Privacy and Security in a Connected Life:
A Study of US, European and Japanese Consumers

Sponsored by Trend Micro
Independently conducted by Ponemon Institute LLC
Publication Date: March 2015
Part 1. Introduction

Privacy and Security in a Connected Life was conducted by Ponemon Institute and sponsored by Trend Micro to learn if consumers are worried about how technology that captures personal information, especially Internet of Things (IoT) or Internet of Everything (IoE), is affecting their privacy and security. In the context of this research, security refers to the safeguards in place to protect personal information from being lost or stolen. Privacy is considered to be an individual’s right to keep sensitive and confidential information from becoming known unless he or she wants the information to be revealed.

In this study of 1,903 consumers in the US, Europe and Japan, we define IoT as the expanding network of billions of connected devices that are permeating our daily lives—from smart phones and smart TVs to our WiFi enabled appliances, wireless medical devices and wearable devices. Because consumers are embracing more connected devices, information security leaders predict that IoT will be one of the most significant disruptive technologies in the near future.

In addition to issues surrounding the privacy and security of IoT, we also study respondents’ perceptions about the value of their personal information such as health information, credit history, purchasing habits, browser settings and if they should be paid for their information.

Because individuals have different opinions about the importance of privacy, we asked respondents to select a privacy profile they most closely identify with today and five years ago. Three profiles were developed by Ponemon Institute based on consumer research conducted over a period of more than 10 years. In Part 3 of this report, we compare the perceptions privacy centric and privacy complacent respondents have about IoT and the value of their personal information. The following are profiles of respondents as shown in Figure 1.

Privacy centric. These respondents will change their behaviors when they experience events that make them worry about the privacy and security of their personal information (20 percent of respondents). Five years ago, 26 percent of respondents say they were privacy centric. This decline could be attributed to individuals believing they are losing the ability to keep their personal information safe. These respondents have become more privacy sensitive.

Privacy sensitive. The majority of respondents (61 percent) are privacy sensitive. These respondents think privacy is important but will rarely change their behaviors or information sharing practices even if they experience an event that affects the privacy or security of their personal information, such as a data breach. Five years ago, 56 percent were privacy sensitive. This increase suggests that individuals are becoming less willing to change behaviors if and when they experience a privacy or security incident.
Privacy complacent. These respondents (19 percent) are the least concerned about privacy and security. These respondents really do not care even if their sensitive information is shared or sold. Respondents in this profile increased slightly.

Other key takeaways include the following:

Mobility, data breaches and social media increase concerns about privacy. Forty-seven percent of respondents say they have become more concerned about the privacy and security of their personal information in the past five years. The reasons these respondents worry about their privacy are: the increased use of mobile devices such as smartphones and tablets (63 percent), they became a victim of a data breach (61 percent) and they use social media more often (53 percent). Almost half (49 percent) are worried about how their personal information is shared, including the sharing of their medical records with third parties.

Most respondents are more concerned about security than privacy in IoT and social media. Eighty percent and 74 percent of respondents are concerned about security in IoT and social media, respectively. However, a smaller percentage of respondents are concerned about privacy in IoT (52 percent) and in social media (54 percent).

Right now respondents do not believe the benefits of IoT outweigh their privacy concerns. While 44 percent do believe the benefits of IoT outweigh their concerns about privacy or security, 42 percent say they do not and 14 percent are unsure.

Most respondents (75 percent) believe they have very little control over their personal information. We believe this is due to respondents’ uncertainty as to what information is collected and a lack of awareness about how their personal information is protected.

Little information is provided about how smart devices protect and use personal information. What can be fueling respondents’ worries about IoT is the lack of information about the security safeguards in place. When asked if manufacturers of devices provided details about how their personal information will be used, 82 percent of respondents say they did not receive any information or they are unsure. Only 18 percent of respondents recall receiving such information.

Respondents would like to receive compensation and information about the smart devices they are using. Consumers are demanding clarification about how their personal information is managed by manufacturers. They also want assurance that if their personal information is lost or stolen, the manufacturer will assume responsibility and provide compensation to help them resolve any negative consequences.

Personal information does have a value to respondents. Sixty-one percent of respondents (29 percent strongly agree + 32 percent agree) understand that their personal data is valuable because it helps companies to market and sell products. Fifty-three percent (25 percent strongly agree + 28 percent agree) believe personal data is a financial asset similar to traded goods, currencies or commodities.

Respondents would provide their personal information in exchange for money if they trust the company. Fifty-six percent of respondents say they would be willing to provide their personal data to trusted companies in exchange for money. On average, respondents would accept $76 for their passwords and $60 for information about their health condition. Social Security numbers are valued at $56.
Part 2. Key findings

In this section, we present an analysis of the key findings of this research. The complete audited findings are presented in the appendix of this report. We have organized the findings according to the following topics:

- Does privacy matter?
- A privacy problem: losing control over personal information
- Does personal information have a price?

Does privacy matter?

Use of mobile devices and data breaches has increased concerns about privacy. Forty-seven percent of respondents say they have become more concerned about the privacy and security of their personal information in the past five years.

As shown in Figure 2, reasons these respondents worry about their privacy are: the increased use of mobile devices such as smartphones and tablets (63 percent), they became a victim of a data breach (61 percent) and they use social media more often (53 percent). Almost half (49 percent) are worried about sharing their personal information, including medical records shared with third parties.

Figure 2. Why are you more concerned about your privacy?
More than one response permitted
n = 885

- I am using my mobile devices such as smartphones and tablets more often 63%
- I became a victim of a data breach 61%
- I use social media more often 53%
- More of my personal information including medical records is being shared with third parties 49%
- I have growing concerns about government surveillance 23%
- I am using location tracking devices more often 15%
- I know someone who became a victim of a data breach 13%
- I use mobile payment methods including mobile wallet 12%
- I became a victim of identity theft 7%
Experience with smart devices is limited. As shown in Figure 3, most respondents are using or planning to use smartphones/tablets and smart TVs (76 percent and 70 percent, respectively). Also revealed is that there is little use or planned use of smart security systems, Google Glass and fitness tracking wearables (84 percent, 79 percent or 71 percent, respectively).

Figure 3. What smart devices consumers use, plan to use or have no plan to use

More than one response permitted
The benefits of IoT do not outweigh concerns about privacy and security. Is the use of smart devices connected to the Internet worth potential risks to privacy and security? While 44 percent do believe the benefits of IoT outweigh their concerns about privacy or security, 42 percent say they do not and 14 percent are unsure.

Figure 4. Do you believe the benefits of IoT outweigh your concerns about privacy or security?

n = 1,903
A privacy problem: losing control of personal information

Uncertainty and the lack of control over how personal information is collected, shared, and stored could deter many consumers from using smart devices. Based on a scale of 1 to 10, Figure 5 shows that only 16 percent of respondents (10 percent + 6 percent) say they have a high degree of control over their personal information in IoT. Seventy-five percent (48 percent + 27 percent) believe they have very little control over their personal information. We believe this is due to respondents’ uncertainty as to what information is collected and a lack of awareness about how their personal information is protected.

Figure 5. How much control do you have over your personal information in IoT
1 = low control to 10 = high control
n = 1,903
Respondents are unaware of all the sensitive data collected about them. In IoT, devices are capable of collecting and sharing a wide range of personal information. In addition to tracking browsing behavior, software in devices can report on usage, location, and performance, whether through smartphone applications, video games, metadata from digital cameras, or applications running on personal computing devices. Recently it was reported that Samsung Smart TVs collect data from voice communications and even share them with a third party.¹

Figure 6 reveals that respondents believe their most sensitive information, such as purchasing habits, health conditions, Social Security numbers and credit history, is rarely collected and used by companies. In contrast, 56 percent are aware that information about their physical location (GPS) is collected because of the prevalent use of smartphones and tablets. However, many respondents (44 percent) do not seem to be aware of the tracking capabilities of their devices. When asked specifically about devices that collect information, the majority of respondents believe the devices that collect the most information are: Google Glass, smart security and smart phones or tablets.

**Figure 6. What personal information consumers believe is collected about them in IoT**

More than one response permitted

n = 1,903

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email address</td>
<td>80%</td>
</tr>
<tr>
<td>Home address</td>
<td>73%</td>
</tr>
<tr>
<td>Name</td>
<td>71%</td>
</tr>
<tr>
<td>Physical location (GPS)</td>
<td>56%</td>
</tr>
<tr>
<td>Browser settings &amp; histories</td>
<td>51%</td>
</tr>
<tr>
<td>Gender</td>
<td>51%</td>
</tr>
<tr>
<td>Payment account details</td>
<td>46%</td>
</tr>
<tr>
<td>Photos &amp; videos</td>
<td>43%</td>
</tr>
<tr>
<td>Names of friends &amp; family members</td>
<td>41%</td>
</tr>
<tr>
<td>Phone numbers</td>
<td>39%</td>
</tr>
<tr>
<td>Marital status</td>
<td>36%</td>
</tr>
<tr>
<td>Hobbies, tastes &amp; preferences</td>
<td>34%</td>
</tr>
<tr>
<td>Purchase histories</td>
<td>26%</td>
</tr>
<tr>
<td>Health condition</td>
<td>21%</td>
</tr>
<tr>
<td>School or employer</td>
<td>18%</td>
</tr>
<tr>
<td>Special dates including date of birth</td>
<td>11%</td>
</tr>
<tr>
<td>Social Security number *</td>
<td>5%</td>
</tr>
<tr>
<td>Credit history</td>
<td>4%</td>
</tr>
</tbody>
</table>

* This response was only available for US participants

¹“Smart TV eavesdropping furor prompts senator to quiz Samsung and LG on privacy”, by John Ribiero, PCWorld, February 12, 2015.
Little information is provided about how smart devices protect and use personal information. What can be fueling respondents’ worries about IoT is the lack of information about the security safeguards in place. When asked if manufacturers of devices provided details about how their personal information will be used, 82 percent of respondents say they did not receive any information or they are unsure. Only 18 percent of respondents recall receiving such information.

It is unclear whether this finding is attributable to manufacturers not providing such information or respondents are not aware that such information is available to them. In any event, respondents believe they do not have such information at hand for assurance.

If the manufacturer did provide information about how their personal information is protected, Figure 7 shows what these 18 percent of respondents remember. Forty-eight percent say they received a promise their data is shared only with trusted parties followed by the ability to opt out of data collection and/or data sharing (44 percent). Forty-five percent say they cannot recall if any of the critical information in the figure was provided to them.

**Figure 7. What protections are in place to protect your personal information?**
More than one response permitted
n = 271

<table>
<thead>
<tr>
<th>Protection Provided</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>My data is shared only with trusted parties</td>
<td>48%</td>
</tr>
<tr>
<td>I can opt out of data collection and/or data sharing</td>
<td>44%</td>
</tr>
<tr>
<td>I can turn off tracking activities anytime</td>
<td>22%</td>
</tr>
<tr>
<td>The device provides strong authentication controls</td>
<td>21%</td>
</tr>
<tr>
<td>My personal information collected is encrypted</td>
<td>16%</td>
</tr>
<tr>
<td>I can remotely disable the device if it is lost or stolen</td>
<td>16%</td>
</tr>
<tr>
<td>I can erase any information collected about me</td>
<td>15%</td>
</tr>
<tr>
<td>There is someone to contact if I have concerns about privacy</td>
<td>8%</td>
</tr>
<tr>
<td>None of the above</td>
<td>45%</td>
</tr>
</tbody>
</table>
Respondents are more concerned about their security than privacy. Figure 8 reveals respondents’ concerns about privacy and security. According to Figure 8, 80 percent of respondents are very concerned about the security of their personal data when using smart devices. Seventy-four percent are concerned about their security when using social media such as Facebook and Google.

A higher concern among respondents about the security of their personal information could be based upon the fear of becoming a victim of identity theft. While individuals can have security without privacy, they cannot have privacy without security.

In contrast, a much smaller percentage (54 percent) rates their concern about privacy when using social media as high or very high. Similarly, 52 percent rate concerns about privacy when using smart devices connected to IoT as high or very high.

This finding is consistent with the privacy profiles of respondents. As discussed previously, most respondents are privacy sensitive and think privacy is important but they are not willing to change their behavior such as stopping their use of social media because of privacy concerns.

Figure 8. How concerned are you about maintaining security and privacy in IoT and social media?
Very high and high responses
N = 1,903
Respondents would like to receive compensation and information about the smart devices they are using. Consumers are demanding clarification about how their personal information is managed by manufacturers. They also want assurance that if their personal information is lost or stolen, the manufacturer will assume responsibility and provide compensation to help them resolve any negative consequences.

As shown in Figure 9, manufacturers of smart devices should do the following: compensate consumers if their information is lost or stolen (74 percent), tell what information is collected and how the information is used (71 percent), allow consumers to control what information is collected (60 percent) and tell them what they should do if the smart device is hacked (60 percent).

**Figure 9. Manufacturers of smart devices should provide the following information**
More than one response permitted
n = 1,903

- Compensate me if my information is lost or stolen: 74%
- Tell me what information is collected: 71%
- Tell me how the information is used: 71%
- Tell me what I should do if the smart device is hacked: 60%
- Allow me to control what information is collected: 60%
- Tell me when my personal information is lost or stolen: 57%
- Assurance that my data is safeguarded: 52%
- Let me know how I can protect my information from being lost or stolen: 50%
- Don’t know: 17%
- No information is necessary: 14%
**Personal information is off limits to employers.** The majority of respondents do not believe their employer has the right to access personal data on their smart device if they use it at work or connect to their employer's Internet (52 percent) and 9 percent are unsure, according to Figure 10.

**Figure 10. Does your employer have the right to access personal data on your Smart device if you use it at work or connect to your employer’s Internet?**

n = 1,903
Respondents do not believe they are in control when sharing personal data and making purchases. Only 32 percent of respondents (see Q19 in the appendix) strongly agree or agree they still control how their personal information is collected, shared and stored after they willingly share personal data with companies.

Further, in purchasing situations that require the sharing of personal information, respondents believe they have lost control over their personal information. According to Figure 11, 70 percent of respondents say they rarely or never have control over their data after browsing websites and making online purchases and 63 percent say they rarely or never have control over their personal information when making purchases at a store.

**Figure 11. Do you have control over how your personal data is used?**
n = 1,903

- **Control over personal data after browsing websites and/or making online purchases**
  - Yes, most of the time: 13%
  - Yes, some of the time: 17%
  - Rarely: 51%
  - No: 21%

- **Control over personal data after shopping at a store and share personal information**
  - Yes, most of the time: 15%
  - Yes, some of the time: 23%
  - Rarely: 42%
  - No: 19%
Confusion exists over how personal information is used. Twenty-five percent of respondents do not know how companies use their personal information. If they do, they believe it is mainly for marketing purposes to understand their preferences as well as those of others. Forty-two percent say their data is sold for unknown purposes.

Figure 12. What do you believe companies do with your personal data?
More than one response permitted
n = 1,903

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>The data is used to understand my preferences</td>
<td>62%</td>
</tr>
<tr>
<td>The data is used to understand other consumers’ preferences</td>
<td>57%</td>
</tr>
<tr>
<td>The data is sold by those collecting it for unknown purposes</td>
<td>42%</td>
</tr>
<tr>
<td>The data is used to provide me with better security</td>
<td>38%</td>
</tr>
<tr>
<td>I do not know how companies use my personal data</td>
<td>25%</td>
</tr>
</tbody>
</table>

Respondents are mostly negative about the ads they receive based on their purchasing and browsing habits. Fifty-five percent of respondents say the ads they receive are rarely (18 percent) or never valuable to them (37 percent).

Figure 13. Do you believe ads based on your purchasing and browsing habits are helpful?

n = 1,903

<table>
<thead>
<tr>
<th>Opinion</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, most of the time</td>
<td>20%</td>
</tr>
<tr>
<td>Yes, some of the time</td>
<td>25%</td>
</tr>
<tr>
<td>Rarely</td>
<td>18%</td>
</tr>
<tr>
<td>No</td>
<td>37%</td>
</tr>
</tbody>
</table>
Does personal information have a price?

**Personal information does have a value to respondents.** According to Figure 14, 61 percent of respondents (29 percent strongly agree + 32 percent agree) understand that their personal data is valuable because it helps companies to market and sell products. Fifty-three percent (25 percent strongly agree + 28 percent agree) believe personal data is a financial asset similar to traded goods, currencies or commodities.

**Figure 14. What consumers think about the value of their personal information**

\[n = 1,903\]

![Bar Chart]

- Blue bars: Personal data helps to market and sell products to others and me
- Red bars: Personal data is a financial asset similar to traded goods, currencies or commodities
The majority of respondents do not believe loyalty programs provide adequate compensation. As mentioned previously, 82 percent of respondents do not know or are unsure about how manufacturers of smart devices use and protect their personal information. However, when it comes to loyalty cards, more respondents (56 percent) do have full or some understanding what companies do with their data. This is probably due to the various benefits and compensation loyalty cards provide.

Sixty-seven percent of respondents participate in a loyalty program. According to Figure 15, 64 percent of respondents say they mainly receive discounts on future purchases or early access to sales or discounts or hard to get products or services (48 percent). Sixty-one percent say this compensation is not enough (40 percent) or they are unsure (21 percent).

**Figure 15. How are you compensated for your participation in loyalty programs?**
More than one response permitted
n = 1,285

<table>
<thead>
<tr>
<th>Compensation</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discounts on future purchases</td>
<td>64%</td>
</tr>
<tr>
<td>Early access to sales or discounts or hard to get products or services (i.e. tickets to a playoff game)</td>
<td>48%</td>
</tr>
<tr>
<td>Free and upgraded flights</td>
<td>29%</td>
</tr>
<tr>
<td>Cash back or reimbursements</td>
<td>28%</td>
</tr>
<tr>
<td>Concierge services</td>
<td>13%</td>
</tr>
<tr>
<td>Free goods and services</td>
<td>13%</td>
</tr>
</tbody>
</table>
Respondents would provide their personal information in exchange for money if they trust the company. Fifty-six percent of respondents say they would be willing to provide their personal data to trusted companies in exchange for money, as shown in Figure 16.

Figure 16. Would you be willing to provide your personal data to trusted companies in exchange for money?

n = 1,903

<table>
<thead>
<tr>
<th>Response</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>56%</td>
</tr>
<tr>
<td>No, I would not provide my personal data for any amount of money</td>
<td>36%</td>
</tr>
<tr>
<td>Unsure</td>
<td>7%</td>
</tr>
</tbody>
</table>
How much is one piece of data worth? We asked respondents who would be willing to share their personal information in exchange for money to indicate what would be the minimum amount they would accept as compensation in exchange for different data categories. On average, respondents believe one piece of data is worth $19.60. The most expensive pieces of data are: passwords (log in credentials) $75.80, health condition $59.80, payment details $36, credit history $29.20 and purchase habits $20.60. The cheapest pieces of data are: gender $2.90, name $3.90 and phone numbers $5.90.

Figure 17. How much is your personal data worth?
Extrapolated average value = $19.60
n = 1,078

* This response was only available for US participants
Part 3. U.S., Japan and Europe Comparisons

In this section, we present an analysis of findings from each country and region. As shown, although there are similarities among US, Japan and Europe, there are some differences that may be attributable to cultural differences and regional trends.

Are respondents more worried about their privacy? The majority of respondents in all regions have not become more concerned about their privacy in the past five years despite mega breaches, increased surveillance and smart devices tracking behaviors and locations. Forty-five percent of US respondents, 46 percent of Japanese respondents and 49 percent of European respondents say they have become more concerned about their privacy in the past five years.

Figure 18 reveals the basis of these respondents' concerns. In general, they say data breaches, the sharing of medical records, increased use of mobile devices and social devices have made them more concerned about their privacy.

Figure 18. Why are you more concerned about your privacy?
More than one response permitted
n = 885

- More of my personal information including medical records is being shared with third parties
  - US (335) 59% 40%
  - JP (274) 49% 49%
  - EU (276) 69% 49%

- I became a victim of a data breach
  - US (335) 73% 55%
  - JP (274) 56%
  - EU (276) 66%

- I am using my mobile devices such as smartphones and tablets more often
  - US (335) 66% 53%
  - JP (274) 69% 66%
  - EU (276) 69% 69%

- I use social media more often
  - US (335) 63% 46%
  - JP (274) 50%
  - EU (276) 63%

- I have growing concerns about government surveillance
  - US (335) 19% 11%
  - JP (274) 39% 11%
  - EU (276) 39% 11%

- I know someone who became a victim of a data breach
  - US (335) 16% 6%
  - JP (274) 18%
  - EU (276) 11%

- I am using location tracking devices more often
  - US (335) 15% 9%
  - JP (274) 21%
  - EU (276) 21%

- I use mobile payment methods including mobile wallet
  - US (335) 14% 13%
  - JP (274) 9%
  - EU (276) 9%

- I became a victim of identity theft
  - US (335) 6%
  - JP (274) 6%
  - EU (276) 5%
In the US, more respondents (73 percent) are concerned about their privacy because of a data breach that resulted in the loss or theft of personal information. This might be due to the frequency of well-publicized data breaches in the US. Japanese and European respondents worry that the use of their mobile devices are putting their privacy in jeopardy (69 percent and 66 percent, respectively). It is also interesting to note that European respondents are the most concerned about government surveillance.

**Respondents are concerned about their privacy and security.** Figure 19 reveals respondents’ concerns about privacy and security in IoT and social media. According to Figure 19, Europeans are much more concerned about their privacy than the US and Japanese respondents.

In contrast, the majority of all respondents worry about the security of their personal information when using devices connected to the Internet or when using social media. Europeans are more concerned about security than US and Japan when using social media.

**Figure 19. Concerns about security and privacy in IoT and when using social media**

On a scale of 1 = low concern to 10 = high concern respondents who rated their concern 7+

![Chart showing concerns about security and privacy in IoT and social media](chart.png)

<table>
<thead>
<tr>
<th>Samples</th>
<th>Concerns about security in the IoT</th>
<th>Concerns about security when using social media</th>
<th>Concerns about privacy in the IoT</th>
<th>Concerns about privacy when using social media</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.</td>
<td>558</td>
<td>506</td>
<td>327</td>
<td>342</td>
</tr>
<tr>
<td>Japan</td>
<td>494</td>
<td>422</td>
<td>292</td>
<td>298</td>
</tr>
<tr>
<td>Europe</td>
<td>462</td>
<td>457</td>
<td>350</td>
<td>383</td>
</tr>
</tbody>
</table>
Little information is provided about how smart devices protect and use personal information. Respondents' worries about IoT can be exacerbated by the lack of information provided by manufacturers about the security safeguards in place. When asked if manufacturers of devices provided details about how their personal information will be used, respondents say they did not receive any information or they are unsure (81 percent in US, 82 percent in Japan and 82 percent in Europe).

If the manufacturer did provide information about how their personal information is protected, Figure 20 shows what respondents remember. Japan and European respondents remember the promise that their data is shared only with trusted parties (50 percent of respondents). Whereas, US respondents remember the commitment they can opt out of data collection and/or data sharing. Many respondents in all regions say they haven’t received any of the information listed.

**Figure 20. What protections are in place to protect your personal information?**
More than one response permitted
n = 271

<table>
<thead>
<tr>
<th>Protection Provided</th>
<th>US (97)</th>
<th>JP (90)</th>
<th>EU (84)</th>
</tr>
</thead>
<tbody>
<tr>
<td>My data is shared only with trusted parties</td>
<td>44%</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>I can opt out of data collection and/or data sharing</td>
<td>38%</td>
<td>49%</td>
<td>44%</td>
</tr>
<tr>
<td>I can turn off tracking activities anytime</td>
<td>23%</td>
<td>24%</td>
<td>18%</td>
</tr>
<tr>
<td>The device provides strong authentication controls</td>
<td>19%</td>
<td>19%</td>
<td>23%</td>
</tr>
<tr>
<td>My personal information collected is encrypted</td>
<td>12%</td>
<td>16%</td>
<td>16%</td>
</tr>
<tr>
<td>I can remotely disable the device if it is lost or stolen</td>
<td>13%</td>
<td>15%</td>
<td>19%</td>
</tr>
<tr>
<td>I can erase any information collected about me</td>
<td>16%</td>
<td>16%</td>
<td>16%</td>
</tr>
<tr>
<td>There is someone to contact if I have concerns about privacy</td>
<td>9%</td>
<td>5%</td>
<td>10%</td>
</tr>
<tr>
<td>None of the above</td>
<td>40%</td>
<td>49%</td>
<td>46%</td>
</tr>
</tbody>
</table>
Europeans are more likely to agree they have control over personal data willingly shared. As shown in Figure 21, 43 percent of respondents in Europe believe even if they share their personal data with companies they have control over it. Only 22 percent of US respondents believe they have control. A possible reason is that EU laws and regulations may provide European respondents with confidence they have this control.

Figure 21. Even if I willingly share my personal data with companies, I still control how they collect, share and store my personal data
Strongly agree and agree response combined

Pay for personal data is popular around the globe. The majority of respondents would share personal information in exchange for money. However, more European respondents would not exchange personal information for any amount of money.

Figure 22. Would you be willing to provide your personal data to trusted companies in exchange for money?

Pay for personal data is popular around the globe. The majority of respondents would share personal information in exchange for money. However, more European respondents would not exchange personal information for any amount of money.
How much is one piece of data worth? We asked respondents to indicate what would be the minimum amount they would accept as compensation in exchange for different data categories. Figure 23 shows interesting differences among US, Japanese and European respondents for seven data categories. US respondents put a much higher price on information about their health condition. Japanese and European respondents would want more money for their passwords or login details.

Also interesting is the value US respondents placed on GPS location compared to their Japanese and European peers. This may be due to concerns over security or possibly because many retailers are using this to drive marketing or location services.

Figure 23. How much is your personal data worth?

n = 1,078

<table>
<thead>
<tr>
<th>Data Category</th>
<th>US ($61.6)</th>
<th>JP ($35.0)</th>
<th>EU ($82.0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health condition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passwords (login details)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Security number *</td>
<td>$55.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment details (credit card)</td>
<td>$45.1</td>
<td>$20.8</td>
<td>$42.2</td>
</tr>
<tr>
<td>Credit history</td>
<td>$40.1</td>
<td>$26.7</td>
<td>$38.4</td>
</tr>
<tr>
<td>Physical location (GPS)</td>
<td>$38.4</td>
<td>$4.8</td>
<td>$5.1</td>
</tr>
<tr>
<td>Names of friends &amp; family members</td>
<td>$27.4</td>
<td>$24.2</td>
<td>$18.8</td>
</tr>
</tbody>
</table>

* This response was only available for US participants
Part 4. Analysis of privacy centric and privacy complacent respondents

In this section, we analyze respondents according to their self-reported privacy preference. Our analysis compares respondents who are privacy centric (n = 387) versus those who are privacy complacent (n = 355). The middle category termed privacy sensitive is removed to highlight maximum differences.

In general, privacy centric respondents are most concerned about the privacy and security of their personal information. However, they are also the most aware about the privacy practices of manufacturers and are more confident they have control over their personal information. In contrast, privacy complacent respondents seem to be indifferent to what might happen to their privacy and security. They also are less likely to believe they have control over how their personal information is collected, shared and stored.

Events in the past five years have increased the concerns privacy centric respondents have about their privacy. As shown in Figure 24, there is a difference in the concerns expressed by privacy centric and privacy complacent respondents (e.g. a 10 percent difference between centric and complacent subsamples).

Figure 24. Have you become more concerned about privacy and security of your personal data over the past 5 years?

<table>
<thead>
<tr>
<th>Choices</th>
<th>Centric</th>
<th>Complacent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>205</td>
<td>153</td>
</tr>
<tr>
<td>No</td>
<td>182</td>
<td>202</td>
</tr>
<tr>
<td>Total</td>
<td>387</td>
<td>355</td>
</tr>
</tbody>
</table>
Privacy centric respondents have a heightened level of concern over all factors that affect the privacy and security of their personal data. The number one concern for both centric and complacent respondents is the fact they were involved in a data breach followed by the increase use of mobile devices, as shown in Figure 25. This finding reveals that data breaches and new technologies have more impact on privacy centric respondents.

**Figure 25. If you became more concerned, what are the main reasons?**

More than one response permitted

<table>
<thead>
<tr>
<th>Choices</th>
<th>Centric (n = 205)</th>
<th>Complacent (n = 153)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I became a victim of a data breach</td>
<td>139</td>
<td>77</td>
</tr>
<tr>
<td>I am using my mobile devices such as smartphones and tablets more often</td>
<td>127</td>
<td>92</td>
</tr>
<tr>
<td>More of my personal information including medical records is being shared with third parties</td>
<td>113</td>
<td>73</td>
</tr>
<tr>
<td>I use social media more often</td>
<td>107</td>
<td>69</td>
</tr>
<tr>
<td>I have growing concerns about government surveillance</td>
<td>68</td>
<td>31</td>
</tr>
<tr>
<td>I know someone who became a victim of a data breach</td>
<td>13</td>
<td>11</td>
</tr>
<tr>
<td>I became a victim of identity theft</td>
<td>3</td>
<td>10</td>
</tr>
</tbody>
</table>

Table 4: Frequency of responses to items summarized in Figure 25
Complacent respondents are more likely to use IoT devices such as Google Glass, smart kitchen appliances, smart TV and smartphones. As shown in Figure 26, centric and complacent respondents agree on fitness wearables, smart meters and smart thermostats.

**Figure 26. Respondents who say they have no plan to use the presented smart device**
More than one response permitted

<table>
<thead>
<tr>
<th>Choices</th>
<th>Centric</th>
<th>Complacent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smartphone/Tablet</td>
<td>77</td>
<td>35</td>
</tr>
<tr>
<td>Smart TV</td>
<td>80</td>
<td>44</td>
</tr>
<tr>
<td>Smart electric meter</td>
<td>148</td>
<td>102</td>
</tr>
<tr>
<td>Smart kitchen appliances</td>
<td>172</td>
<td>93</td>
</tr>
<tr>
<td>Smart home thermostat</td>
<td>183</td>
<td>125</td>
</tr>
<tr>
<td>Fitness status tracking wearable</td>
<td>209</td>
<td>154</td>
</tr>
<tr>
<td>Smart security systems</td>
<td>220</td>
<td>152</td>
</tr>
<tr>
<td>Google Glass</td>
<td>246</td>
<td>133</td>
</tr>
</tbody>
</table>

Table 4: Frequency of responses to items summarized in Figure 26
Privacy centric respondents are more aware of the communications from companies about privacy of personal information. However, as shown in Figure 27, it is still a small percentage of respondents in both classifications who are aware of information about how their personal data will be used. However, it is likely that privacy complacent respondents do not look for such information from manufacturers.

Figure 27. Did any of the manufacturers of the devices you use (or plan to use) provide you with information about how your personal information will be used?

Table 5: Frequency of responses to items summarized in Figure 27

<table>
<thead>
<tr>
<th>Choices</th>
<th>Centric</th>
<th>Complacent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>101</td>
<td>47</td>
</tr>
<tr>
<td>No</td>
<td>148</td>
<td>177</td>
</tr>
<tr>
<td>Unsure</td>
<td>66</td>
<td>71</td>
</tr>
</tbody>
</table>
Privacy centric respondents are much more concerned about maintaining their privacy in IoT. As shown in Figure 28, 45 percent of privacy centric respondents rate their concern about IoT privacy as very high. The implication is that manufacturers of IoT devices should understand the concerns of these potential consumers of their products.

Figure 28. How concerned are you about maintaining your privacy in IoT?
10-point scale from 1 = low to 10 = high

Table 5: Frequency of responses to items summarized in Figure 28

<table>
<thead>
<tr>
<th>Choices</th>
<th>Centric</th>
<th>Complacent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2 (low)</td>
<td></td>
<td>57</td>
</tr>
<tr>
<td>3 or 4</td>
<td>15</td>
<td>75</td>
</tr>
<tr>
<td>5 or 6</td>
<td>70</td>
<td>128</td>
</tr>
<tr>
<td>7 or 8</td>
<td>128</td>
<td>43</td>
</tr>
<tr>
<td>9 or 10 (high)</td>
<td>174</td>
<td>53</td>
</tr>
<tr>
<td>Total</td>
<td>387</td>
<td>355</td>
</tr>
</tbody>
</table>
Privacy centric respondents are also much more concerned about maintaining their security in IoT. Again, manufacturers should be attuned to the concerns of the privacy centric respondents, according to Figure 29. As discussed previously, privacy complacent respondents are not concerned about how their information is collected, used and shared by manufacturers.

Figure 29. How concerned are you about your security in IoT?
10-point scale from 1 = low to 10 = high

![Graph showing security concerns]

Table 6: Frequency of responses to items summarized in Figure 29

<table>
<thead>
<tr>
<th>Choices</th>
<th>Centric</th>
<th>Complacent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2 (low)</td>
<td></td>
<td>43</td>
</tr>
<tr>
<td>3 or 4</td>
<td>8</td>
<td>67</td>
</tr>
<tr>
<td>5 or 6</td>
<td>31</td>
<td>121</td>
</tr>
<tr>
<td>7 or 8</td>
<td>124</td>
<td>53</td>
</tr>
<tr>
<td>9 or 10 (high)</td>
<td>224</td>
<td>71</td>
</tr>
<tr>
<td>Total</td>
<td>387</td>
<td>355</td>
</tr>
</tbody>
</table>
Despite being concerned about their privacy, privacy centric respondents are more convinced than privacy complacent respondents that the benefits of IoT outweigh their worries. A possible explanation is that privacy centric respondents believe they are more aware of the privacy issues and understand how they can best protect their personal information. As shown in Figure 30, 60 percent of privacy centric respondents vs. 40 percent of privacy complacent respondents say the benefits of IoT outweigh concerns.

Figure 30. Do you believe the benefits of IoT outweigh your concerns about privacy or security?

Table 7: Frequency of responses to items summarized in Figure 30

<table>
<thead>
<tr>
<th>Choices</th>
<th>Centric</th>
<th>Complacent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>232</td>
<td>142</td>
</tr>
<tr>
<td>No</td>
<td>132</td>
<td>138</td>
</tr>
<tr>
<td>Unsure</td>
<td>23</td>
<td>75</td>
</tr>
<tr>
<td>Total</td>
<td>387</td>
<td>355</td>
</tr>
</tbody>
</table>
Privacy centric respondents are more likely to believe they are in control when sharing their personal information with companies. According to Figure 31, 54 percent of privacy centric respondents are confident they can control how their personal information is used when willingly sharing it with companies. These respondents are also more likely to think of their personal data as a financial asset.

**Figure 31. Attributions about personal information**

Strongly agree and agree response combine

![Graph showing attributions about personal information](image)

<table>
<thead>
<tr>
<th>Choices</th>
<th>Centric</th>
<th>Complacent</th>
</tr>
</thead>
<tbody>
<tr>
<td>My personal data is a financial asset similar to traded goods, currencies or commodities.</td>
<td>271</td>
<td>167</td>
</tr>
<tr>
<td>Even if I willingly share my personal data with companies, I still control how they collect, share and store my personal data.</td>
<td>209</td>
<td>89</td>
</tr>
</tbody>
</table>
Privacy centric respondents also believe they have more control over their personal information when browsing websites and making purchases. As shown in Figure 32, 49 percent of privacy centric respondents are confident that most or some of the time they have control over how their personal data is used by online companies. In contrast, only 22 percent of privacy complacent respondents say they have control. One possible explanation is that privacy complacent respondents admit to not caring about how their personal information is used and believe they have relinquished control.

Figure 32. After browsing websites and/or making online purchases, do you believe you have control over how your personal data is used?

![Bar chart showing control over personal data usage]

Table 9: Frequency of responses to items summarized in Figure 32

<table>
<thead>
<tr>
<th>Choices</th>
<th>Centric</th>
<th>Complacent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, most of the time</td>
<td>81</td>
<td>32</td>
</tr>
<tr>
<td>Yes, some of the time</td>
<td>108</td>
<td>46</td>
</tr>
<tr>
<td>Rarely</td>
<td>151</td>
<td>199</td>
</tr>
<tr>
<td>No</td>
<td>46</td>
<td>78</td>
</tr>
<tr>
<td>Total</td>
<td>387</td>
<td>355</td>
</tr>
</tbody>
</table>
Privacy centric respondents care more about the privacy of their personal information than exchanging it for money. According to Figure 33, 65 percent of privacy centric respondents would not give their personal information away for any amount of money.

**Figure 33. Would you be willing to provide your personal data to trusted companies in exchange for money?**

![Bar chart showing responses to Figure 33](image)

<table>
<thead>
<tr>
<th>Choices</th>
<th>Centric</th>
<th>Complacent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>89</td>
<td>238</td>
</tr>
<tr>
<td>No, I would not provide my personal data for any amount of money</td>
<td>252</td>
<td>82</td>
</tr>
<tr>
<td>Unsure</td>
<td>46</td>
<td>36</td>
</tr>
<tr>
<td>Total</td>
<td>387</td>
<td>355</td>
</tr>
</tbody>
</table>
Privacy centric respondents put a higher price on their personal information. On average, privacy complacent respondents would provide sensitive and personal information to organizations at a very low price, as revealed in Figure 34.

Figure 34. How much would a trusted company have to pay you to obtain the following data about you?
Average for 19 personal data categories
Conclusion

The objective of the study is to understand what consumers throughout the world think about the quickly emerging IoT. With many IoT devices flooding the marketplace and becoming part of our everyday life, how can consumers truly understand the impact on their privacy and security? As evidence, respondents are not often informed and aware about what personal information is collected, used, shared and how it is protected.

While security of personal information in IoT and social media is shown in this research as being most important, privacy still matters. Eighty-one percent of respondents are either privacy centric or sensitive and the lack of control over personal information is a major worry. Another concern is the lack of knowledge about what information is collected about them. Therefore, it makes sense that so many respondents do not plan to use many of the IoT devices featured in this research.

These findings reveal the following opportunities and responsibilities for companies operating in the IoT space:

- Create communications and outreach programs to inform consumers about what personal data is collected, how it is shared, how to get additional information about the privacy and security of their information and how they can opt out of any data collection or sharing.

- Provide consumers with assurance they have control over their information and it is secure. Explain how they can disable tracking features, erase information collected and remotely disable the device if it is lost or stolen. Describe security features such as encryption of personal information and the authentication controls in place.

- Educate and train employees about the importance of safeguarding consumers’ information. Create and enforce privacy and security policies.

- Consider the creation of industry standards on achieving privacy and security in IoT.

The IoT can provide many benefits. However, for IoT to succeed consumers must have confidence and trust that companies will respect their privacy and security concerns.
Part 5. Methods

A sampling frame composed of 55,687 consumers located in the United States, Japan and Europe were selected for participation in this survey. As shown in the Table 3, 2,033 respondents completed the survey. Screening removed 130 surveys. The final sample was 1,903 surveys (or a 3.4 percent response rate). All survey responses were captured November 11 through December 8.

<table>
<thead>
<tr>
<th>Table 3. Sample response</th>
<th>US</th>
<th>JP</th>
<th>EU</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total sampling frame</td>
<td>24,008</td>
<td>15,649</td>
<td>16,030</td>
<td>55,687</td>
</tr>
<tr>
<td>Total returns</td>
<td>815</td>
<td>618</td>
<td>600</td>
<td>2,033</td>
</tr>
<tr>
<td>Rejected or screened surveys</td>
<td>71</td>
<td>23</td>
<td>36</td>
<td>130</td>
</tr>
<tr>
<td>Final sample</td>
<td>744</td>
<td>595</td>
<td>564</td>
<td>1,903</td>
</tr>
<tr>
<td>Response Rate</td>
<td>3.1%</td>
<td>3.8%</td>
<td>3.5%</td>
<td>3.4%</td>
</tr>
</tbody>
</table>

Pie Chart 1 reports the highest level of education of respondents. More than half of respondents (58 percent) reported having attended college or earning a college degree.

Pie Chart 1. Highest level of education
n = 1,903
According to Pie Chart 2, more than half of the respondents (59 percent) reported their income to be less than $60,000. Forty-one percent reported their income to be greater than $60,000. The average respondent's income was $69,067.

**Pie Chart 2. Household income**
Expressed in US $, n = 1,903

Pie Chart 3 reports the age of respondents. More than half of the respondents (64 percent) are between the ages of 18 and 45.

**Pie Chart 3. Age of respondents**
n = 1,903
As shown in Pie Chart 4, there are 15 countries represented in the European cluster. The largest country segments are: United Kingdom (21 percent), Germany (17 percent) and France (14 percent).

Pie Chart 4. Countries represented in the European cluster sample
n = 564
Part 6. 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 individuals who are consumers. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period.

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 a subject did not provide a truthful response.
Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured November 11 through December 8.

<table>
<thead>
<tr>
<th>Consolidated global consumer survey response</th>
<th>Freq</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total sampling frame</td>
<td>55,687</td>
<td>100.0%</td>
</tr>
<tr>
<td>Total returns</td>
<td>2,033</td>
<td>3.7%</td>
</tr>
<tr>
<td>Rejected or screened surveys</td>
<td>130</td>
<td>0.2%</td>
</tr>
<tr>
<td>Final sample</td>
<td>1,903</td>
<td>3.4%</td>
</tr>
</tbody>
</table>

Part 1. Privacy profile and the Internet of Things

Q1. Based on the descriptions above, what is your privacy profile today?

<table>
<thead>
<tr>
<th>Privacy profile</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy complacent</td>
<td>19%</td>
</tr>
<tr>
<td>Privacy sensitive</td>
<td>61%</td>
</tr>
<tr>
<td>Privacy centric</td>
<td>20%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q2. Based on the descriptions above, what was your privacy profile five years ago?

<table>
<thead>
<tr>
<th>Privacy profile</th>
<th>Pct%²</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy complacent</td>
<td>17%</td>
</tr>
<tr>
<td>Privacy sensitive</td>
<td>56%</td>
</tr>
<tr>
<td>Privacy centric</td>
<td>26%</td>
</tr>
<tr>
<td>Total</td>
<td>99%</td>
</tr>
</tbody>
</table>

Q3a. Have you become more concerned about privacy and security of your personal data over the past 5 years?

<table>
<thead>
<tr>
<th>Concerned</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>47%</td>
</tr>
<tr>
<td>No</td>
<td>53%</td>
</tr>
</tbody>
</table>

² The total percentage does not sum to 100 percent because of a rounding error.
Q3b. If you became more concerned about the privacy and security of your personal data over the past five years, why? Please select all the reasons why you have become more concerned.

<table>
<thead>
<tr>
<th>Reason</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>I became a victim of a data breach</td>
<td>61%</td>
</tr>
<tr>
<td>I became a victim of identity theft</td>
<td>7%</td>
</tr>
<tr>
<td>I have growing concerns about government surveillance</td>
<td>23%</td>
</tr>
<tr>
<td>I use social media more often</td>
<td>53%</td>
</tr>
<tr>
<td>I am using location tracking devices more often</td>
<td>15%</td>
</tr>
<tr>
<td>I know someone who became a victim of a data breach</td>
<td>13%</td>
</tr>
<tr>
<td>I am using my mobile devices such as smartphones and tablets more often</td>
<td>63%</td>
</tr>
<tr>
<td>I use mobile payment methods including mobile wallet</td>
<td>12%</td>
</tr>
<tr>
<td>More of my personal information including medical records is being shared with third parties</td>
<td>49%</td>
</tr>
<tr>
<td>Total</td>
<td>297%</td>
</tr>
</tbody>
</table>

Q4. Please rate your level of knowledge or familiarity about each device presented using the following scale: 1 = Very familiar, 2 = Familiar, 3 = Somewhat familiar and 4 = Not familiar

<table>
<thead>
<tr>
<th>Device</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fitness status tracking wearable</td>
<td>9%</td>
<td>12%</td>
<td>34%</td>
<td>45%</td>
<td>100%</td>
</tr>
<tr>
<td>Google Glass</td>
<td>11%</td>
<td>15%</td>
<td>21%</td>
<td>54%</td>
<td>100%</td>
</tr>
<tr>
<td>Smart home thermostat</td>
<td>13%</td>
<td>14%</td>
<td>24%</td>
<td>49%</td>
<td>100%</td>
</tr>
<tr>
<td>Smart TV</td>
<td>40%</td>
<td>27%</td>
<td>27%</td>
<td>7%</td>
<td>100%</td>
</tr>
<tr>
<td>Smart kitchen appliances</td>
<td>24%</td>
<td>21%</td>
<td>16%</td>
<td>40%</td>
<td>100%</td>
</tr>
<tr>
<td>Smart security systems</td>
<td>10%</td>
<td>8%</td>
<td>22%</td>
<td>61%</td>
<td>100%</td>
</tr>
<tr>
<td>Smart electric meter</td>
<td>21%</td>
<td>20%</td>
<td>24%</td>
<td>35%</td>
<td>100%</td>
</tr>
<tr>
<td>Smartphone/Tablet</td>
<td>44%</td>
<td>23%</td>
<td>26%</td>
<td>7%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q5. [If not familiar skip to Q8] Do you currently use or plan to use this smart device?

<table>
<thead>
<tr>
<th>Device</th>
<th>Use</th>
<th>Plan to use</th>
<th>No plan to use</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fitness status tracking wearable</td>
<td>8%</td>
<td>21%</td>
<td>71%</td>
<td>100%</td>
</tr>
<tr>
<td>Google Glass</td>
<td>6%</td>
<td>16%</td>
<td>79%</td>
<td>100%</td>
</tr>
<tr>
<td>Smart home thermostat</td>
<td>9%</td>
<td>21%</td>
<td>70%</td>
<td>100%</td>
</tr>
<tr>
<td>Smart TV</td>
<td>30%</td>
<td>40%</td>
<td>30%</td>
<td>100%</td>
</tr>
<tr>
<td>Smart kitchen appliances</td>
<td>19%</td>
<td>25%</td>
<td>57%</td>
<td>100%</td>
</tr>
<tr>
<td>Smart security systems</td>
<td>5%</td>
<td>11%</td>
<td>84%</td>
<td>100%</td>
</tr>
<tr>
<td>Smart electric meter</td>
<td>17%</td>
<td>29%</td>
<td>55%</td>
<td>100%</td>
</tr>
<tr>
<td>Smartphone/Tablet</td>
<td>43%</td>
<td>33%</td>
<td>24%</td>
<td>100%</td>
</tr>
</tbody>
</table>
Q6. What personal information do you believe is collected by the devices listed above? Check your answers in each cell of the following matrix for these smart devices

<table>
<thead>
<tr>
<th></th>
<th>Fitness tracking</th>
<th>Google Glass</th>
<th>Smart thermostat</th>
<th>Smart TV</th>
<th>Smart kitchen</th>
<th>Smart security</th>
<th>Smart meter</th>
<th>Smart phone or tablet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser settings &amp; histories</td>
<td>47%</td>
<td>96%</td>
<td>24%</td>
<td>90%</td>
<td>20%</td>
<td>29%</td>
<td>14%</td>
<td>86%</td>
</tr>
<tr>
<td>Credit history</td>
<td>0%</td>
<td>5%</td>
<td>2%</td>
<td>1%</td>
<td>3%</td>
<td>8%</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>Email address</td>
<td>86%</td>
<td>79%</td>
<td>57%</td>
<td>93%</td>
<td>81%</td>
<td>80%</td>
<td>77%</td>
<td>85%</td>
</tr>
<tr>
<td>Health condition</td>
<td>76%</td>
<td>12%</td>
<td>6%</td>
<td>6%</td>
<td>19%</td>
<td>20%</td>
<td>13%</td>
<td>15%</td>
</tr>
<tr>
<td>Hobbies, tastes &amp; preferences</td>
<td>33%</td>
<td>69%</td>
<td>11%</td>
<td>50%</td>
<td>36%</td>
<td>22%</td>
<td>6%</td>
<td>42%</td>
</tr>
<tr>
<td>Home address</td>
<td>46%</td>
<td>70%</td>
<td>84%</td>
<td>55%</td>
<td>80%</td>
<td>79%</td>
<td>82%</td>
<td>90%</td>
</tr>
<tr>
<td>Marital status</td>
<td>37%</td>
<td>78%</td>
<td>4%</td>
<td>22%</td>
<td>38%</td>
<td>51%</td>
<td>24%</td>
<td>31%</td>
</tr>
<tr>
<td>Name</td>
<td>83%</td>
<td>85%</td>
<td>78%</td>
<td>68%</td>
<td>53%</td>
<td>77%</td>
<td>62%</td>
<td>59%</td>
</tr>
<tr>
<td>Names of friends &amp; family members</td>
<td>26%</td>
<td>51%</td>
<td>12%</td>
<td>62%</td>
<td>45%</td>
<td>58%</td>
<td>13%</td>
<td>62%</td>
</tr>
<tr>
<td>Payment account details</td>
<td>29%</td>
<td>54%</td>
<td>34%</td>
<td>61%</td>
<td>21%</td>
<td>47%</td>
<td>58%</td>
<td>63%</td>
</tr>
<tr>
<td>Phone numbers</td>
<td>16%</td>
<td>28%</td>
<td>21%</td>
<td>26%</td>
<td>15%</td>
<td>90%</td>
<td>20%</td>
<td>92%</td>
</tr>
<tr>
<td>Photos &amp; videos</td>
<td>64%</td>
<td>54%</td>
<td>8%</td>
<td>36%</td>
<td>8%</td>
<td>88%</td>
<td>4%</td>
<td>85%</td>
</tr>
<tr>
<td>Physical location (GPS)</td>
<td>45%</td>
<td>82%</td>
<td>16%</td>
<td>14%</td>
<td>36%</td>
<td>87%</td>
<td>88%</td>
<td>76%</td>
</tr>
<tr>
<td>Purchase histories</td>
<td>1%</td>
<td>69%</td>
<td>1%</td>
<td>45%</td>
<td>39%</td>
<td>12%</td>
<td>1%</td>
<td>41%</td>
</tr>
<tr>
<td>Social Security number</td>
<td>0%</td>
<td>6%</td>
<td>2%</td>
<td>3%</td>
<td>0%</td>
<td>26%</td>
<td>0%</td>
<td>6%</td>
</tr>
<tr>
<td>Special dates including date of birth</td>
<td>6%</td>
<td>13%</td>
<td>2%</td>
<td>9%</td>
<td>30%</td>
<td>20%</td>
<td>2%</td>
<td>3%</td>
</tr>
<tr>
<td>Gender</td>
<td>84%</td>
<td>90%</td>
<td>25%</td>
<td>46%</td>
<td>36%</td>
<td>82%</td>
<td>5%</td>
<td>38%</td>
</tr>
<tr>
<td>School or employer</td>
<td>2%</td>
<td>42%</td>
<td>2%</td>
<td>4%</td>
<td>7%</td>
<td>40%</td>
<td>5%</td>
<td>41%</td>
</tr>
<tr>
<td>Average</td>
<td>38%</td>
<td>55%</td>
<td>22%</td>
<td>38%</td>
<td>31%</td>
<td>51%</td>
<td>26%</td>
<td>51%</td>
</tr>
</tbody>
</table>

Q7a. [Only those who use or plan to use] Did any of the manufacturers of the devices you use (or plan to use) provide you with information about how your personal information is protected?

<table>
<thead>
<tr>
<th></th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>18%</td>
</tr>
<tr>
<td>No</td>
<td>60%</td>
</tr>
<tr>
<td>Unsure</td>
<td>22%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
Q7b. If yes, what protections are in place to protect your personal information?  

<table>
<thead>
<tr>
<th>Protection</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>My data is shared only with trusted parties</td>
<td>48%</td>
</tr>
<tr>
<td>I can turn off tracking activities anytime</td>
<td>22%</td>
</tr>
<tr>
<td>The device provides strong authentication controls</td>
<td>21%</td>
</tr>
<tr>
<td>I can remotely disable the device if it is lost or stolen</td>
<td>16%</td>
</tr>
<tr>
<td>I can erase any information collected about me</td>
<td>15%</td>
</tr>
<tr>
<td>I can opt out of data collection and/or data sharing</td>
<td>44%</td>
</tr>
<tr>
<td>My personal information collected is encrypted</td>
<td>16%</td>
</tr>
<tr>
<td>There is someone to contact if I have concerns about privacy</td>
<td>8%</td>
</tr>
<tr>
<td>None of the above</td>
<td>45%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>234%</td>
</tr>
</tbody>
</table>

Q8. Did any of the manufacturers of the devices you use (or plan to use) provide you with information about how your personal information will be used?  

<table>
<thead>
<tr>
<th>Response</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>18%</td>
</tr>
<tr>
<td>No</td>
<td>58%</td>
</tr>
<tr>
<td>Unsure</td>
<td>24%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
</tbody>
</table>

Q9. How concerned are you about maintaining your privacy in the IoT?  

<table>
<thead>
<tr>
<th>Concern Level</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2 (low)</td>
<td>7%</td>
</tr>
<tr>
<td>3 or 4</td>
<td>10%</td>
</tr>
<tr>
<td>5 or 6</td>
<td>31%</td>
</tr>
<tr>
<td>7 or 8</td>
<td>23%</td>
</tr>
<tr>
<td>9 or 10 (high)</td>
<td>29%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
</tbody>
</table>

Q10. How concerned are you about your security in the IoT?  

<table>
<thead>
<tr>
<th>Concern Level</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2 (low)</td>
<td>3%</td>
</tr>
<tr>
<td>3 or 4</td>
<td>4%</td>
</tr>
<tr>
<td>5 or 6</td>
<td>13%</td>
</tr>
<tr>
<td>7 or 8</td>
<td>24%</td>
</tr>
<tr>
<td>9 or 10 (high)</td>
<td>56%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
<tr>
<td>Q11. How concerned are you about the security of your personal data when using social media (such as Facebook and Google)?</td>
<td>Pct%</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>1 or 2 (low)</td>
<td>7%</td>
</tr>
<tr>
<td>3 or 4</td>
<td>7%</td>
</tr>
<tr>
<td>5 or 6</td>
<td>13%</td>
</tr>
<tr>
<td>7 or 8</td>
<td>30%</td>
</tr>
<tr>
<td>9 or 10 (high)</td>
<td>44%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q12. How concerned are you about the privacy of your personal data when using social media (such as Facebook and Google)?</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2 (low)</td>
<td>11%</td>
</tr>
<tr>
<td>3 or 4</td>
<td>10%</td>
</tr>
<tr>
<td>5 or 6</td>
<td>25%</td>
</tr>
<tr>
<td>7 or 8</td>
<td>30%</td>
</tr>
<tr>
<td>9 or 10 (high)</td>
<td>24%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q13. How much control do you have over how your personal information is collected, shared and stored when using smart devices connected to the IoT?</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2 (low)</td>
<td>48%</td>
</tr>
<tr>
<td>3 or 4</td>
<td>27%</td>
</tr>
<tr>
<td>5 or 6</td>
<td>9%</td>
</tr>
<tr>
<td>7 or 8</td>
<td>10%</td>
</tr>
<tr>
<td>9 or 10 (high)</td>
<td>6%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q14. Do you believe the benefits of the IoT outweigh your concerns about privacy or security?</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>44%</td>
</tr>
<tr>
<td>No</td>
<td>42%</td>
</tr>
<tr>
<td>Unsure</td>
<td>14%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
Q15. I believe the manufacturer of smart devices that connect to the IoT should provide the following information. Please check all that apply.

<table>
<thead>
<tr>
<th>Information Provided</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tell me what information is collected</td>
<td>71%</td>
</tr>
<tr>
<td>Tell me how the information is used</td>
<td>71%</td>
</tr>
<tr>
<td>Allow me to control what information is collected (opt-in and opt-out of information that is collected)</td>
<td>60%</td>
</tr>
<tr>
<td>Let me know how I can protect my information from being lost or stolen</td>
<td>50%</td>
</tr>
<tr>
<td>Tell me what I should do if the smart device is hacked</td>
<td>60%</td>
</tr>
<tr>
<td>Assurance that my data is safeguarded</td>
<td>52%</td>
</tr>
<tr>
<td>No information is necessary</td>
<td>14%</td>
</tr>
<tr>
<td>Tell me when my personal information is lost or stolen</td>
<td>57%</td>
</tr>
<tr>
<td>Compensate me if my information is lost or stolen</td>
<td>74%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>17%</td>
</tr>
<tr>
<td>Total</td>
<td>525%</td>
</tr>
</tbody>
</table>

Q16. Does your employer have the right to access personal data on your Smart device if you use it at work or connect to your employer’s Internet?

<table>
<thead>
<tr>
<th>Access Right</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>39%</td>
</tr>
<tr>
<td>No</td>
<td>52%</td>
</tr>
<tr>
<td>Unsure</td>
<td>9%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Part 2. Value of your personal data

Q17. The personal data I provide to companies is valuable because it helps them to market and sell products to others and me.

<table>
<thead>
<tr>
<th>Value</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>29%</td>
</tr>
<tr>
<td>Agree</td>
<td>32%</td>
</tr>
<tr>
<td>Unsure</td>
<td>23%</td>
</tr>
<tr>
<td>Disagree</td>
<td>11%</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>5%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
Q18. My personal data is a financial asset similar to traded goods, currencies or commodities.

<table>
<thead>
<tr>
<th>Pct%</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>25%</td>
</tr>
<tr>
<td>Agree</td>
<td>28%</td>
</tr>
<tr>
<td>Unsure</td>
<td>22%</td>
</tr>
<tr>
<td>Disagree</td>
<td>17%</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>8%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q19. Even if I willingly share my personal data with companies, I still control how they collect, share and store my personal data.

<table>
<thead>
<tr>
<th>Pct%</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>13%</td>
</tr>
<tr>
<td>Agree</td>
<td>19%</td>
</tr>
<tr>
<td>Unsure</td>
<td>21%</td>
</tr>
<tr>
<td>Disagree</td>
<td>30%</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>18%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q20. After browsing websites and/or making online purchases, do you believe you have control over how your personal data is used?

<table>
<thead>
<tr>
<th>Pct%</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, most of the time</td>
<td>13%</td>
</tr>
<tr>
<td>Yes, some of the time</td>
<td>17%</td>
</tr>
<tr>
<td>Rarely</td>
<td>51%</td>
</tr>
<tr>
<td>No</td>
<td>19%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q21. Do you believe that when you shop at a store and share personal information you have control over how your personal data is used?

<table>
<thead>
<tr>
<th>Pct%</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, most of the time</td>
<td>15%</td>
</tr>
<tr>
<td>Yes, some of the time</td>
<td>23%</td>
</tr>
<tr>
<td>Rarely</td>
<td>42%</td>
</tr>
<tr>
<td>No</td>
<td>21%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
Q22. When you browse the Internet, shop online or make in-store purchases, your personal data is collected. What do you believe companies do with your personal data?

<table>
<thead>
<tr>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>The data is used to understand my preferences 62%</td>
</tr>
<tr>
<td>The data is used to provide me with better security 38%</td>
</tr>
<tr>
<td>The data is used to understand other consumers’ preferences 57%</td>
</tr>
<tr>
<td>The data is sold by those collecting it for unknown purposes 42%</td>
</tr>
<tr>
<td>I do not know how companies use my personal data 25%</td>
</tr>
<tr>
<td>Total 224%</td>
</tr>
</tbody>
</table>

Q23. When you receive ads based upon your purchasing and browsing habits, do you believe this is helpful to you?

<table>
<thead>
<tr>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, most of the time 20%</td>
</tr>
<tr>
<td>Yes, some of the time 25%</td>
</tr>
<tr>
<td>Rarely 18%</td>
</tr>
<tr>
<td>No 37%</td>
</tr>
<tr>
<td>Total 100%</td>
</tr>
</tbody>
</table>

Q24. Do you belong to one or more loyalty programs that provide benefits in exchange for purchases (such as those offered by grocery stores, retailers, pharmacies, credit card companies, airlines and others)?

<table>
<thead>
<tr>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes 67%</td>
</tr>
<tr>
<td>No (Skip to Q28) 33%</td>
</tr>
<tr>
<td>Total 100%</td>
</tr>
</tbody>
</table>

Q25. How are you compensated for your participation in loyalty programs? Please select all that apply.

<table>
<thead>
<tr>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discounts on future purchases 64%</td>
</tr>
<tr>
<td>Early access to sales or discounts or hard to get products or services (i.e. tickets to a playoff game) 48%</td>
</tr>
<tr>
<td>Cash back or reimbursements 28%</td>
</tr>
<tr>
<td>Free goods and services 13%</td>
</tr>
<tr>
<td>Free and upgraded flights 29%</td>
</tr>
<tr>
<td>Concierge services 13%</td>
</tr>
<tr>
<td>Total 195%</td>
</tr>
</tbody>
</table>
Q26. Do you understand how your personal data is being used by your loyalty programs?  
Pct%  
Yes, full understanding 24%  
Yes, some understanding 32%  
No 44%  
Total 100%

Q27. Do you believe you are adequately compensated for participation in your loyalty programs?  
Pct%  
Yes 39%  
No 40%  
Unsure 21%  
Total 100%

Q28a. Would you be willing to provide your personal data to trusted companies in exchange for money?  
Pct%  
Yes 56%  
No, I would not provide my personal data for any amount of money 36%  
Unsure 7%  
Total 100%

Q28b. If yes, how much would a trusted company have to pay you to obtain the following data about you? Please identify only one minimum amount for each data category listed. Response scale was converted from Euros to US$.  
<table>
<thead>
<tr>
<th>Data Category</th>
<th>&lt; $1</th>
<th>$1 to $5</th>
<th>$6 to $10</th>
<th>$11 to $25</th>
<th>$26 to $50</th>
<th>$51 to $100</th>
<th>&gt; $100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser settings &amp; histories</td>
<td>26%</td>
<td>44%</td>
<td>11%</td>
<td>12%</td>
<td>7%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Credit history</td>
<td>10%</td>
<td>9%</td>
<td>13%</td>
<td>24%</td>
<td>32%</td>
<td>6%</td>
<td>6%</td>
</tr>
<tr>
<td>Email address</td>
<td>33%</td>
<td>20%</td>
<td>32%</td>
<td>11%</td>
<td>2%</td>
<td>2%</td>
<td>0%</td>
</tr>
<tr>
<td>Health condition</td>
<td>13%</td>
<td>13%</td>
<td>7%</td>
<td>7%</td>
<td>8%</td>
<td>18%</td>
<td>34%</td>
</tr>
<tr>
<td>Hobbies, tastes &amp; preferences</td>
<td>33%</td>
<td>24%</td>
<td>17%</td>
<td>7%</td>
<td>14%</td>
<td>4%</td>
<td>0%</td>
</tr>
<tr>
<td>Home address</td>
<td>37%</td>
<td>25%</td>
<td>15%</td>
<td>8%</td>
<td>8%</td>
<td>7%</td>
<td>1%</td>
</tr>
<tr>
<td>Marital status</td>
<td>40%</td>
<td>33%</td>
<td>14%</td>
<td>7%</td>
<td>2%</td>
<td>3%</td>
<td>1%</td>
</tr>
<tr>
<td>Name</td>
<td>44%</td>
<td>42%</td>
<td>9%</td>
<td>2%</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Names of friends &amp; family members</td>
<td>23%</td>
<td>13%</td>
<td>17%</td>
<td>14%</td>
<td>20%</td>
<td>8%</td>
<td>4%</td>
</tr>
<tr>
<td>Passwords (login details)</td>
<td>2%</td>
<td>2%</td>
<td>4%</td>
<td>11%</td>
<td>16%</td>
<td>26%</td>
<td>40%</td>
</tr>
<tr>
<td>Payment details (credit card)</td>
<td>11%</td>
<td>13%</td>
<td>9%</td>
<td>19%</td>
<td>19%</td>
<td>22%</td>
<td>7%</td>
</tr>
<tr>
<td>Phone numbers</td>
<td>29%</td>
<td>30%</td>
<td>31%</td>
<td>7%</td>
<td>2%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Photos &amp; videos</td>
<td>24%</td>
<td>28%</td>
<td>17%</td>
<td>18%</td>
<td>9%</td>
<td>2%</td>
<td>1%</td>
</tr>
<tr>
<td>Physical location (GPS)</td>
<td>20%</td>
<td>27%</td>
<td>24%</td>
<td>9%</td>
<td>12%</td>
<td>4%</td>
<td>3%</td>
</tr>
<tr>
<td>Purchase histories</td>
<td>9%</td>
<td>11%</td>
<td>29%</td>
<td>28%</td>
<td>15%</td>
<td>5%</td>
<td>3%</td>
</tr>
<tr>
<td>Social Security number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Special dates including date of birth</td>
<td>45%</td>
<td>32%</td>
<td>11%</td>
<td>8%</td>
<td>4%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Gender</td>
<td>70%</td>
<td>22%</td>
<td>4%</td>
<td>3%</td>
<td>2%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>School or employer</td>
<td>28%</td>
<td>23%</td>
<td>19%</td>
<td>13%</td>
<td>9%</td>
<td>7%</td>
<td>0%</td>
</tr>
</tbody>
</table>
### Part 3. Demographics

#### D1. Gender

<table>
<thead>
<tr>
<th></th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Female</td>
<td>51%</td>
</tr>
<tr>
<td>Male</td>
<td>49%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

#### D2. Age

<table>
<thead>
<tr>
<th>Age</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 to 25</td>
<td>21%</td>
</tr>
<tr>
<td>26 to 35</td>
<td>24%</td>
</tr>
<tr>
<td>36 to 45</td>
<td>19%</td>
</tr>
<tr>
<td>46 to 55</td>
<td>15%</td>
</tr>
<tr>
<td>56 to 65</td>
<td>13%</td>
</tr>
<tr>
<td>65+</td>
<td>7%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

#### D3. Highest Level of Education

(US scale presented):

<table>
<thead>
<tr>
<th>Education</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>High School</td>
<td>19%</td>
</tr>
<tr>
<td>Vocational</td>
<td>23%</td>
</tr>
<tr>
<td>College (attended, no degree)</td>
<td>24%</td>
</tr>
<tr>
<td>College (4 year degree)</td>
<td>25%</td>
</tr>
<tr>
<td>Post Graduate</td>
<td>8%</td>
</tr>
<tr>
<td>Doctorate</td>
<td>1%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

#### D4. Household Income

(Expressed in US$):

<table>
<thead>
<tr>
<th>Income Range</th>
<th>Pct%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than $25,000</td>
<td>11%</td>
</tr>
<tr>
<td>$25,000 to $40,000</td>
<td>21%</td>
</tr>
<tr>
<td>$40,001 to $60,000</td>
<td>27%</td>
</tr>
<tr>
<td>$60,001 to $80,000</td>
<td>17%</td>
</tr>
<tr>
<td>$80,001 to $100,000</td>
<td>10%</td>
</tr>
<tr>
<td>$100,001 to $150,000</td>
<td>8%</td>
</tr>
<tr>
<td>$150,001 to $250,000</td>
<td>6%</td>
</tr>
<tr>
<td>More than $250,000</td>
<td>2%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

---

**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.