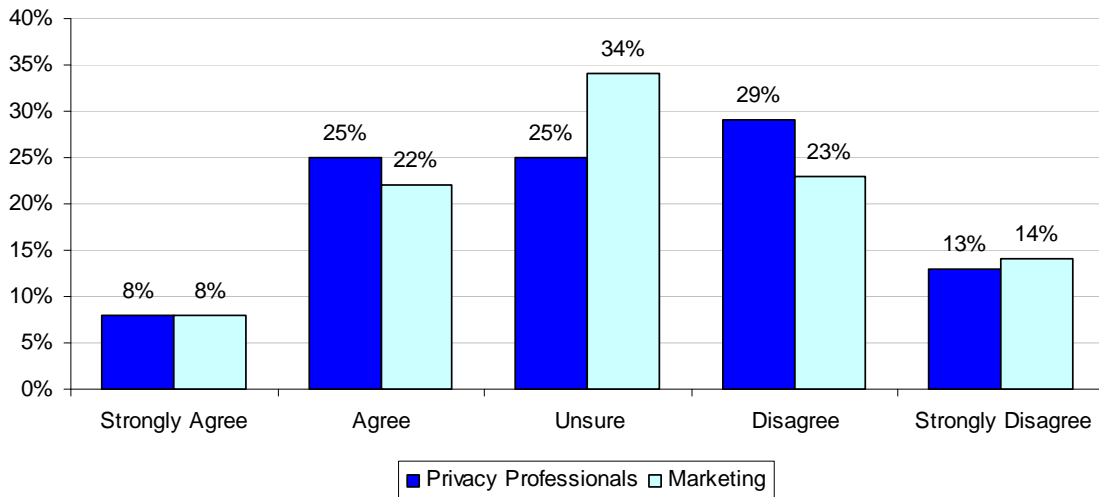
According to the results of our study, 40% of privacy professionals are optimistic that their organizations' marketing practices, including email marketing campaigns, protect personal information. However, only 25% of marketers are confident that this is the case. There is also considerable discrepancy between how privacy professionals and marketers view the likelihood that their marketing programs violate individual privacy rights. Bar Chart 3 shows that the majority of privacy professionals (68%) strongly agree or agree that their marketing programs do not violate individual privacy rights while the majority of marketers (60%), again, are uncertain.

Bar Chart 3  
Our organization's consumer marketing programs do not violate individual's privacy rights.



There is more agreement between marketers and privacy professionals concerning whether marketing programs create risks of personal data loss or theft (Bar Chart 4). However, the results are not positive. Both groups are not confident that their marketing programs are protecting consumer data: 67% of privacy professionals and 71% of marketers disagree or are uncertain about the assertion that their organization's consumer marketing programs do not create personal data loss theft.

Bar Chart 4  
Our organization's consumer marketing programs do not create risks of personal data loss or theft.



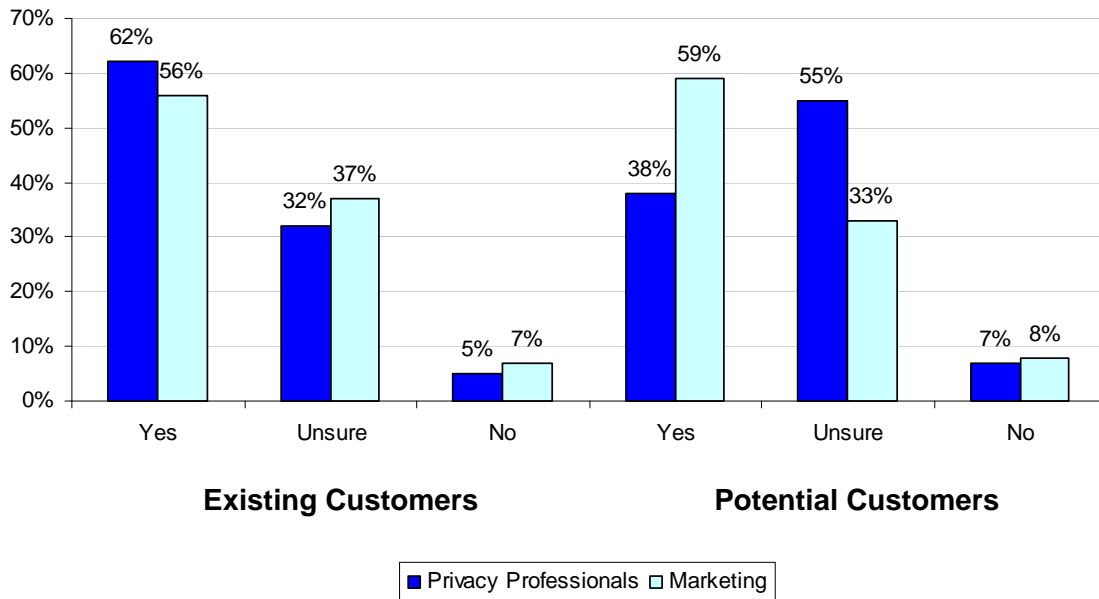
**Data breaches involving the loss or theft of consumer or customer information occur frequently and can result in the loss of existing and potential customers.**

Eighty-one percent of privacy professionals and 56% of marketers report that their organizations have had a data breach involving the loss or theft of consumer or customer information, with an additional 32% of marketers and 9% of privacy professionals uncertain. Only a small minority of both privacy professionals and marketers report that their organization has not had a data breach.

Of those organizations reporting a data breach, the majority (59% as reported by the privacy professionals and 83% as reported by the marketers) have had more than one breach in the past 24 months. While 67% of privacy professionals knew that the breach required consumer notification, many marketers were uncertain.

Both groups believe that data breaches affect the ability to acquire and retain customers (Bar Chart 5). While there was a lot of uncertainty among respondents in both groups, only a small minority (well under 10% for both groups) believe that the data breach did not result in the loss of existing or potential customers. Interestingly, more privacy professionals think that a data breach will affect the relationship with existing customers whereas marketing thinks that there will be a greater affect on attracting potential customers. Both groups also agree that the incident(s) resulted – or could result – in the diminishment of the marketing campaign objectives.

Bar Chart 5  
If your organization experienced a breach, did the incident(s) result in the loss of existing or potential customers?

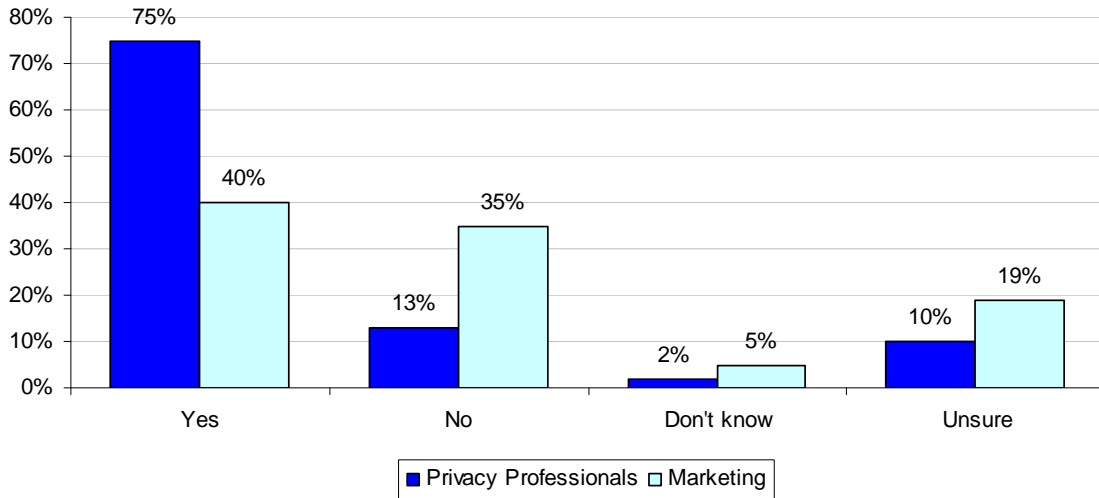


**Third parties are cited as the source of many data breaches. However, marketers are less knowledgeable about whether or not their organizations have policies that limit the types of personal information they can share.**

According to 46% of the privacy professionals and 48% of the marketers who experienced a data breach, a third party such as a vendor, business partner or contractor was the source of the breach. However, there is a significant gap in perceptions between both groups in whether the organization limits the types of personal information it will share with third parties for purposes of marketing as shown in Bar Chart 6. Seventy-five percent of privacy professionals believe their

organizations limit types of information but only 40% of marketers report that they do. Whereas, 35% of marketers acknowledge that they believe their organizations do not limit data they outsource.

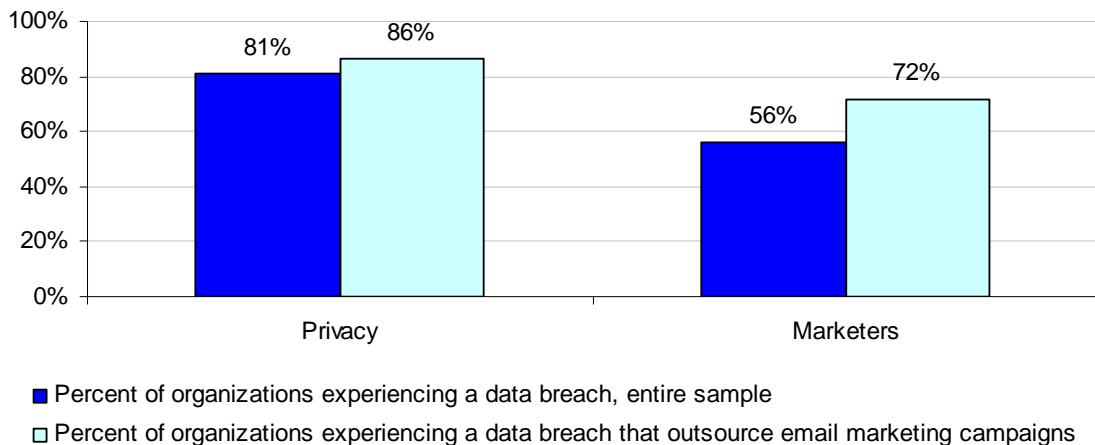
Bar Chart 6  
Does your organization limit the types of personal information it will share with third-parties for purposes of marketing?



**Organizations that outsource email marketing campaigns appear to be more likely (higher percentage frequency) to experience a data breach.**

As reported previously, 81% of privacy professionals and 56% of marketers say that their organizations had a data breach. Further analysis reveals, as shown in Bar Chart 7, that 86% of privacy professionals who work in organizations that outsource email marketing campaigns had a data breach and 72% of marketers who work in organizations that outsource email marketing campaigns had a data breach.

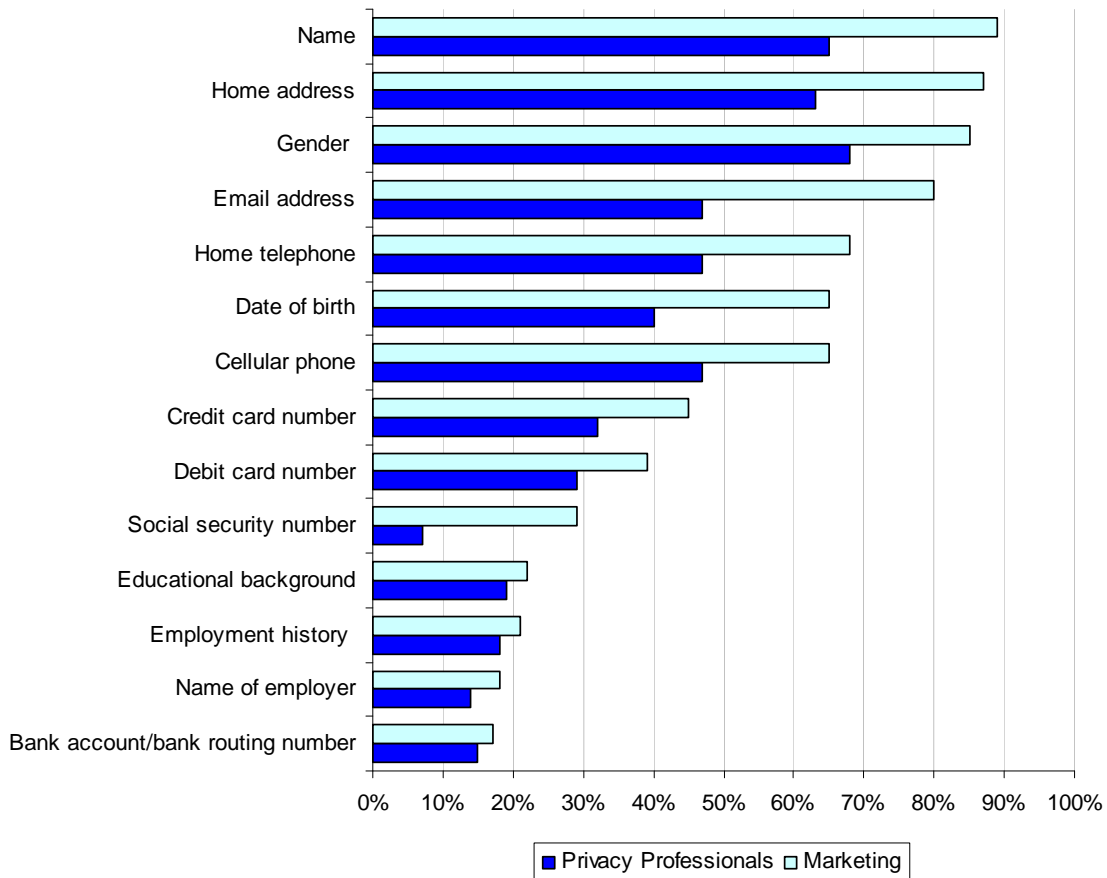
Bar Chart 7  
Did your organization have a data breach and outsource email marketing campaigns?



**Although they acknowledge that privacy is an important personal issue for them (99% of privacy professionals and 93% of marketers), marketers are willing to share sensitive information. However, privacy professionals and marketers don't agree on what types of personally identifiable information should be trusted to a third party.**

Not only are marketers more apt to not limit data sharing practices, they also share a wider array of consumer information. Bar Chart 8 indicates some of the personal data privacy professionals and marketers would share. The differences in opinion between the groups are noticeable. Of particular interest, there is sensitive personally identifiable information that marketers would share, including credit number (45%), debit card number (39%), social security number (29%), and bank account/routing number (17%).

Bar Chart 8  
If your organization limits the types of personal information it will share with third parties for the purposes of marketing, please indicate the types of personal information that your organization will share.



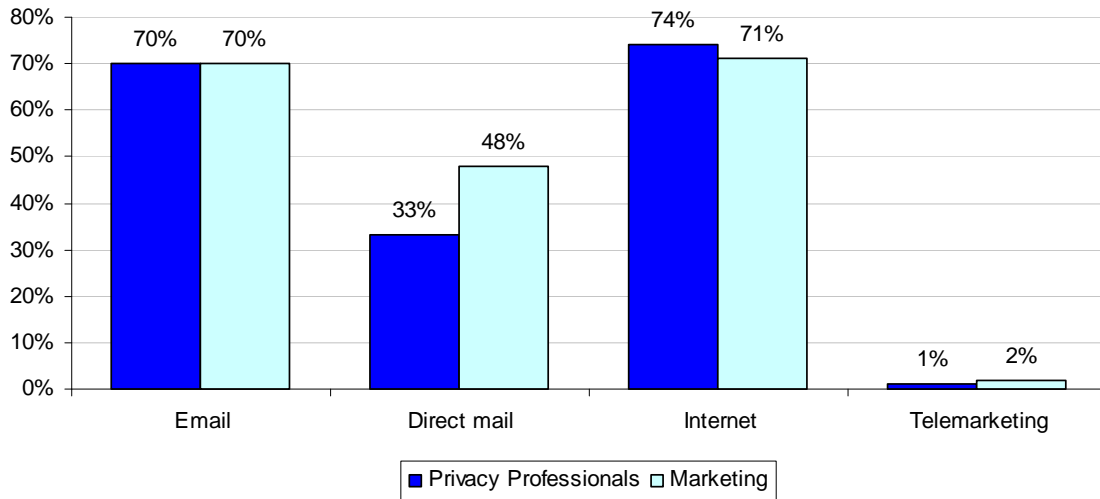
**A majority of organizations outsource marketing activities but will consider in-sourcing email marketing campaigns to protect customers' personal information.**

Fifty-nine percent of marketers and 53% of privacy professionals report that their organizations outsource marketing activities, most commonly Internet marketing and email marketing campaigns. The reasons cited are to reduce costs and improve efficiency. Even though outsourcing is prevalent, some organizations decide to keep marketing activities in-house. Both marketers and privacy professionals cite quality of service and data protection and privacy as reasons why they don't outsource to third parties.

**Email and Internet marketing channels present the greatest threat to consumers and customers’ personal information. Both groups agree that they would consider in-sourcing to reduce risks to personal information. This suggests there is an understanding that if the personal data was kept within the organization it would be easier to safeguard.**

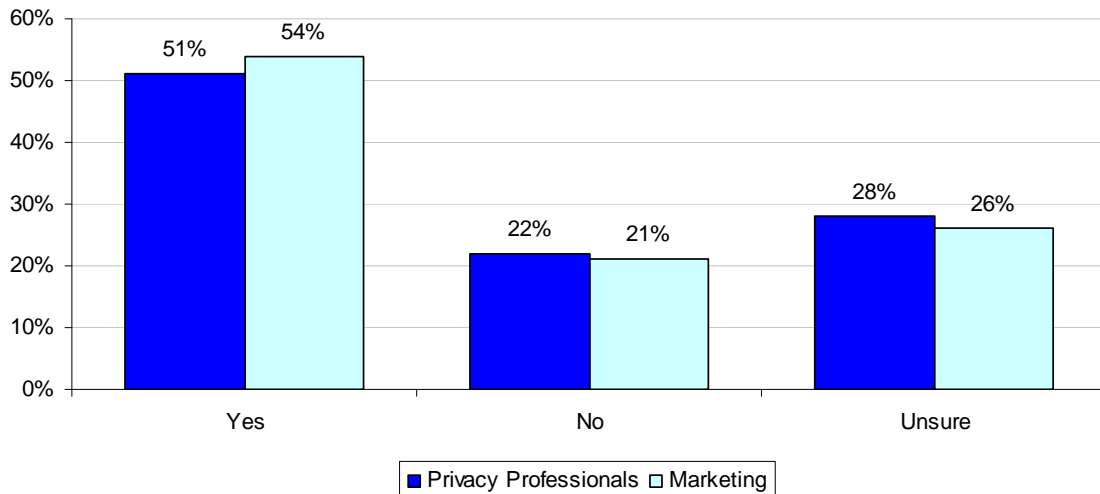
Of the various marketing campaigns, companies consider Internet marketing and email marketing to be the outbound marketing channels that present the greatest privacy risk (Bar Chart 9).

Bar Chart 9  
Which of the following outbound marketing channels present the greatest risks to privacy within your organization today?



Consequently, as Bar Chart 10 indicates, about half of marketers and privacy professionals would consider in-sourcing email marketing campaigns to protect customers’ personal information. An additional 28% percent of privacy professionals and 26% of marketers are unsure.

Bar Chart 10  
Would you ever consider in-sourcing your email marketing campaign to protect the privacy of your customers’ personal information?



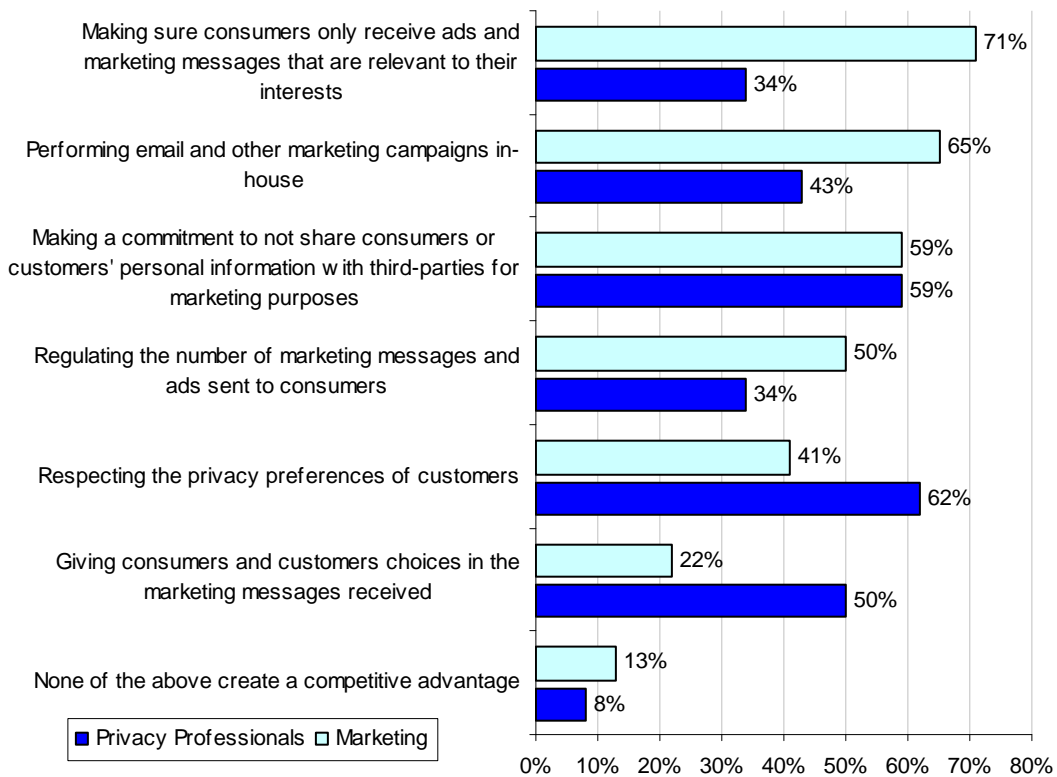
**Consumers’ trust of an organization’s privacy commitments is important to both groups, but there is uncertainty whether superior privacy practices create a competitive advantage.**

Ninety-one percent of privacy professionals and 75% of marketers believe it is important for customers to trust an organization’s privacy commitments. However, there is uncertainty among both groups that advancing **superior** privacy practices is a competitive advantage, according to 35% of privacy professionals and 43% of marketers.

While approximately the same percentage of marketers (40%) and privacy professionals (38%) agree that advancing superior privacy practices can be a competitive advantage, the groups differ on what those competitive advantages would be, as shown in Bar Chart 11.

Privacy professionals believe that respecting the privacy preferences of customers (62%) and making a commitment not to share consumers or customers’ personal information with third parties for marketing purposes (59%) are important. Meanwhile, marketers believe making sure consumers only receive ads and marketing messages that are relevant to their interests (71%) and performing email and other marketing campaigns in-house (65%) are important practices (65%).

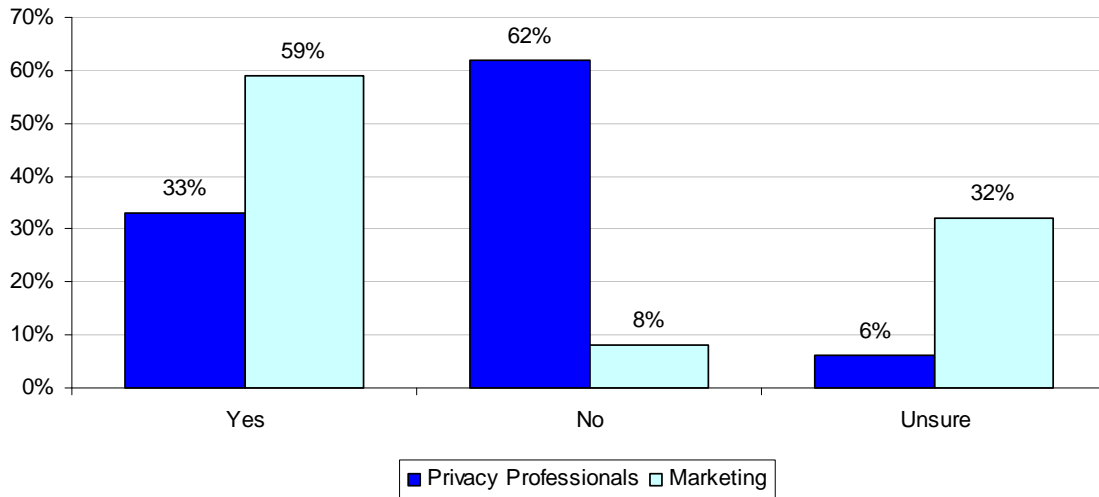
Bar Chart 11  
Which of the following practices do you believe create a competitive advantage?



**There is a huge difference in perceptions about privacy requirements being a hindrance to marketing initiatives.**

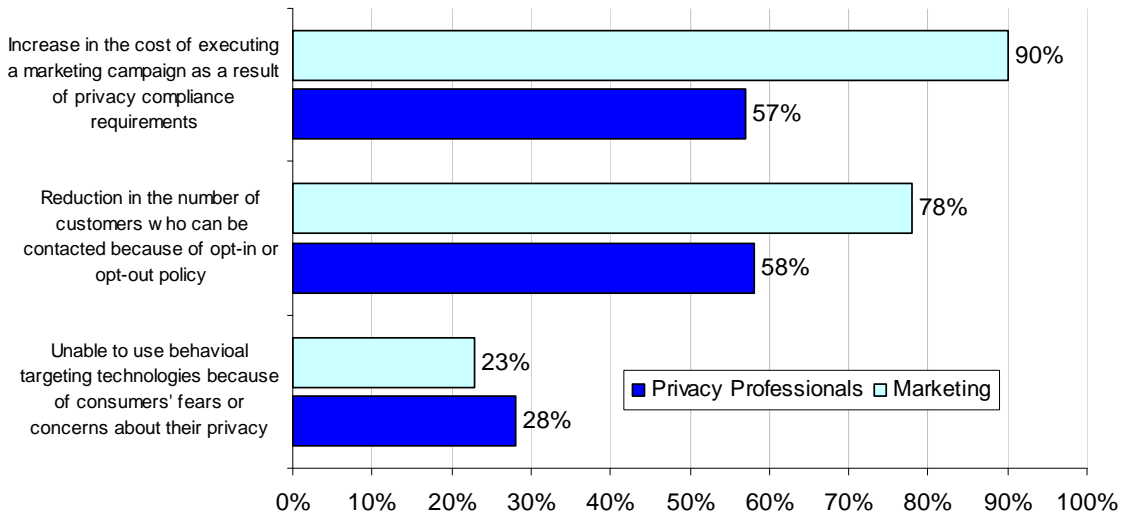
While both groups hold similar perceptions about the importance of having trusted relationships with their customers, marketers and privacy professionals are more definitive – and have opposite views - when considering if privacy requirements make it more difficult to market to present and potential customers. As shown in Bar Chart 12, the majority of marketers (59%) believe that it is more difficult, while the majority of privacy professionals (62%) indicate that it is not.

Bar Chart 12  
Do you believe your organization's privacy requirements make it more difficult to market to present and potential future customers?



However, there is agreement between marketers and privacy professionals about why privacy requirements make it more difficult to market to present and future customers. Although it is to differing degrees, both groups agree that privacy requirements increase the cost of a marketing campaign and reduce the number of customers who can be contacted because of opt-in or opt-out policy (Bar Chart 13).

Bar Chart 13  
Why is it more difficult to market to customers because of privacy?



### III. Recommendations

Marketers and privacy professionals differ in their perceptions about how email marketing practices affect consumers' privacy rights and risks to personal information. However, both groups understand the importance of establishing a trusted relationship with existing and prospective customers.

Marketers also believe that consumers are willing to give up some personal information in order to receive emails with messages that they find relevant, according to previous research conducted by Ponemon Institute. However, privacy professionals believe that consumers expect that organizations respect their privacy preferences. It is interesting that both groups think making a commitment to not share personal information with third parties for marketing purposes can be a competitive advantage.

We believe the following practices can both strengthen an organization's privacy practices and the effectiveness of marketing campaigns.

- When outsourcing personal data, organizations should make sure the third parties are held to the same standards of data protection and control as they have in their own organizations. This can be accomplished through assessing the data security practices of the third party. Organizations should also determine if the third party is outsourcing to other vendors and if those vendors have the same quality of data protection controls.
- Organizations should identify how privacy can support the organization's business and marketing models. For example, privacy professionals should demonstrate how the organization's privacy and data security practices can influence consumers' decisions to choose their organization over the competition. In addition, with more privacy laws expected to be passed, privacy professionals should assist marketers in collecting more information but in compliance with regulations.
- On-premise technology that delivers targeted emails without requiring the transfer of data to a third party will not only enhance the success of an organization's marketing campaigns but will also reduce the likelihood of a data breach involving sensitive data. Privacy professionals

can advise marketers on how to ensure that the data used to send relevant messages is in alignment with corporate privacy policies and consumers' needs and expectations.

- Privacy professionals should partner with marketers on quantifying the positive impact of privacy and trust to brand image. They should promote the goal of treating customer information as an asset and as a result should be protected from a data breach.

These practices would help bridge the existing gap between marketers and privacy professionals. Working together, they can help reduce the risks to consumer data and create a more trusted relationship with consumers. As previous Ponemon Institute research has demonstrated, trust results in consumers being more receptive to marketing messages and, as a result, more interested in purchasing products and services.

#### IV. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- 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. Despite non-response tests, 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: The accuracy is based on contact information and the degree to which the list is representative of American consumers. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.
- 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 the possibility that a subject did not provide a truthful response.

#### V. Sample

Table 1 reports the sample characteristics. We asked 30,359 adult-aged Americans to participate in this Web survey: 8,956 privacy and data protection professionals and 21,403 marketers. In total, 1,737 respondents completed their survey results. Of returned instruments, 347 survey forms were rejected because of reliability checks. A total of 1,390 surveys were analyzed in our final sample: 521 from privacy professionals and 869 from marketers. This sample represents a 5.82% net response rate for privacy professionals and 4.06% net response rate for marketers.

<b>Table 1: Sample characteristics</b>	Privacy Professionals Freq.	Privacy Professionals Pct%	Marketing Freq.	Marketing Pct%
Sampling frame	8,956	100.00%	21,403	100.00%
Bounced back	803	8.97%	3,006	14.04%
Total response	629	7.02%	1108	5.18%
Rejected surveys	108	1.21%	239	1.12%
Final sample	521	5.82%	869	4.06%

Following are key demographics survey respondents. Table 2 reports the respondent's organizational level. The majority of the respondents are directors, managers or associates/staff.

<b>Table 2: Organization level of current position</b>	Privacy Professionals	Marketing
--	-----------------------	-----------

Senior Executive	1%	0%
Vice President	1%	2%
Director	19%	14%
Manager	26%	35%
Associate/staff	44%	38%
Other	9%	11%

Table 3 provides primary department the respondent or IT security leader reports to within the organization.

<b>Table 3: Primary person respondent or IT security leader reports to</b>	Privacy Professionals	Marketing
Marketing	1%	78%
Privacy	39%	0%
Compliance	26%	0%
Research	0%	10%
Information technology	23%	7%
Security	9%	0%
Other	2%	5%

The Privacy professionals who responded to this survey typically report to someone in the privacy (39%), compliance (26%) or information technology (23%) departments, whereas marketing professionals report primarily through the marketing department (78%), and a small group is within research (10%).

Table 4 describes the respondents' experience. On average, the privacy professionals have approximately nine years of experience, with more than four years in the privacy field. The marketers have, on average, more than nine years of experience with approximately five years in marketing.

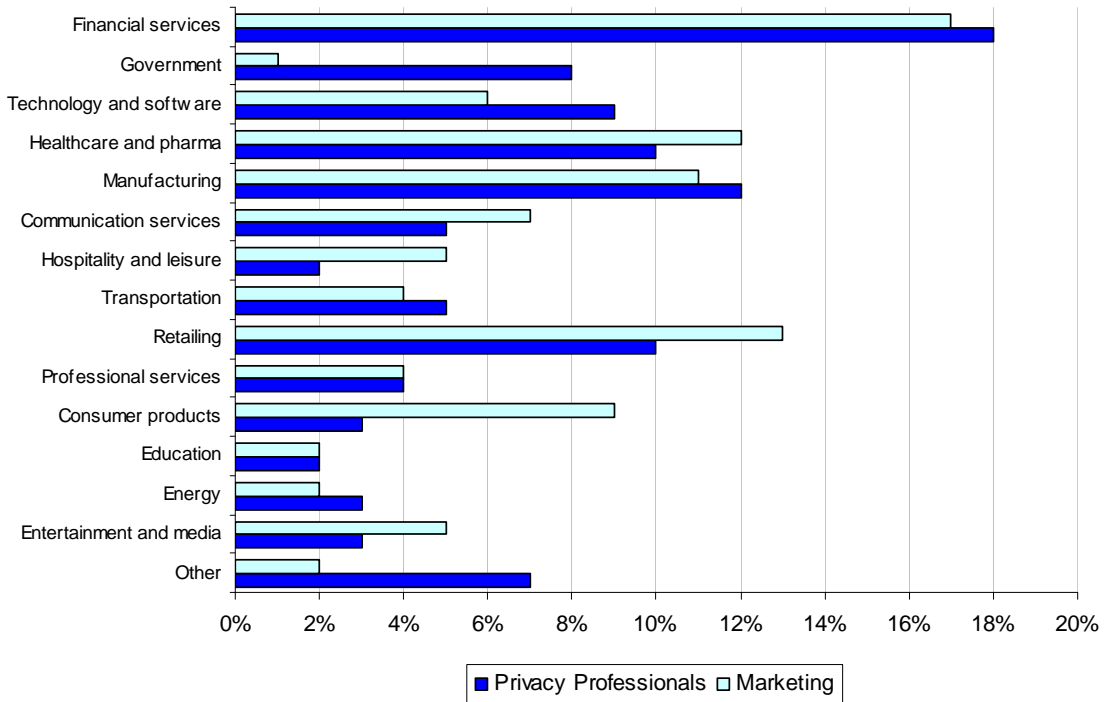
<b>Table 4: Experience levels</b>	Privacy Professionals	Marketing
Total years of overall experience	8.55	9.11
Total years of marketing or privacy experience	4.65	5.13
Total years in current position	3.07	2.85

The next set of data provides further information about the employers. Table 5 reports if the company is publicly traded. The majority of the respondents are from companies that are publicly traded on the New York Stock Exchange.

<b>Table 5: Company exchange listing</b>	Privacy Professionals	Marketing
Major stock exchange (NYSE or NASDAQ)	65%	61%
Minor stock exchange	4%	6%
Not listed on stock exchange	31%	33%

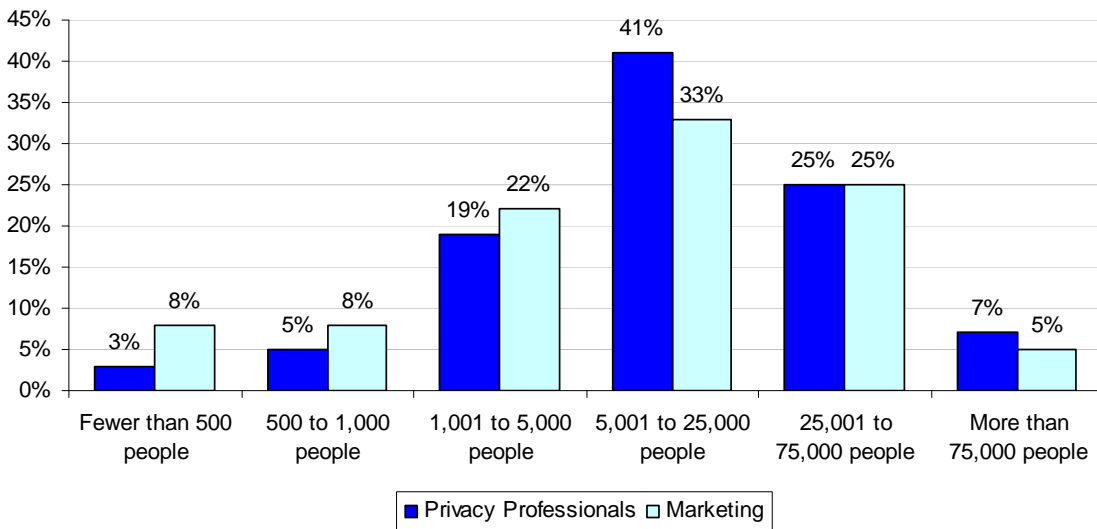
Bar Chart 14 shows the company's industry focus. Financial services; healthcare and pharmaceuticals; retailing; and manufacturing are the industries that are most commonly represented in the survey from both groups.

Bar Chart 14  
What industry best describes your organization's industry focus?



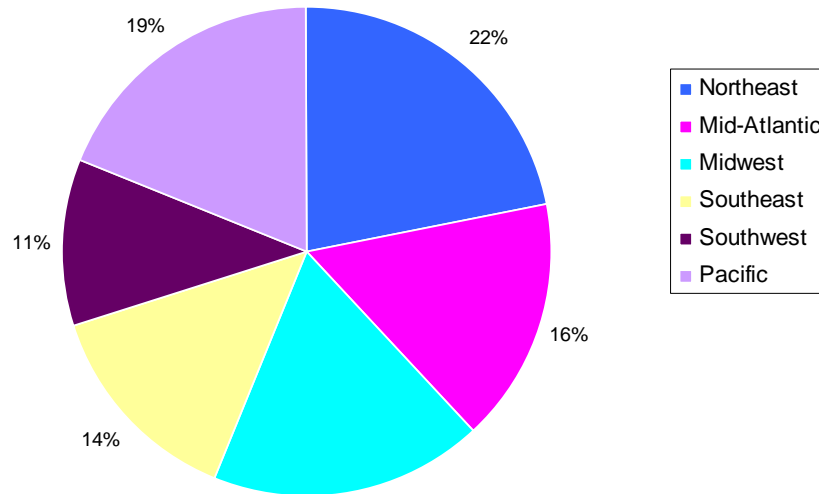
Bar Chart 15 displays the worldwide headcount of the respondent's companies. The respondents work for organizations of all sizes, with the largest group of respondents working for companies that employ 5001 to 25,000 people.

Bar Chart 15  
What is the worldwide headcount of your organization?

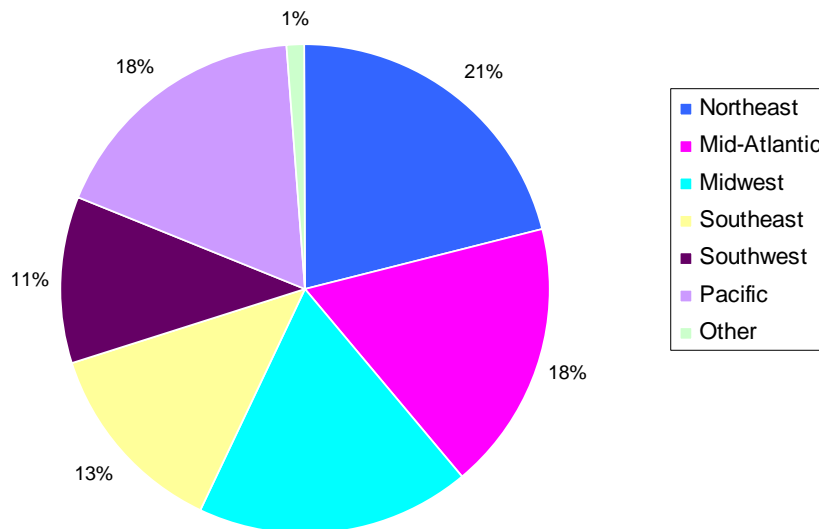


Pie Charts 1 and 2 report the distribution of respondents by region of the United States. As shown, they represent all major regions of the country. The northeast region represents the largest number of respondents, and the southwest region represents the smallest number of respondents.

**Pie Chart 1: Geographic regions of the United States  
Privacy Professionals**



**Pie Chart 2: Geographic regions of the United States  
Marketing**



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 us by letter, phone call or email:

Ponemon Institute LLC  
Attn: Research Department  
2308 US 31 North  
Traverse City, Michigan 49686  
1.800.887.3118  
[research@ponemon.org](mailto: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.