# Public Spaces Survey Study

Sponsored by 3M

Independently conducted by Ponemon Institute LLC

Publication Date: April 2017

# Public Spaces Survey Study

Ponemon Institute, April 2017

## Part 1. Introduction

Ponemon Institute is pleased to present the results of the *Public Spaces Survey* sponsored by 3M.

The purpose of this survey is to examine professional workers' sensitivity to visual hacking risks while working in public spaces. We conducted one-to-one interviews with professionals working on laptops in public places. Such places included cafes (various stores) and hotel lobbies (one national chain), which are both susceptible to visual hacking risk. The research was conducted in four cities in the United States. The researcher solicited more than 200 potential interviewees, resulting in a voluntary sample of 46 individuals.

**Procedures for the recruitment of interviewees:**

At first, the researcher silently observed the possible interviewee to make sure she or he is using a laptop computer in an open space. Before starting the interview, the researcher screened the interviewee, making sure she or he is a bona fide professional worker.

As a prelude to the interview, the researcher introduced Ponemon Institute as the organization responsible for conducting the study. The researcher did not reveal 3M as the sponsor of this research.

Interviewees were compensated $20 for approximately a 10-minute interview. No personally identifiable information was collected from these individuals. All survey procedures were conducted in conformance with CASRO[1] ethics and privacy practices.

Data was collected using a diagnostic interview script that contained objective (fixed formatted) questions relating to the individual's awareness and understanding of visual hacking risks in public spaces. The researcher provided the following definition as a prelude to the interview:

- What is visual hacking? Somebody sneaks a peek on a computer screen or smartphone at something they shouldn't be seeing, and you've been visually hacked. It's that easy. Organizations spend millions on IT security but do little to prevent the display of sensitive, proprietary and confidential data in plain sight. Failing to address this vulnerability can put any organization at risk.

**Key considerations for the interviewer:**

Before approaching the potential interviewee, the interviewer observed potential interviewees who were using laptops (not a tablet or smart phone). The interviewer scouted out "professional-looking" participants based on dress and demeanor.

Whenever feasible, the interviewer looked at qualitative cues to determine whether or not interviewees seemed concerned that their computer screens may be seen by others and what they appear to be doing (or not doing) to protect data from prying eyes. Following are some of the cues observed by the interviewee:

- Interviewees look as though they are trying to keep screens out of view of others
- Interviewees are using a privacy filter
- Interviewees appear concerned about using their laptops in crowded venues

Whenever feasible, the interviewer tried to view the type(s) of information on the interviewee's screen. This observation was conducted before launching the interview script. The interviewer attempted to make sure potential interviewees were doing work-related activities on their laptop rather than merely residing in the public space for other casual reasons.

During the interview process, the interviewer asked a few questions directed at the type of information that was visible on the interviewee's screen. For example, is it charts or figures displaying financial information? Is this information considered confidential or sensitive?

[1]CASRO is the Council of American Survey Research Organizations. Ponemon Institute is a member in good standing, which requires compliance to a rigorous ethics code. See www.CASRO.org for details.

**Public Spaces interview questions:**

Interviews were conducted over a four-week period ending on March 27, 2016. Following is the exact order of questions presented to all 46 interviewees.

Q1a. How important is the privacy of your personal information?

Q1b. If important, what steps do you take to protect the privacy of your personal information?

Q1c. If not important, why?

Q2. Prior to now, have you ever heard the term visual hacking?

Q3a. How concerned are you about visual hacking?

Q3b. If concerned, why?

Q3c. If not concerned, why?

Q4. What steps are you taking to protect your personal information when traveling on business or working in public places?

Q5a. Have you ever had someone look over your shoulder at your laptop in a public place?

Q5b. If yes, how frequently has this happened?

Q6a. Have you ever inadvertently looked at someone's laptop in a public place?

Q6b. If yes, how frequently has this happened?

Q7a. Does your company have a privacy or data protection policy?

Q7b. If yes, what is contained in the policy?

Q7c. If yes, does the policy address visual hacking issues?

Q7d. If yes, are employees in your company generally compliant with this policy?

Q7e. If no, why?

Q8. Where are employees of your company most vulnerable to visual hacking?

Q9. How should your company educate its employees about privacy and data protection issues?

Q10a. Are you familiar with privacy and data protection solutions?

Q10b. If yes, which ones?

## Part 2. Key Findings

More than 80 percent of interviewees believe the privacy of their personal information is important or very important to them.

**Figure 1. How important is the privacy of your personal information?**
n = 46 interviewees

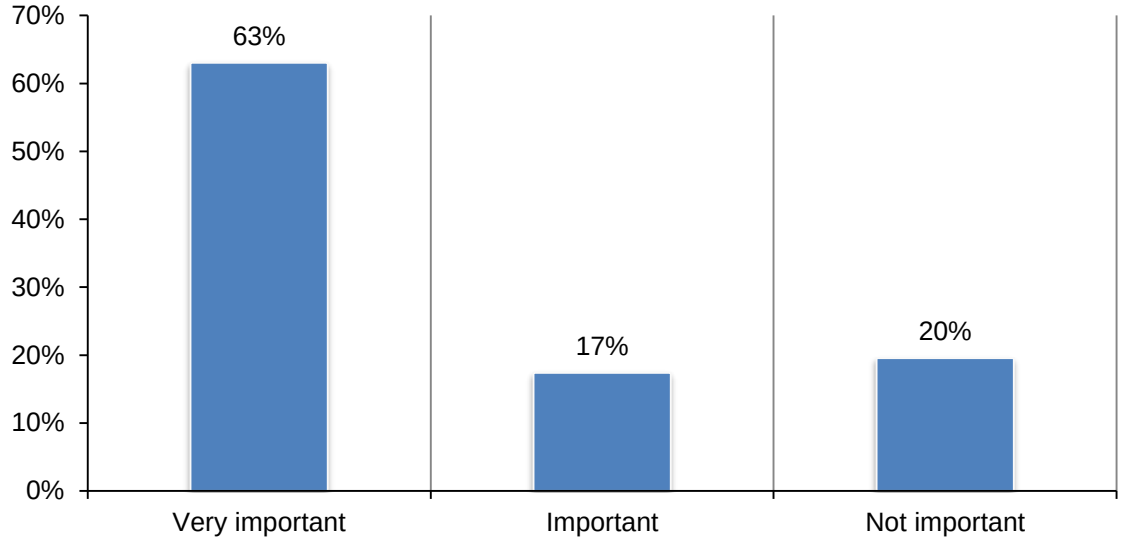



**Table 1. If not important, why?**

| Paraphrased verbatim | Times mentioned |
|---|---|
| Privacy is not a priority for me | 7 |
| I can't do anything to protect my privacy | 6 |
| I'm anonymous on the Internet, so I don't need to worry about privacy | 5 |
| I like sharing personal information on the Internet and social media | 4 |
| I have nothing to hide | 3 |
| I have never been harmed, despite data breaches involving my personal information | 2 |
| In today's world, it is not possible to protect (my privacy) | 2 |
| Privacy fears are not grounded in reality | 1 |
| No comment | 1 |

**Table 2. What steps do you take to protect the privacy of your personal information?**

| Paraphrased verbatim | Times mentioned |
|---|---|
| Avoid visiting high-risk websites | 21 |
| Change passwords | 19 |
| No steps taken | 18 |
| Never provide Social Security Number | 12 |
| Use hard (complex) passwords | 11 |
| Lock laptop and other mobile devices with passcode or biometric | 9 |
| Exercise care when using public networks (WiFi) | 8 |
| Make sure laptop and other mobile devices have up-to-date security software | 8 |
| Exercise care when using my credit or debit card online | 7 |
| Exercise care when working on laptop or mobile devices in public places | 7 |
| Choose high privacy settings on browser | 6 |
| Exercise care when receiving/opening emails from unknown parties | 6 |
| Never share my password(s) with anyone else | 6 |
| Visit websites known to be authentic (avoid spoofed sites) | 6 |
| Whenever feasible, encrypt data on laptop and other mobile devices | 6 |
| Erase cookies in my browser | 5 |
| Exercise care when downloading free software/updates and apps | 5 |
| Exercise care when talking to others in public places | 5 |
| Shut down laptop when not in use (idle) | 5 |

**Figure 2. Prior to now, have you ever heard the term visual hacking?**
n = 46 interviewees

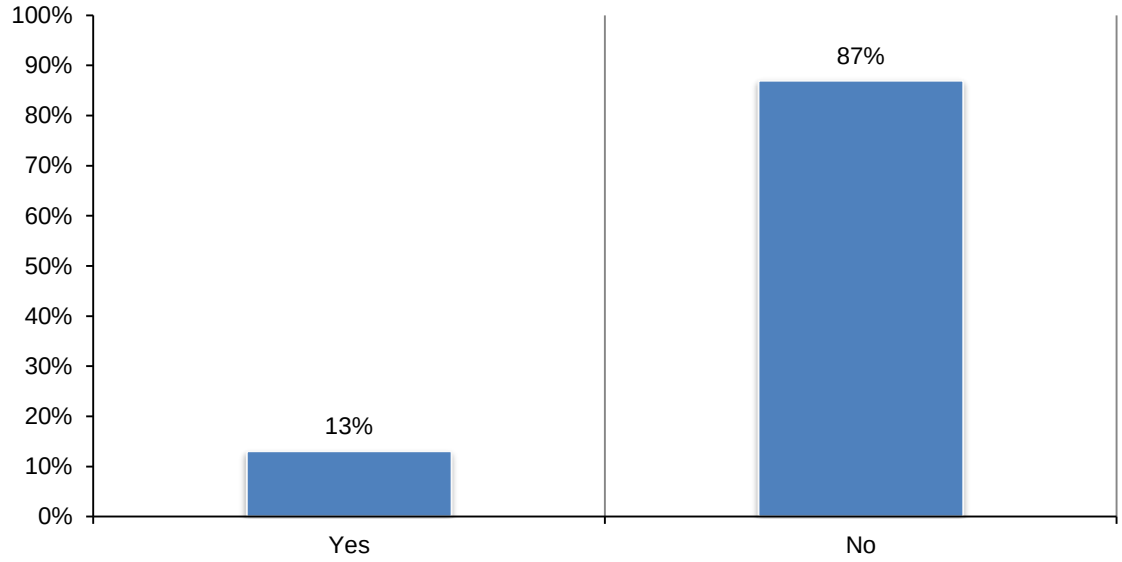



**Figure 3. How concerned are you about visual hacking?**
n = 46 interviewees

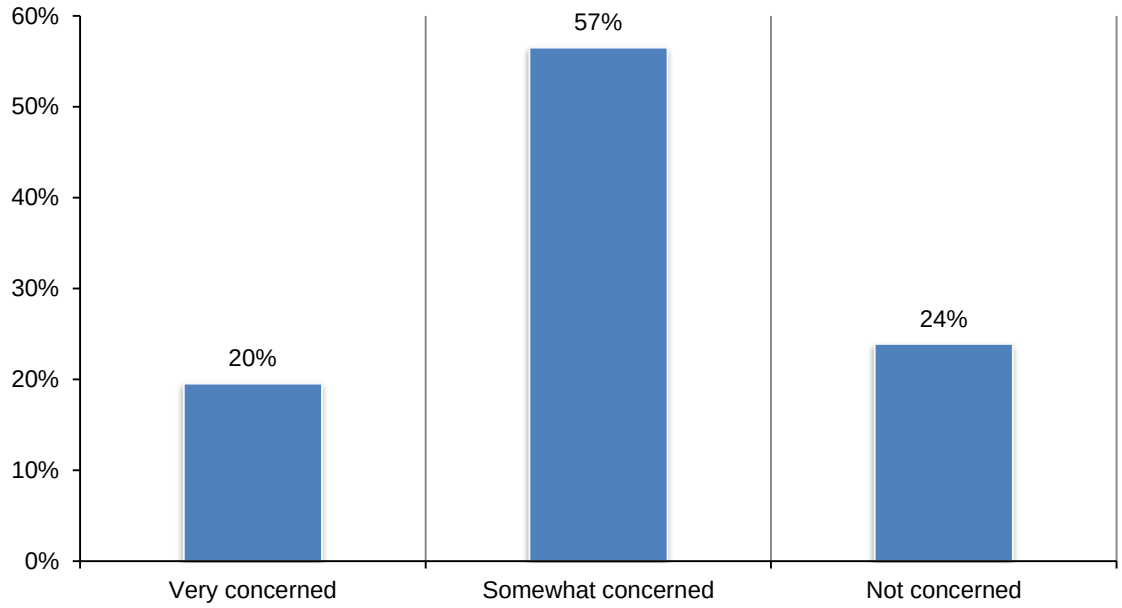


**Figure 4. If concerned about visual hacking, why?**
n = 35 interviewees

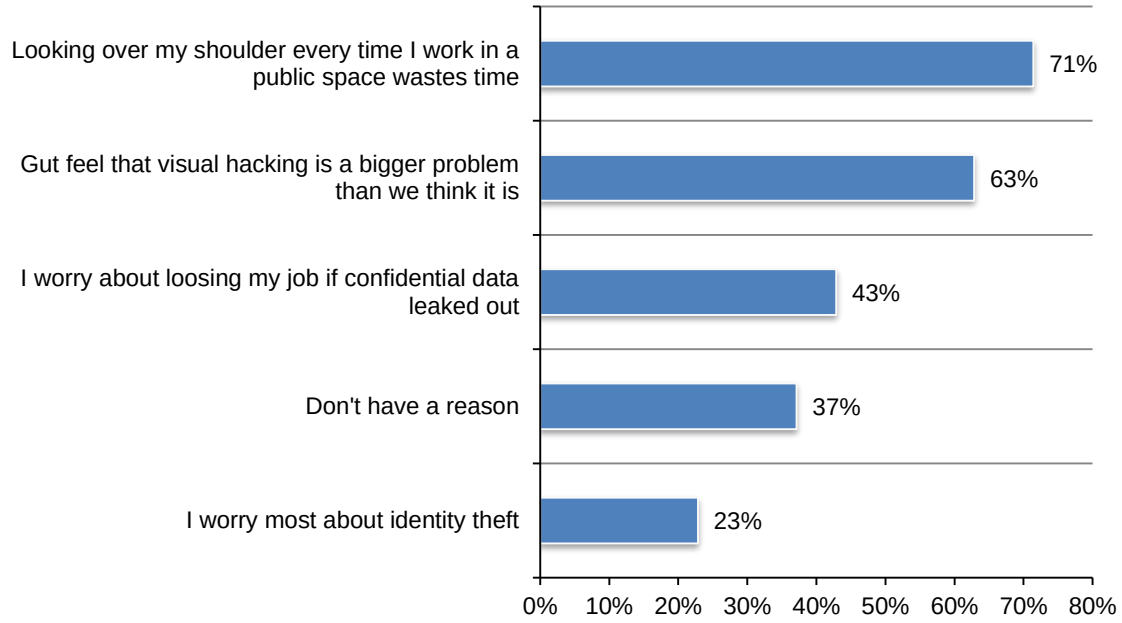



**Figure 5. If not concerned about visual hacking, why?**
n = 11 interviewees

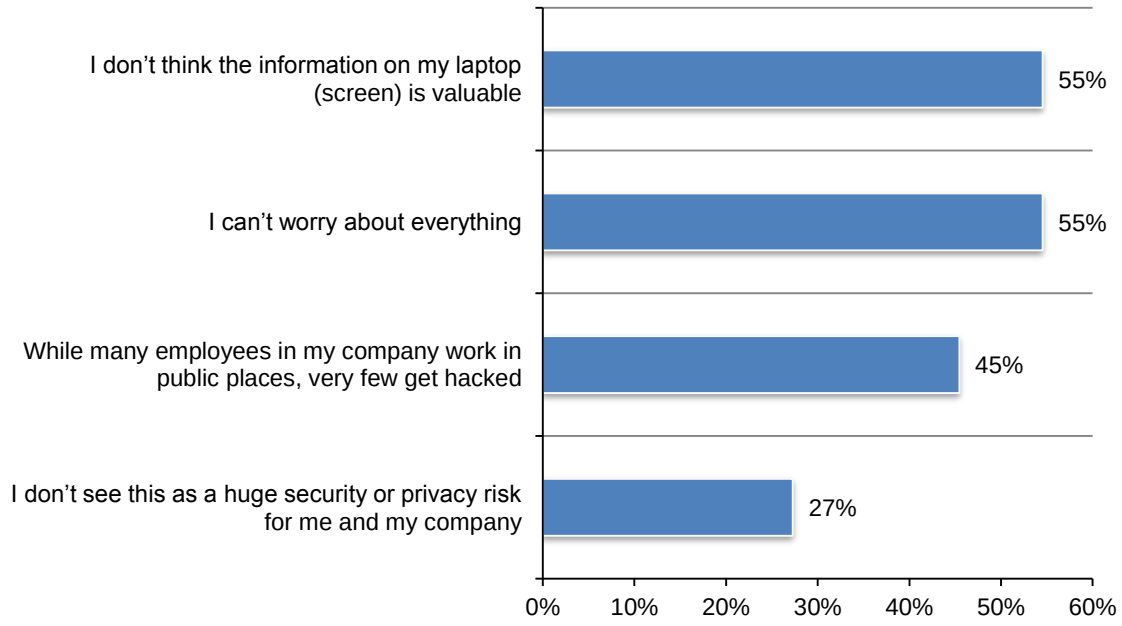


**Table 3. What steps are you taking to protect your personal information when traveling on business or working in public places?**
n = 35 interviewees

| Paraphrased verbatim | Times mentioned |
|---|---|
| No steps taken | 18 |
| Exercise care when working in close proximity to others in public places | 13 |
| Exercise care when using my credit or debit card with cabs and restaurants | 12 |
| Lock laptop and other mobile devices with passcode or biometric | 9 |
| Exercise care when using public networks (WiFi) | 8 |
| Make sure laptop and other mobile devices have up-to-date security software | 8 |
| Exercise care when working on laptop or other mobile devices in public places | 7 |
| Never share my password(s) with anyone else | 6 |
| Visit websites known to be authentic (avoid spoofed sites) | 6 |
| Shut down laptop when not in use (idle) | 5 |
| Never share smart phone with others | 2 |
| Update laptop and other mobile devices as soon as security patches are available | 2 |

**Figure 6. Have you ever had someone look over your shoulder at your laptop in a public place?**
n = 46 interviewees

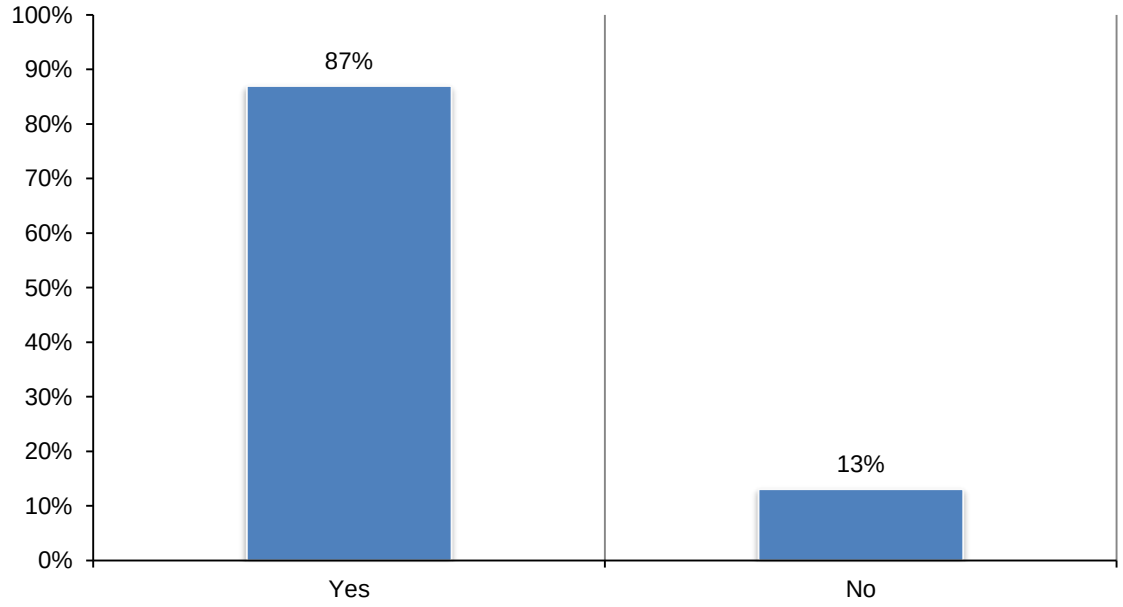


**Figure 7. If yes, how frequently has this happened?**
n = 40 interviewees

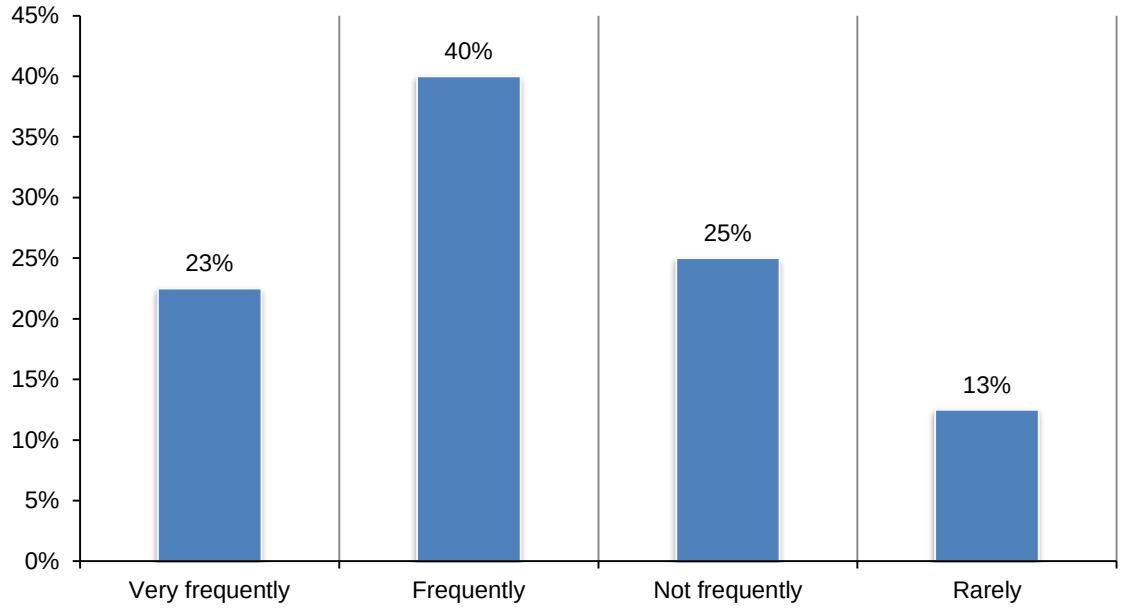



**Figure 8. Have you ever inadvertently looked at someone's laptop in a public place?**
n = 46 interviewees

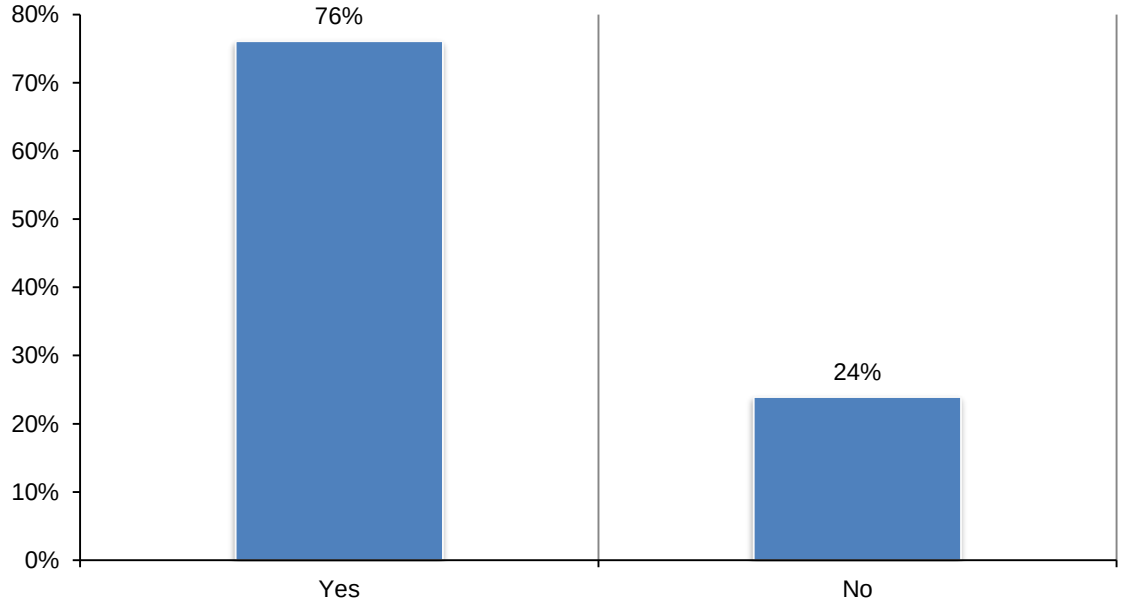


**Figure 9. If yes, how frequently has this happened?**
n = 35 interviewees

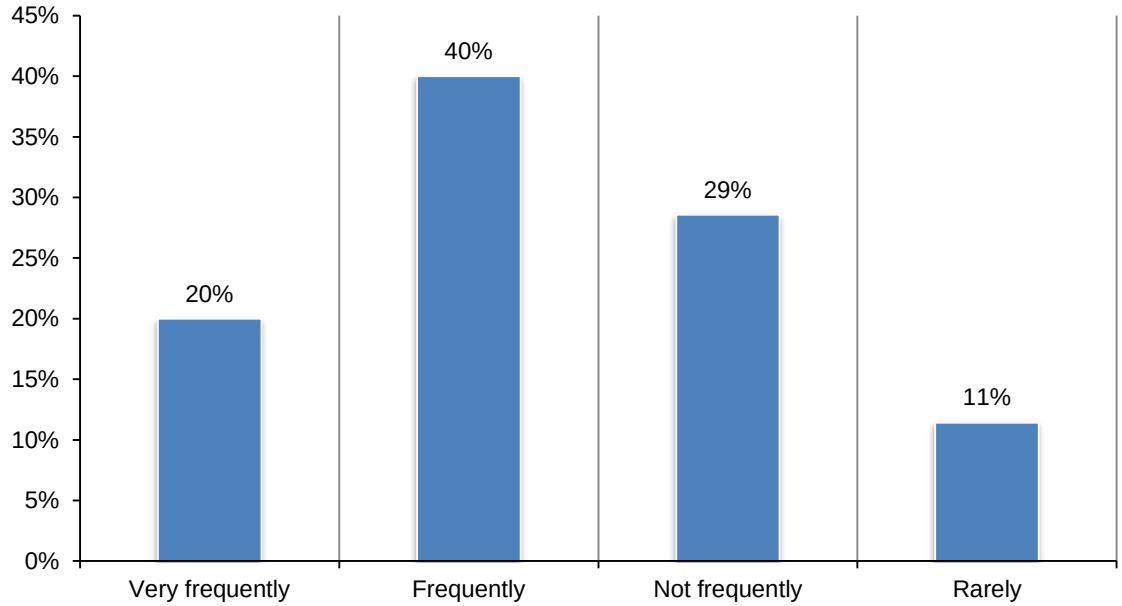



**Figure 10. Does your company have a privacy or data protection policy?**
n = 46 interviewees

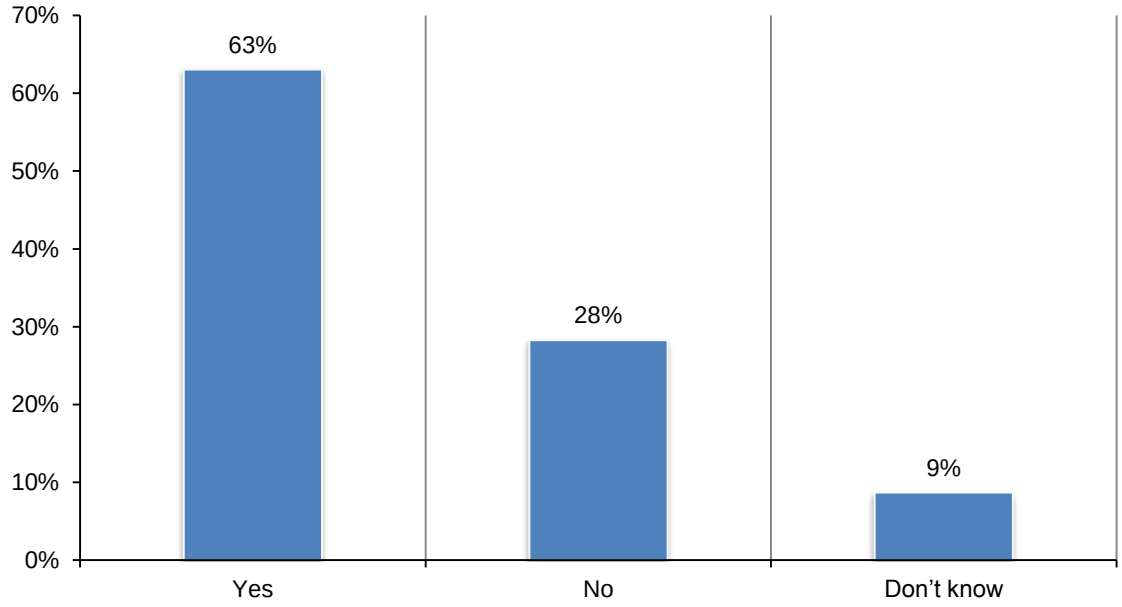


**Table 4. What is contained in the policy?**
n = 29 interviewees

| Paraphrased verbatim | Times mentioned |
|---|---|
| Can't recall | 13 |
| Does and don'ts such as never share your password | 10 |
| Privacy rights and legal (compliance) requirements | 9 |
| Shredding documents | 9 |
| Maintaining a clean desk | 8 |
| Why privacy and data protection is everyone's business | 6 |
| About getting permission to collect and share data | 5 |
| Accessing only the data you have a right to see | 5 |
| Good email practices (including falling prey to phishing scams) | 5 |
| Accessing the company's computers from remote or home office | 3 |

**Figure 11. If yes, does the policy address visual hacking issues?**
n = 29 interviewees

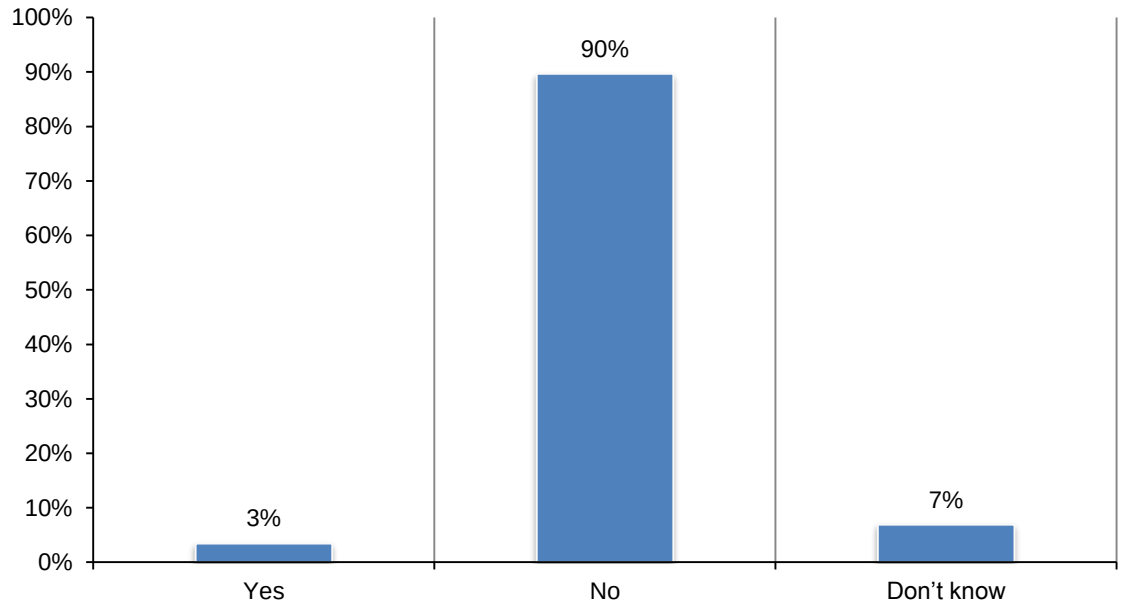



**Figure 12. Are employees in your company generally compliant with this policy?**
n = 29 interviewees

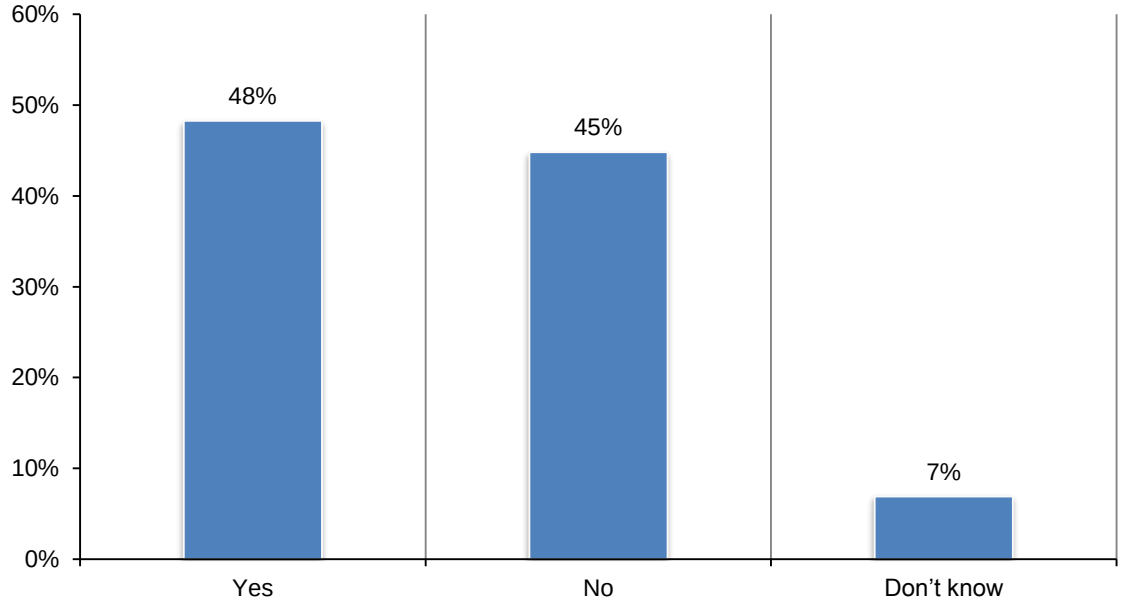


**Table 5. If no, why?**
n = 13 interviewees

| Paraphrased verbatim | Times mentioned |
|---|---|
| Most people don't care about privacy or security | 4 |
| Most employees cut corners when it comes to security | 3 |
| Too many policies that all say the same thing | 2 |
| Policies are too complex and boring to read | 3 |
| Security is only important if or when you get caught | 1 |
| Don't know | 7 |

**Figure 13. Where are employees of your company most vulnerable to visual hacking?**
n = 46 interviewees

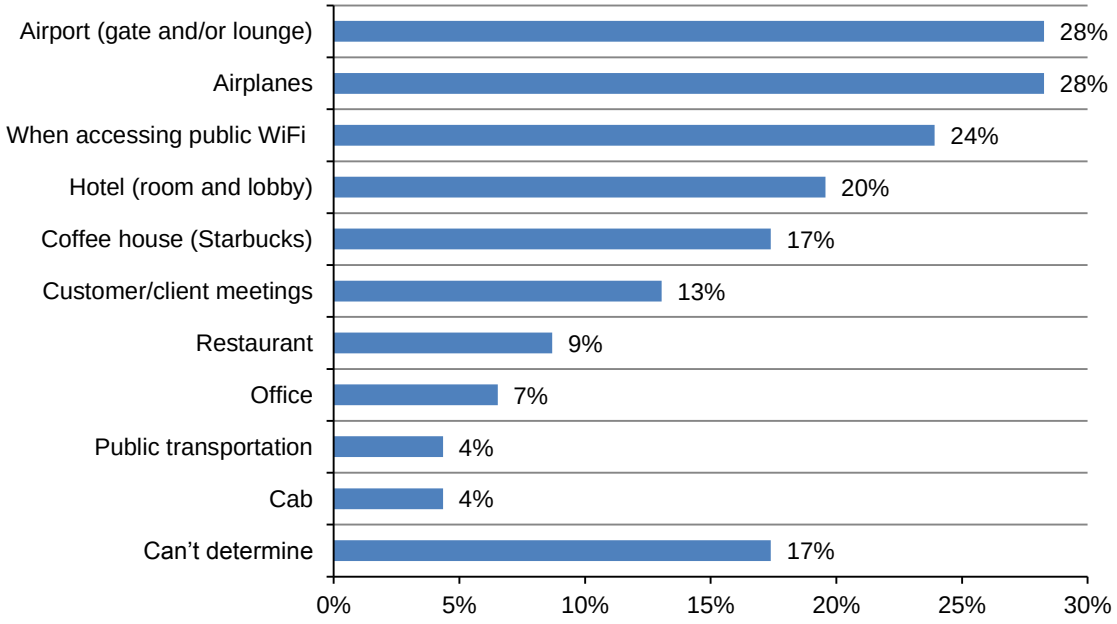


**Figure 14. How should your company educate its employees about privacy and data protection issues?**
n = 46 interviewees

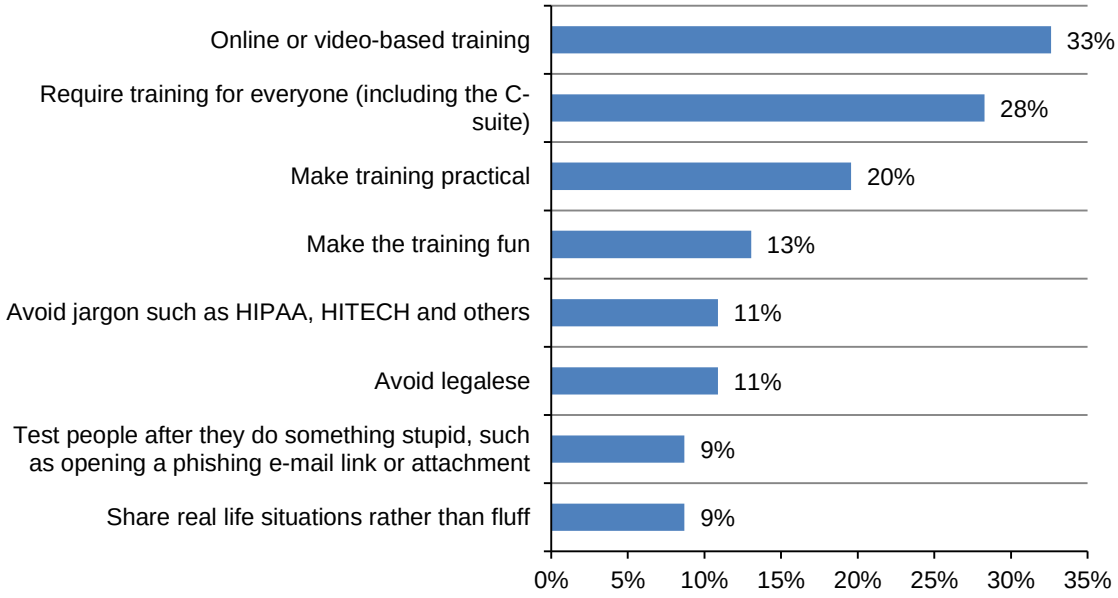



**Figure 15. Are you familiar with privacy and data protection solutions?**
n = 46 interviewees

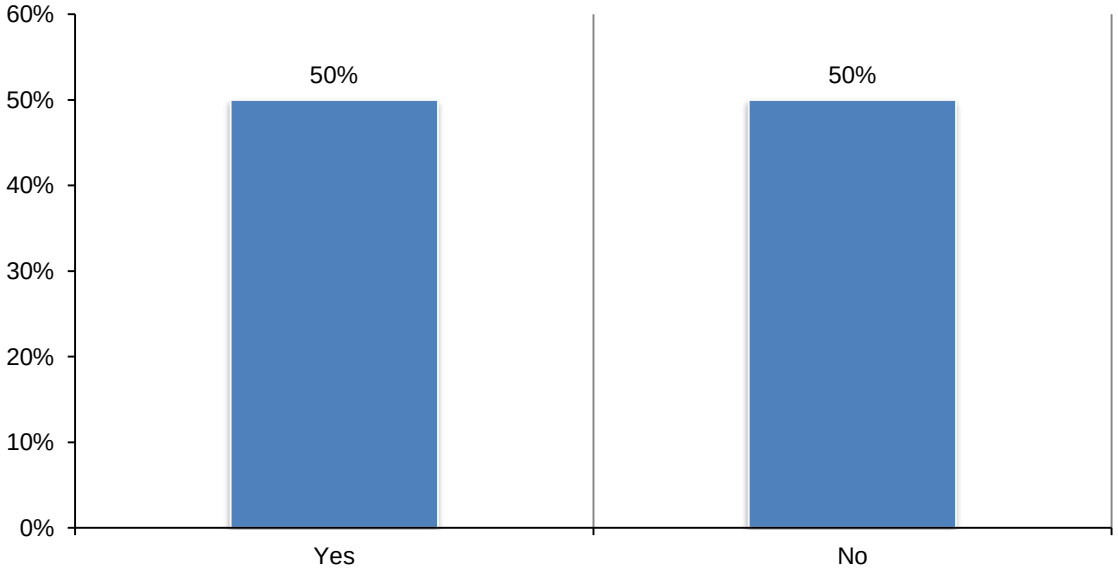
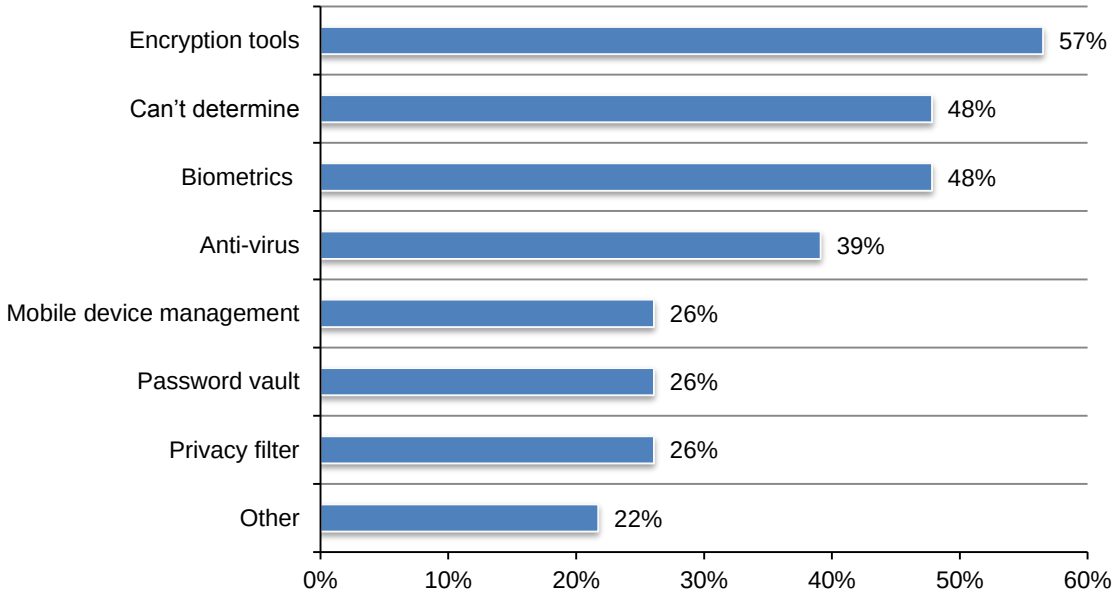


**Figure 16. If yes, which ones?**
n = 23 interviewees

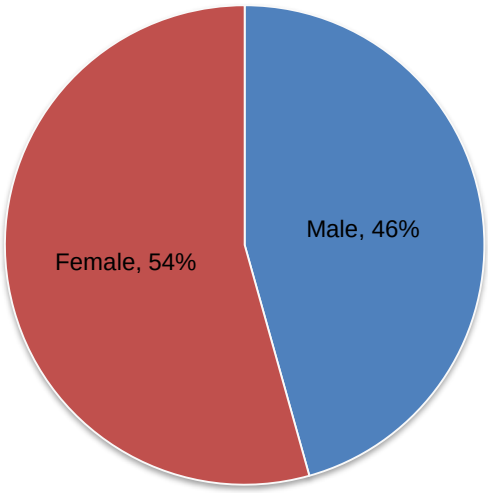


**Part 3. Demographics**

Data was collected using a diagnostic interview script that contained objective (fixed formatted) and demographic questions relating to the individual's awareness and understanding of visual hacking risks in public spaces. Interviews were conducted over a four-week period.

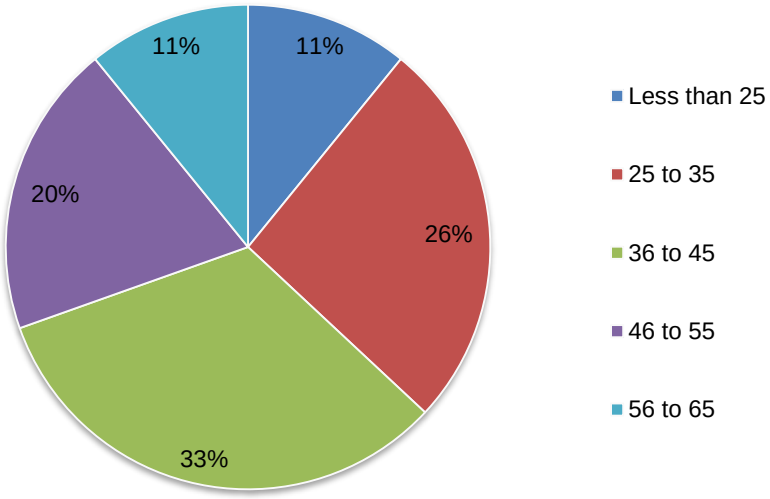
As shown in Figure 16, 54 percent of interviewees are female and 46 percent are male.

**Pie Chart 1. Gender of interviewees**
n = 46 interviewees




More than half (59 percent) of interviewees are between the ages of 24 to 45 years.

**Pie Chart 2. Age range of interviewees**
n = 46 interviewees



**Part 4. Limitations**

There are inherent limitations to interview-based research that need to be carefully considered before drawing inferences from the findings presented here. The following items are specific limitations:

- Findings are based on a small sample of 46 individuals, which limits our ability to draw definitive conclusions from interview responses.
- We acknowledge it is possible that individuals who did not participate are substantially different than does who did in terms of the orientation to privacy and visual hacking risks.
- The quality of interview research is based on the integrity of confidential responses received from interviewees. There is always the possibility that some interviewees did not record accurate results.
- A final limitation of this study concerns the public space where interviews took place. It is possible that sample size and composition might differ across different venues -- for instance, at airports or in-air flights.

**Please contact** research@ponemon.org **or call us at 800.887.3118 if you have any questions.**

## 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 organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.