Ponemon INSTITUTE

Privacy and Security in a Digital World

A Study of Consumers in the United States

Sponsored by IDX

Independently conducted by Ponemon Institute LLC

Publication Date: July 2020

Ponemon INSTITUTE

Privacy and Security in a Digital World:
A Study of Consumers in the United States
July 2020

Table of Contents	Page

Part 1. Introduction

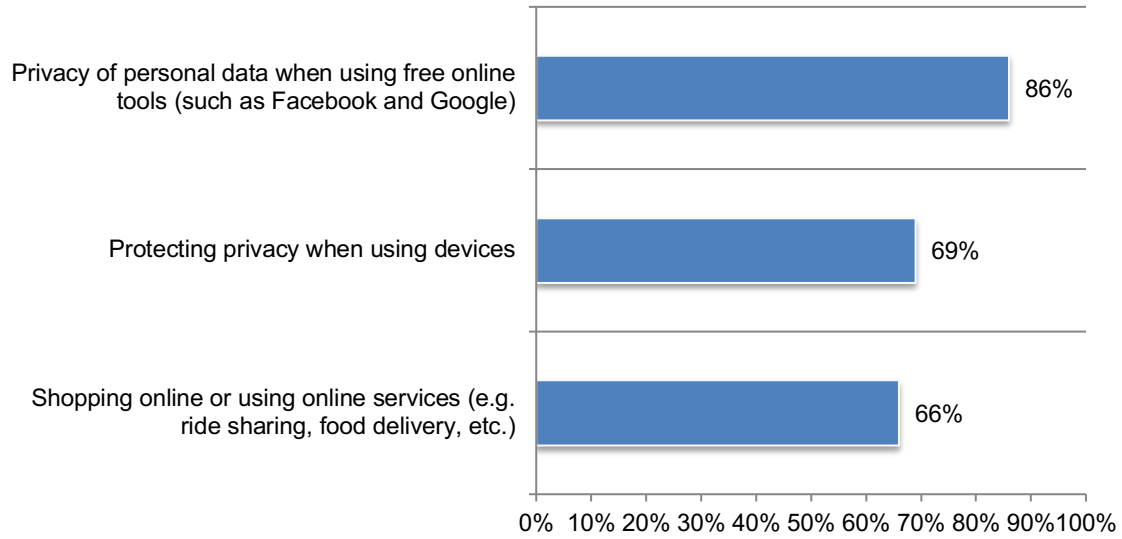
Privacy and Security in a Digital World: A Study of Consumers in the United States was conducted to understand the concerns consumers have about their privacy as more of their lives become dependent upon digital technologies. Based on the findings, the report also provides recommendations for how to protect privacy when using sites that track, share and sell personal data. Sponsored by IDX, we surveyed 652 consumers in the US. For the majority of these consumers, privacy of their personal information does matter.

Consumers are very concerned about their privacy when using Facebook, Google and other online tools. Consumers were asked to rate their privacy concerns on a scale of 1 = not concerned to 10 = very concerned when using online tools, devices and online services. Figure 1 presents the very concerned responses (7+ responses).

As shown, 86 percent of respondents say they are very concerned when using Facebook and Google, 69 percent of respondents are very concerned about protecting privacy when using devices and 66 percent of respondents say they are very concerned when shopping online or using online services.

When asked if they believe that Big Tech companies like Google, Twitter and Facebook will protect their privacy rights through self-regulation, 40 percent of consumers say industry self-regulation will suffice. However, 60 percent of consumers say government oversight is required (34 percent) or a combination of government oversight and industry self-regulation (26 percent) is required.

Figure 1. Concerns about privacy when using devices, free online tools and when shopping online or using online services
1 = not concerned to 10 = very concerned, 7+ responses presented



Following are the most salient findings:

- The increased use of social media and awareness about the potential threat to their digital privacy has consumers more concerned about their privacy. In fact, social media websites are the least trusted (61 percent of consumers) followed by shopping sites (52 percent of consumers).

- Consumers are most concerned about losing their civil liberties and having their identity stolen if personal information is lost, stolen or wrongfully acquired by outside parties (56 percent and 54 percent of respondents, respectively). Only 25 percent of consumers say they are concerned about marketing abuses if their personal information is lost or stolen.

- Seventy-four percent of consumers say they rarely (24 percent) or never (50 percent) have control over their personal data. Despite this belief, 54 percent of consumers say they do not limit the data they provide when using online services. Virtually all consumers believe their email addresses and browser settings & histories are collected when using their devices, according to 96 percent and 90 percent of consumers, respectively.

- Home is where the trust is. Forty-six percent of consumers, when asked the one location they trust most when shopping online, banking and other financial activities online, say it is their home. Only 10 percent of consumers say it is when using public WiFi.

- Consumers believe search engines, social media and shopping sites are sharing and selling their personal data, according to 92 percent, 78 percent and 63 percent of consumers. To increase trust in online sites, consumers want to be explicitly required to opt-in before the site shares or sells their personal information, according to 70 percent of consumers.

- Consumers reject advertisers' use of their personal information to market to them. Seventy-three percent of consumers say advertisers should allow them to "opt-out" of receiving ads on any specific topic at any time, and 68 percent of consumers say they should not be able to serve ads based on their conversations and messaging. Sixty-four percent of consumers say they do not want to be profiled unless they grant permission.

- Online ads and the "creepy" factor. Sixty-six percent of consumers say they have received online ads that are relevant but not based on their online search behavior or publicly available information frequently (41 percent of consumers) or rarely (25 percent of consumers). Sixty-four percent of consumers say they think it is "creepy" when that happens.

- Forty-five percent of consumers are not aware that their devices have privacy controls they can use to set their level of information sharing. Of the 55 percent of consumers who are aware, 60 percent say they review and update settings on their computers and 56 percent say they review and update settings on their smartphones.

- Fifty-four percent of consumers say online service providers should be held most accountable for protecting consumers' privacy rights when going online. Forty-five percent of consumers say they themselves should be most accountable.

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:

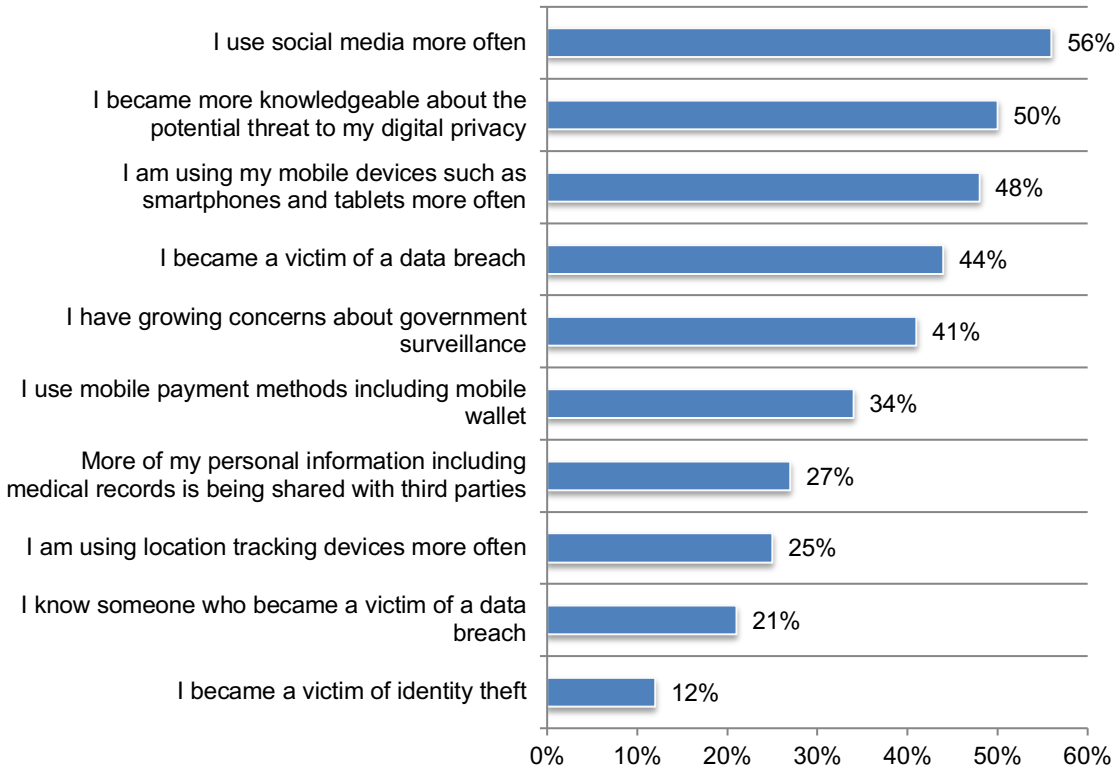
- Does digital privacy matter?
- Consumers' trust in the use of online sites
- Perceptions about third parties' and advertisers' use of consumer information
- Consumers' actions to protect their personal information
- Differences in consumers' attitudes about digital privacy based on their privacy profile
- Differences in consumers' attitudes about digital privacy based on their age
- Recommendations on how consumers can protect their digital privacy

Does digital privacy matter?

Use of social media has increased concerns about privacy. Sixty-eight percent of respondents say they have become more concerned about the privacy and security of their personal information in the past three years.

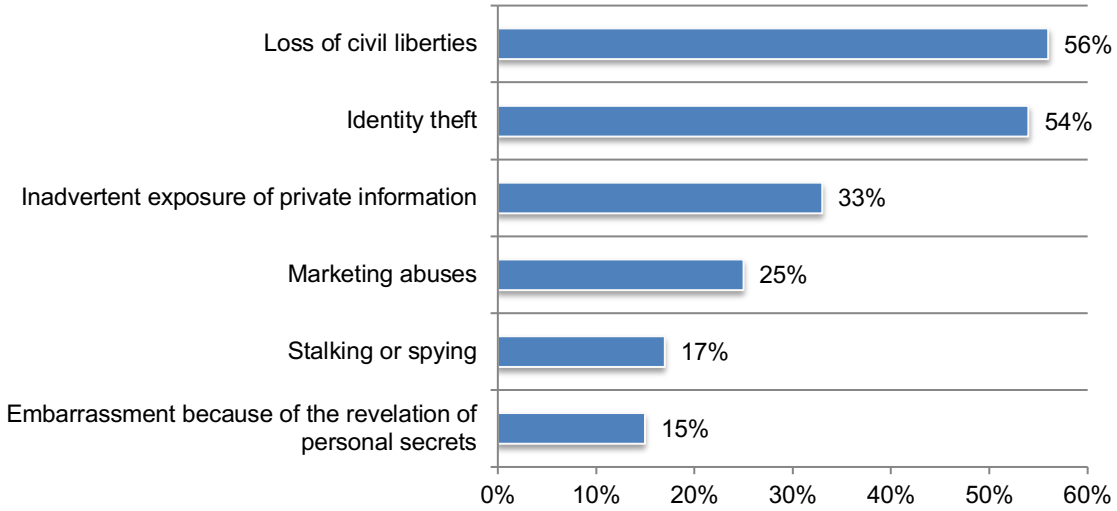
As shown in Figure 2, reasons these respondents worry about their privacy are: the increased use of social media (56 percent), they became more knowledgeable about the potential threat to their digital privacy (50 percent) and the increased use of mobile devices such as smartphones and tablets (48 percent). Forty-four percent say they are more worried about the protection of their personal information because they became a victim of a data breach.

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



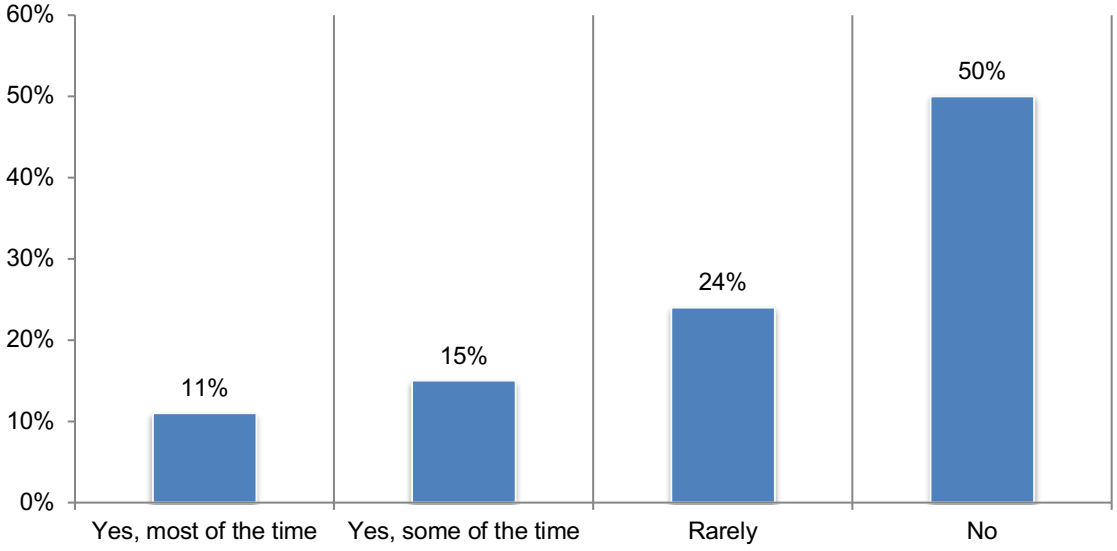
Consumers are most concerned about losing their civil liberties and having their identity stolen if personal information is lost, stolen or wrongfully acquired by outside parties. Only 25 percent of consumers say they are concerned about marketing abuses if their personal information is lost or stolen, as shown in Figure 3.

Figure 3. What are your primary concerns if personal information is lost, stolen or wrongfully acquired by outside parties?
Two responses permitted



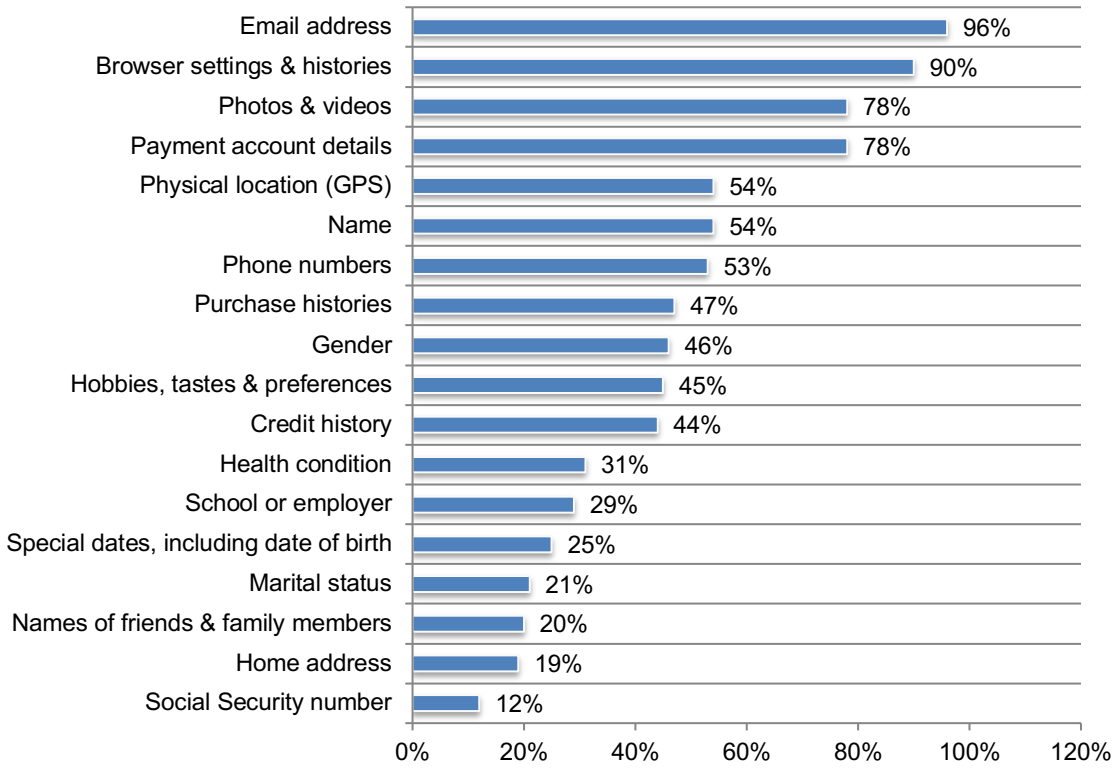
Consumers believe they do not have control over their personal data. As shown in Figure 4, 74 percent of consumers say they rarely (24 percent) or never (50 percent) have control over how their personal data will be used.

Figure 4. Do you have control over how your personal data will be used?



Virtually all consumers believe their email addresses and browser settings and histories are collected when using their devices. Figure 5 presents the types of personal information that could be collected by consumers' use of their various devices. Ninety-six percent of respondents say their email addresses are collected and 90 percent of respondents say browser settings and histories are collected. Only 12 percent of respondents say their Social Security numbers are collected.

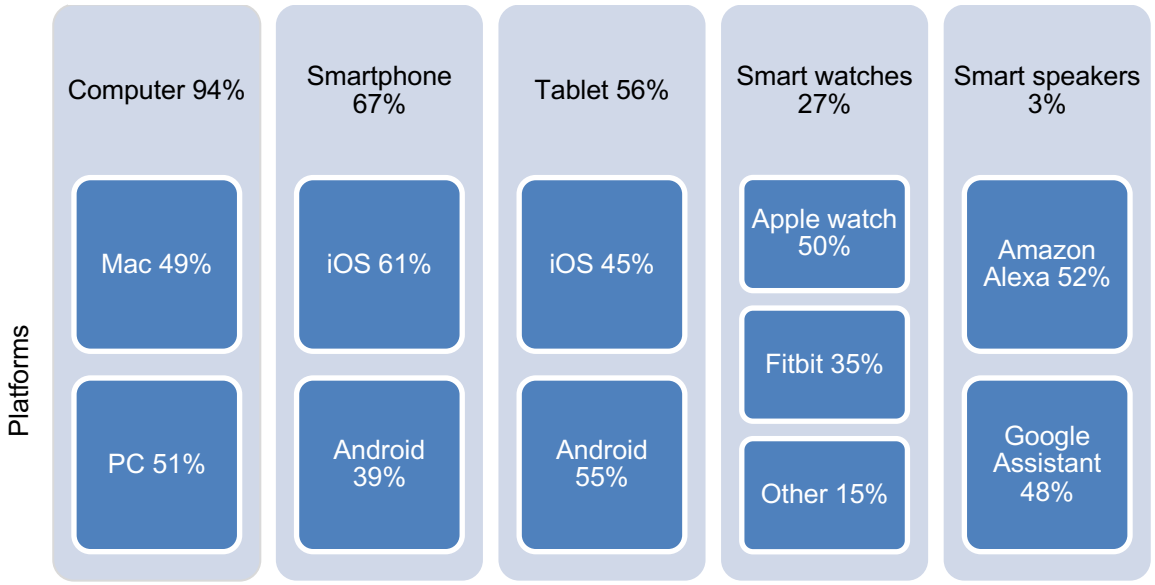
Figure 5. What personal information consumers believe is collected about them
More than one response permitted



Consumers' trust in the use of online services

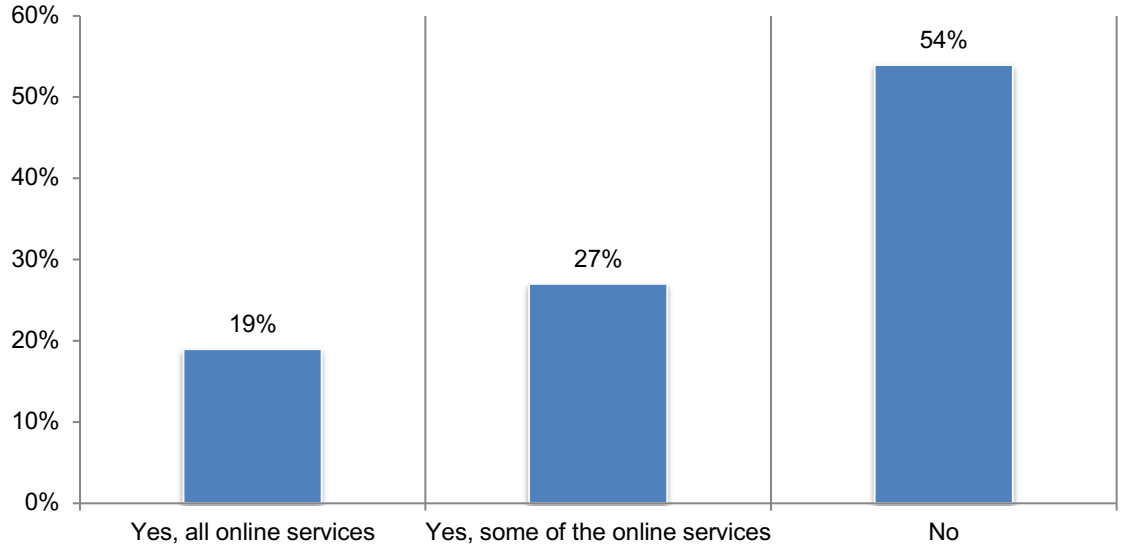
Figure 6 presents the online devices and platforms used by consumers in this study. As shown, 67 percent of respondents use smartphones and 61 percent use the iOS platform and 39 percent use an Android platform. Fifty-six percent of consumers use a tablet and 45 percent of these consumers use an iOS platform and 55 percent use an Android platform.

Figure 6. The online devices and primary platforms used by consumers



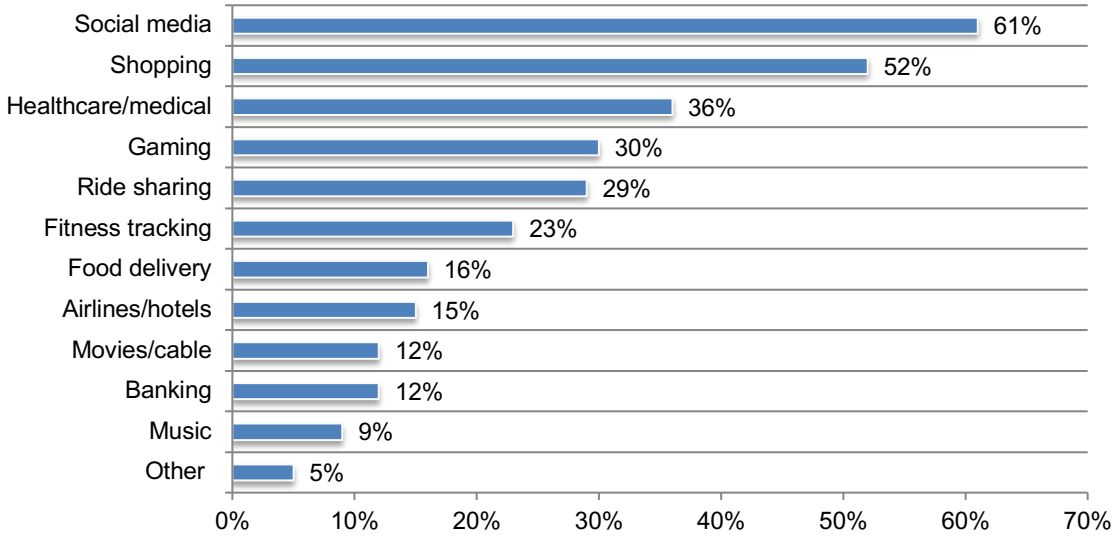
While 74 percent of consumers say they have no control over the personal information that is collected on them, they are not limiting the data they provide when using online services. According to Figure 7, 54 percent of consumers say they do not consciously limit what personal data they are providing.

Figure 7. Do you consciously try to limit providing personal data when using online services?



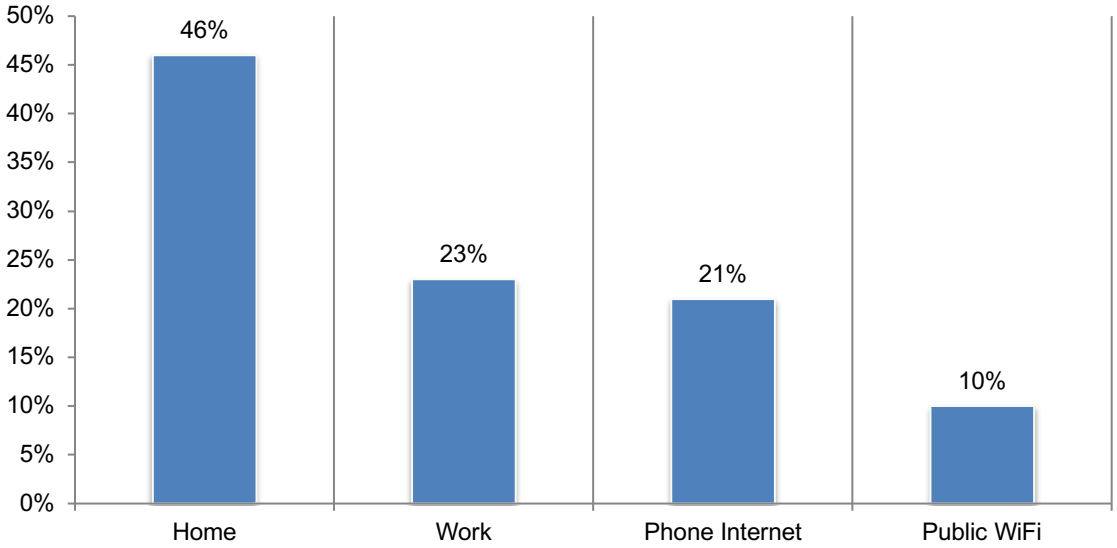
As discussed previously, consumers are more concerned about their privacy because of their use of social media. As shown in Figure 8, social media is the least trusted site followed by shopping sites.

Figure 8. What types of online sites do you trust the least?
Three responses permitted



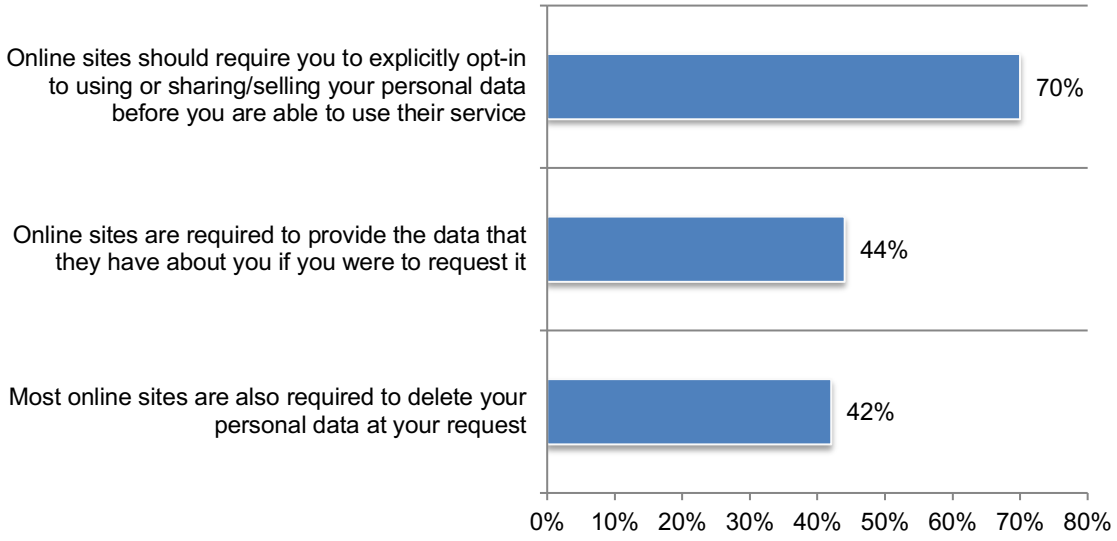
Home is where the trust is. When asked to name the one location they trust the most when shopping online, banking and doing other financial activities online, 46 percent of consumers say it is their home. Only 10 percent of consumers say it is when using public WiFi, as shown in Figure 9.

Figure 9. Where do you have the most trust when doing online shopping, banking and other financial activities online?
Only one choice permitted



To increase trust in online sites, consumers want to be explicitly required to opt-in before the site shares or sells their personal information. According to Figure 10, 70 percent of consumers agree that online sites should require them to explicitly opt-in to using or sharing/selling their personal data before being able to use their services. Only 42 percent say most online sites should be required to delete their personal data at their request.

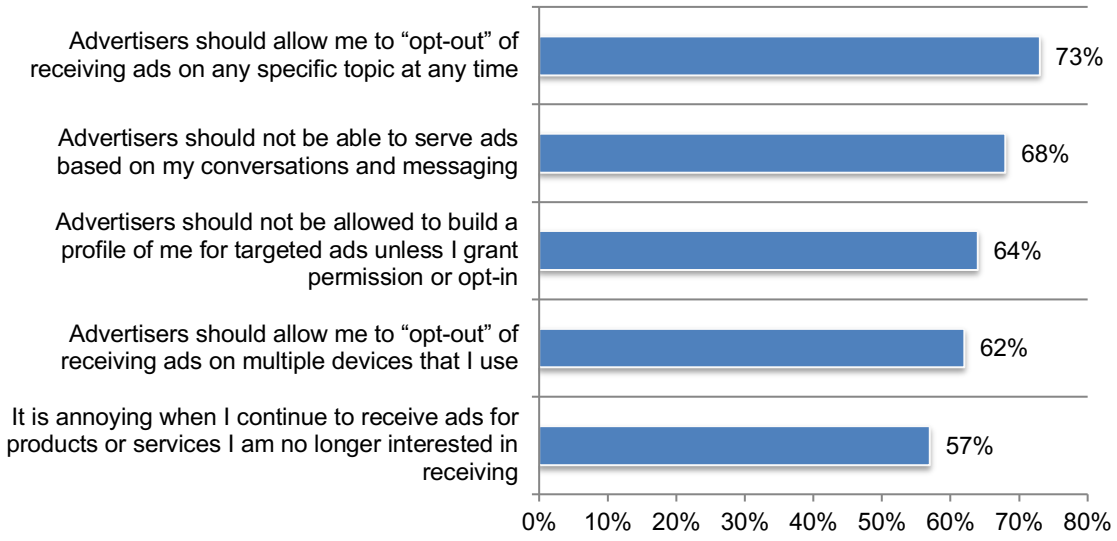
Figure 10. Perceptions about the practices of online sites
Yes responses presented



Perceptions about third parties' and advertisers' use of consumer information

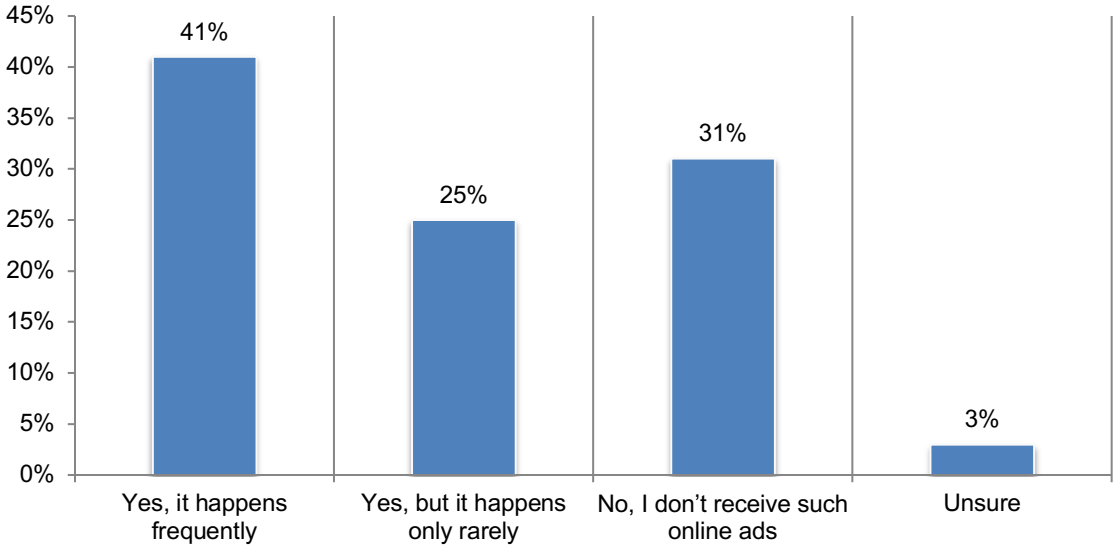
Consumers reject advertisers' use of their personal information for marketing purposes. Figure 11 lists various ways companies market to consumers when they are online. In every case, the majority of consumers want advertisers to change their practices. Seventy-three percent of consumers say advertisers should allow them to "opt-out" of receiving ads on any specific topic at any time and 68 percent of consumers say they should not be able to serve ads based on their conversations and messaging. Sixty-four percent of consumers say they do not want to be profiled unless they grant permission.

Figure 11. Perceptions about advertisers' practices
Strongly agree and Agree responses presented



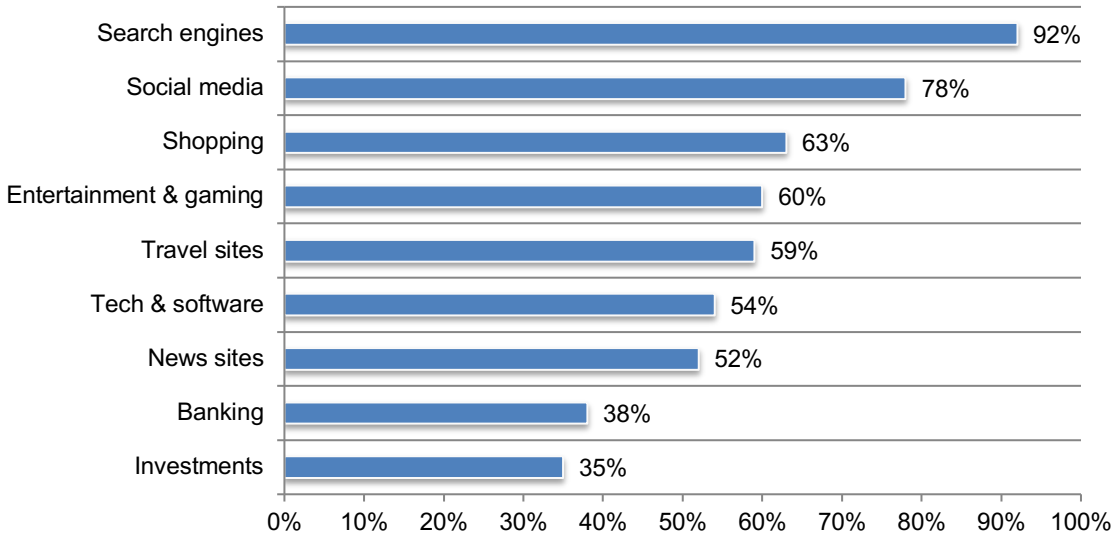
Online ads and the "creepy' factor. Sixty-six percent of consumers say they have received online ads that are relevant but not based on their online search behavior or publicly available information frequently (41 percent) or rarely (25 percent), as shown in Figure 12. Sixty-four percent of consumers say they think it is "creepy" when that happens.

Figure 12. Have you received online ads that are relevant but not based on your online search behavior or publicly available information?



Consumers believe search engines, social media and shopping sites are sharing and selling their personal data. According to Figure 13, 92 percent of consumers say search engines are selling and sharing their personal data followed by 78 percent of consumers who say social media is engaging in these practices.

Figure 13. Do you believe that the types of websites listed below share or sell your personal data?
Yes responses



Consumers' actions to protect their personal information

Many consumers are not taking steps to enhance their privacy and limit the sharing of their data. According to Figure 14, 45 percent of consumers are not aware that their devices have privacy controls they can use to set their level of information sharing. Of the 55 percent who are aware, 60 percent say they review and update settings on their computers and 56 percent say they review and update settings on their smartphones.

Figure 14. Which devices have you reviewed privacy controls and updated them to enhance your privacy and/or limit data sharing?
More than one response permitted

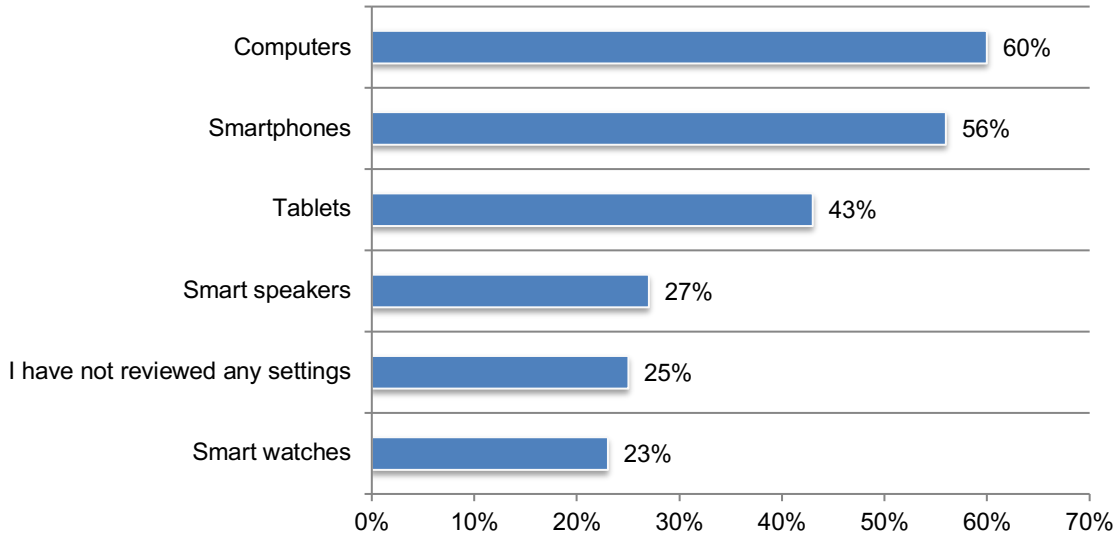
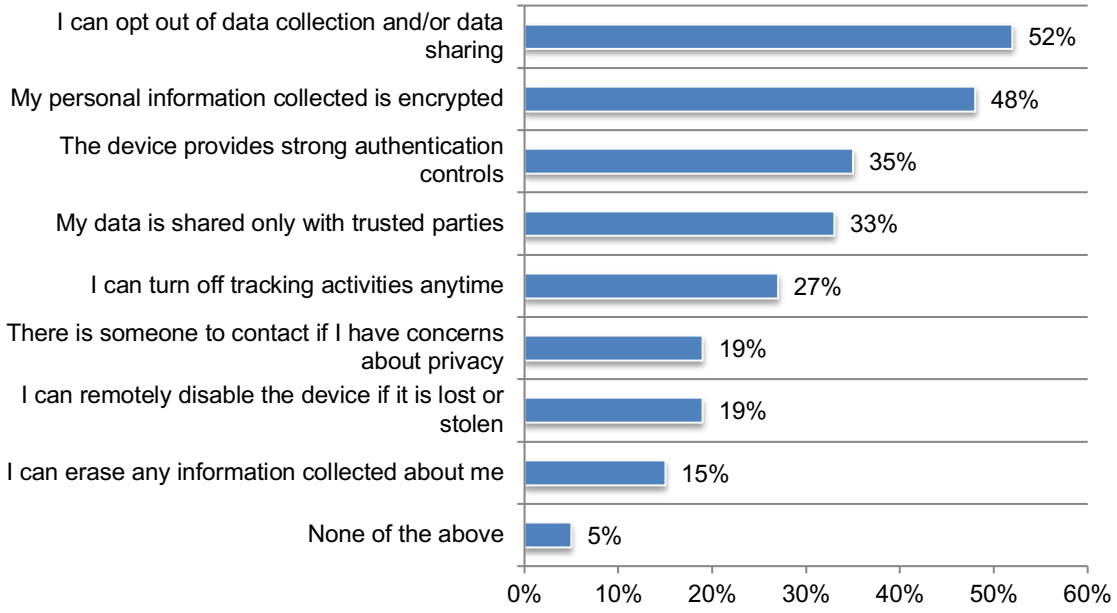


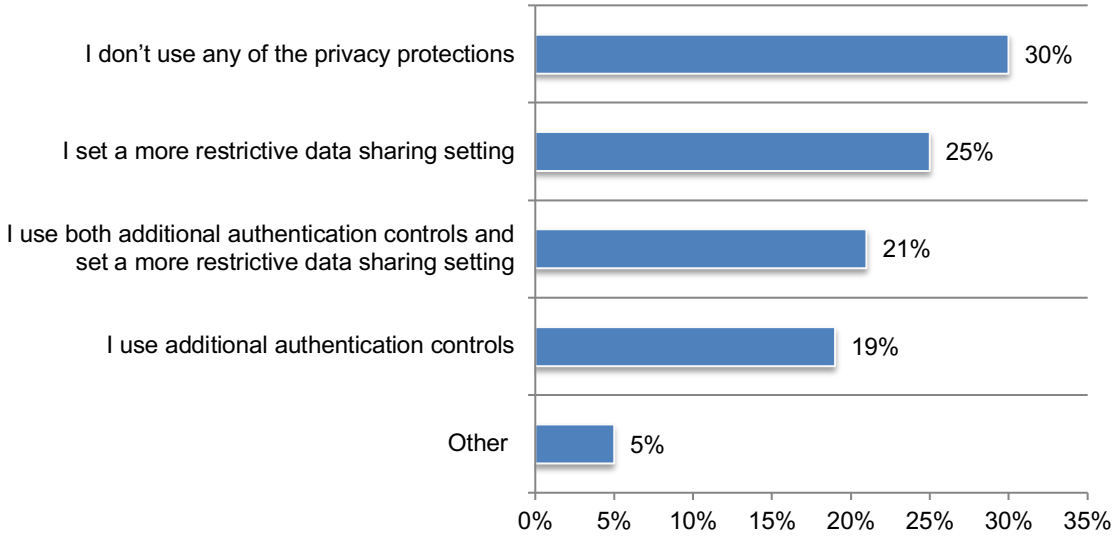
Figure 15 lists the protections available to consumers to protect personal information. Opting out of data collection and/or data sharing and encryption of personal information are available (52 percent of consumers and 48 percent of consumers, respectively). Only 27 percent of consumers say they can turn off tracking activities anytime and 19 percent say they can remotely disable the device if it is lost or stolen.

Figure 15. What protections are in place to protect your personal information?
More than one response permitted



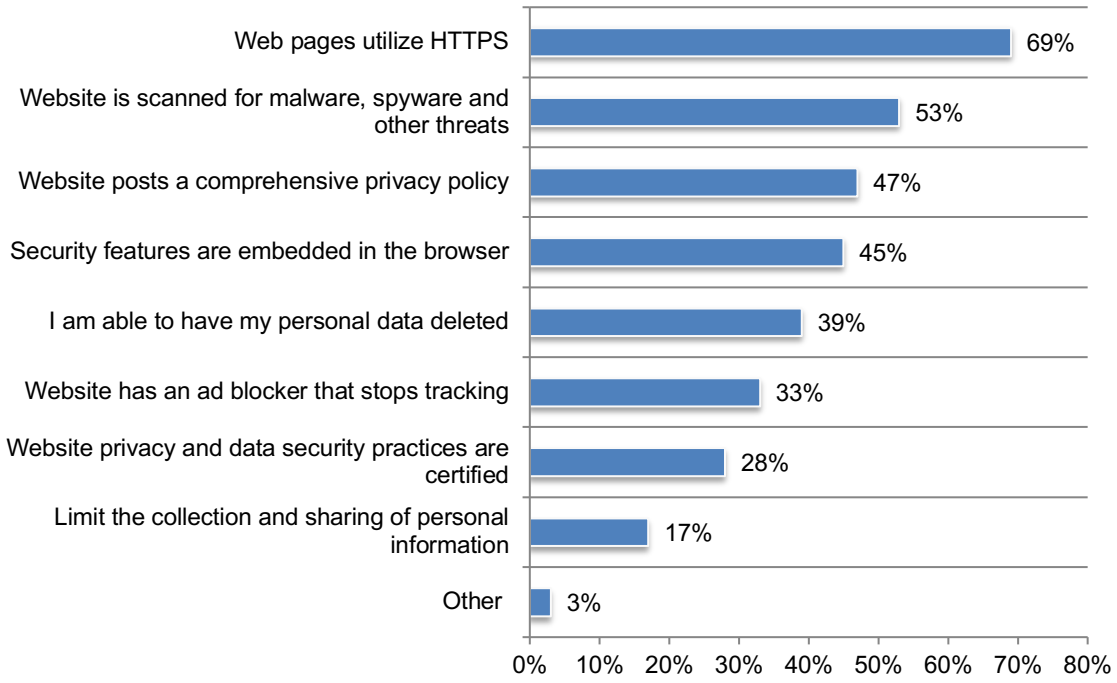
Most consumers are using privacy protections provided by their devices. As shown in Figure 16, 65 percent of consumers are using some type of privacy protection. These consumers are using a more restrictive data sharing setting (25 percent), using both additional authentication controls and a more restrictive data sharing setting (21 percent) and using additional authentication controls (19 percent).

Figure 16. Do you use any of the privacy protections provided by the devices you use?
Only one choice is permitted



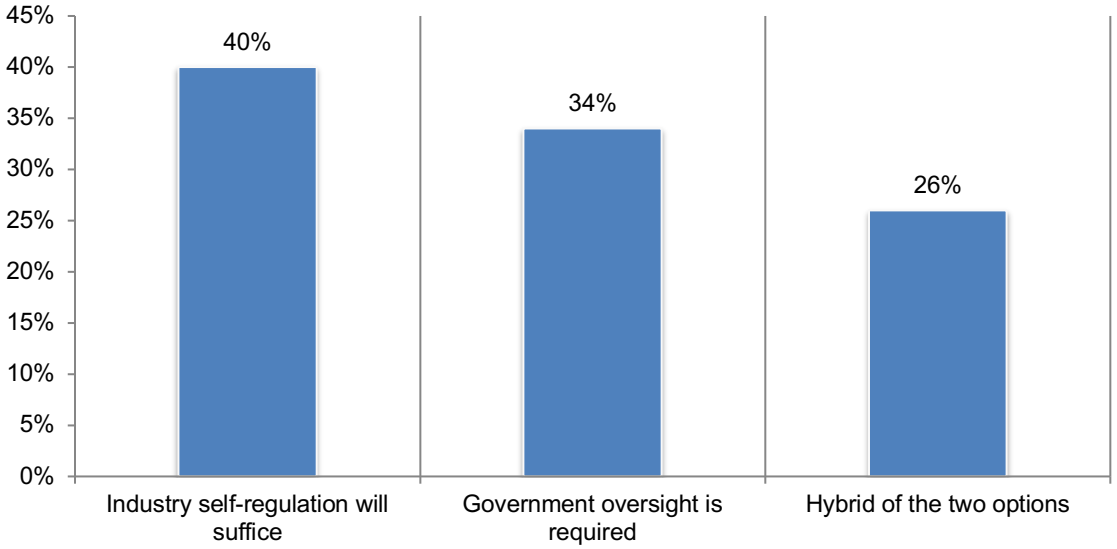
Consumers are concerned about their online privacy but have low expectations. According to Figure 17, 69 percent of consumers expect web pages to use HTTPS. However, only 33 percent of consumers expect the website to have an ad blocker that stops tracking and only 17 percent of consumers say they expect the website to limit the collection and sharing of personal information.

Figure 17. Do you expect the websites you access to provide you with the following privacy tools and settings?
More than one response permitted



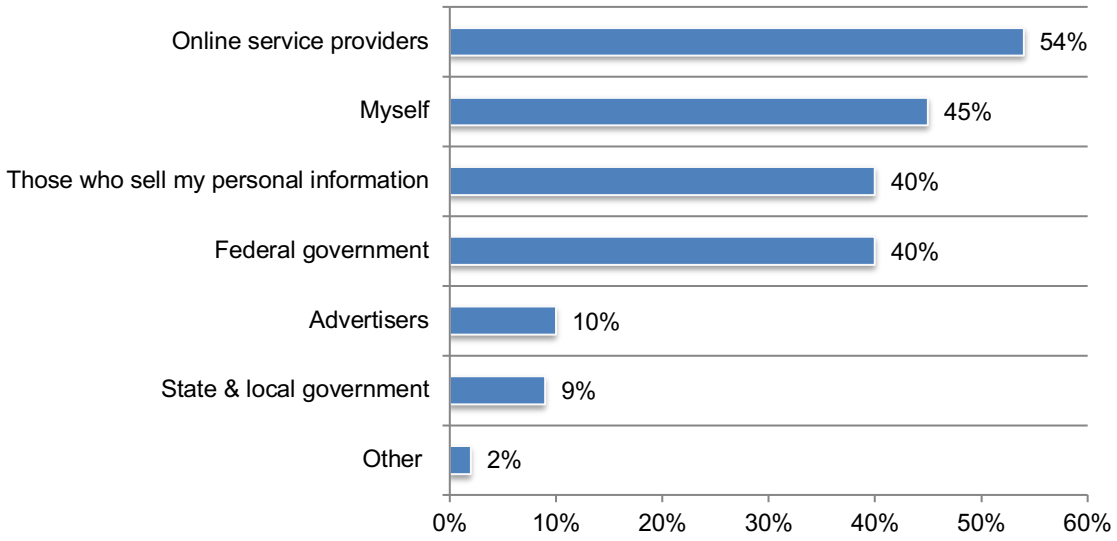
Most consumers do not believe Big Tech companies alone will protect their privacy rights through self-regulation. According to Figure 18, 60 percent of consumers say government oversight is required (34 percent) or a hybrid of the two options (26 percent).

Figure 18. Do you believe that Big Tech companies (like Google, Twitter and Facebook, among others) will protect your privacy rights through self-regulations, or does the government need to step in and regulate these companies?



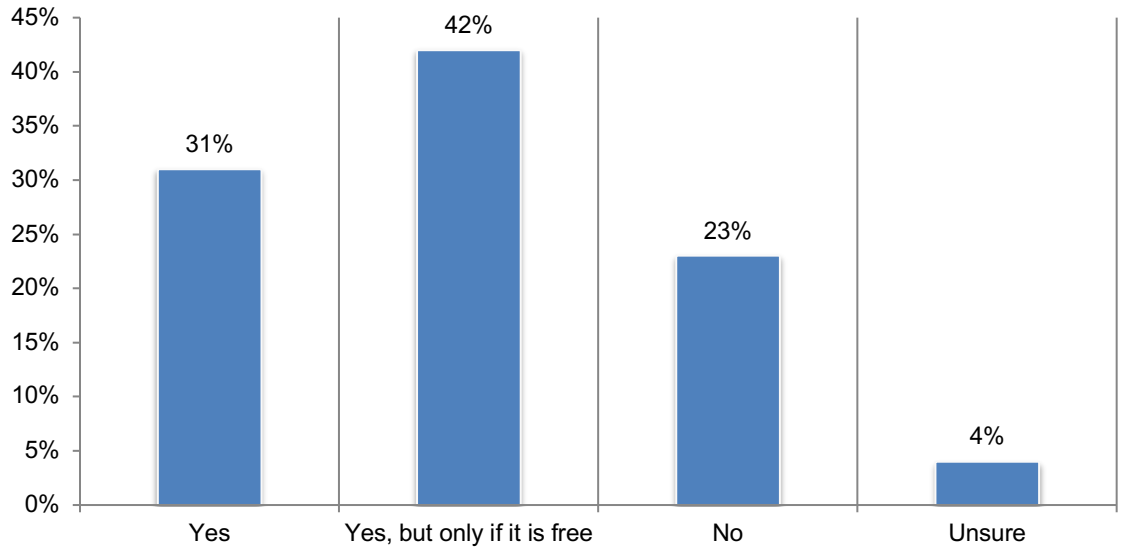
Consumers say online service providers should be held most accountable for protecting consumers' privacy rights when online. According to Figure 19, 54 percent of consumers say online service providers should be accountable for protecting the privacy of consumers. Forty-five say they themselves should assume responsibility.

Figure 19. Whom do you expect is most accountable for protecting your privacy rights when online?
Top two choices permitted



Consumers would prefer an online tool that is free. As shown in Figure 20, 31 percent of consumers would consider using and buying an online tool that would help protect their privacy when using sites that they believe are tracking, sharing and selling their personal data. However, 42 percent would use such a tool only if it is free.

Figure 20. Would you ever consider using/buying an online tool that would help you protect your privacy when using sites that track, share and sell your personal data?



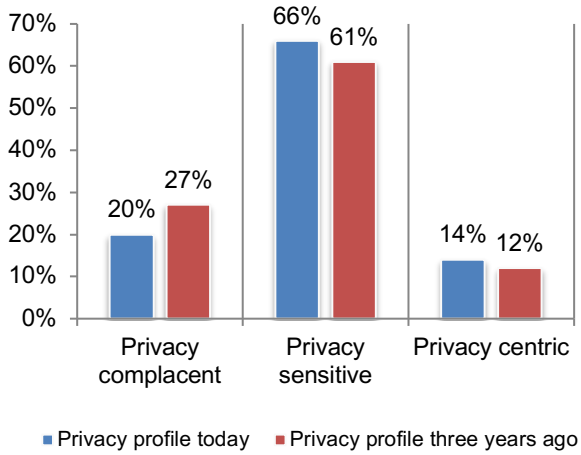
Differences in consumers' attitudes about digital privacy based on their privacy profile

In this section, we analyze the findings of the research based on what consumers in this study think about how they approach privacy in their lives. We group respondents according to three profiles: privacy centric[1], privacy sensitive and privacy complacent. The majority of respondents do care about their privacy at some level.

The most concerned about their privacy are those consumers who self-report they are privacy centric. As shown in Figure 21, only 14 percent of respondents say they are privacy centric and believe events that minimize their sense of privacy or diminish the safety of sensitive personal information will have a significant impact on their behavior. Twelve percent of respondents say they were privacy centric three years ago.

Most respondents (66 percent) say they have become more privacy sensitive over the past three years. While privacy is important to these respondents, they would not change their behaviors or information sharing practices.

Figure 21. Privacy Profiles

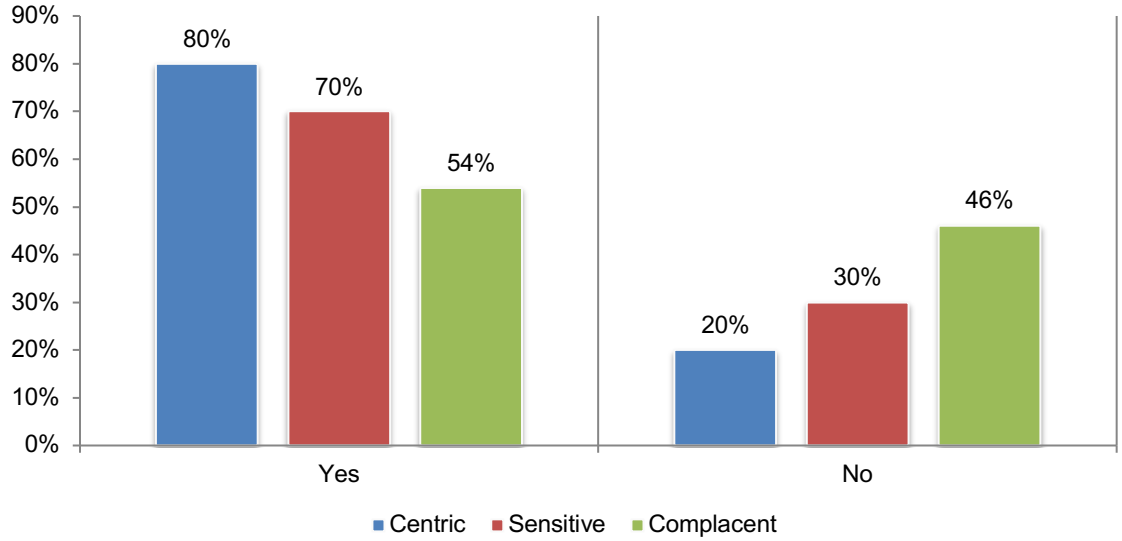


The least concerned are the privacy complacent respondents who really do not care very much if their sensitive personal information is shared or sold. However, the percentage of respondents self-reporting they are privacy complacent has declined significantly over the past three years.

[1]In this study, we asked respondents to select a privacy profile that reflects their perceptions about privacy and security developed by Ponemon Institute. These are: Events that minimize your sense of privacy or diminish the safety of your sensitive personal information will have a significant impact your behavior (privacy centric). While you say that privacy is important to you, it does not affect your behaviors or information sharing practices (privacy sensitive).
You really don't care very much about the sharing or selling of your sensitive personal information (privacy complacent).

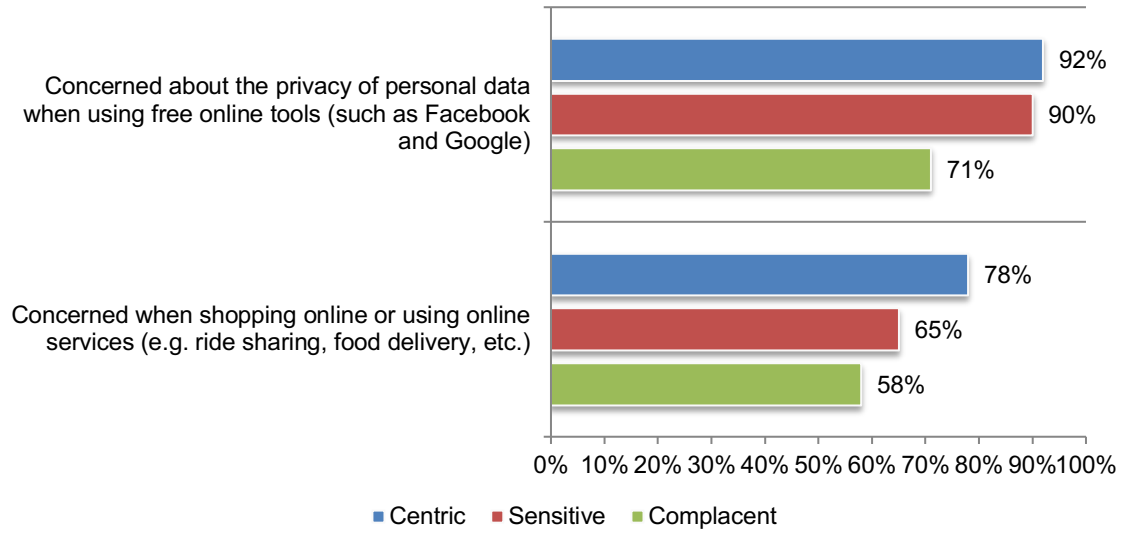
As shown in Figure 22, privacy centric consumers (80 percent) are, understandably, far more likely to have become concerned about the privacy of their personal data over the past three years. Fifty-four percent of complacent consumers have become more concerned about their privacy.

Figure 22. Have you become more concerned about the privacy of your personal data over the past three years?



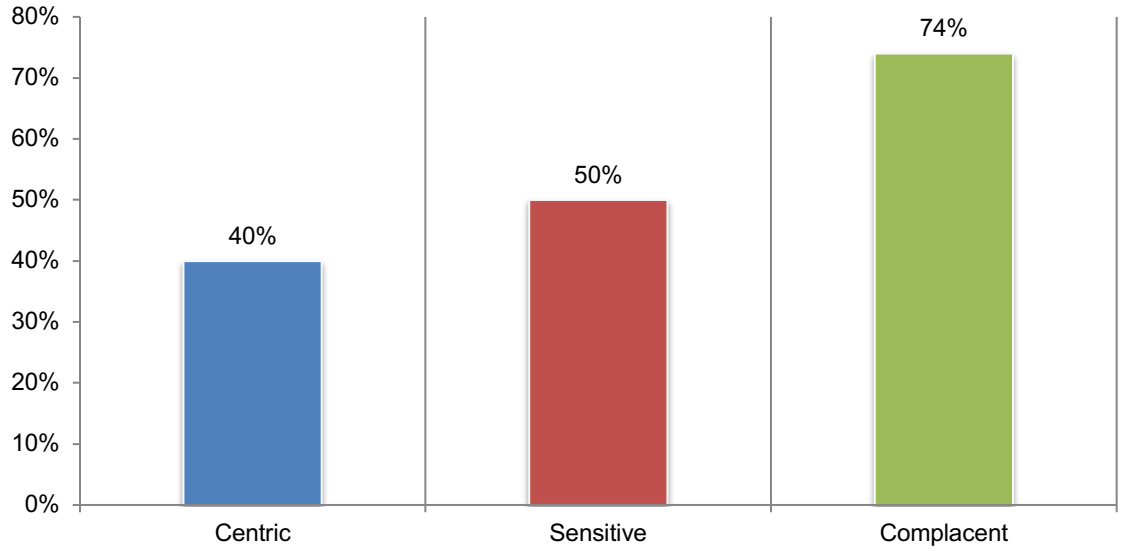
Privacy centric and sensitive respondents are far more concerned about the privacy of personal data when using free online tools, such as Facebook and Google. Consumers were asked to rate their concern about their privacy when online. Figure 23 shows the very concerned responses (7+ responses). According to the findings, 92 percent of privacy centric consumers and 90 percent of privacy sensitive consumers are very concerned about their privacy when using free online tools.

Figure 23. How concerned are you about the privacy of your personal data when using free online tools and online services?
1 = not concerned to 10 = very concerned, 7+ responses presented



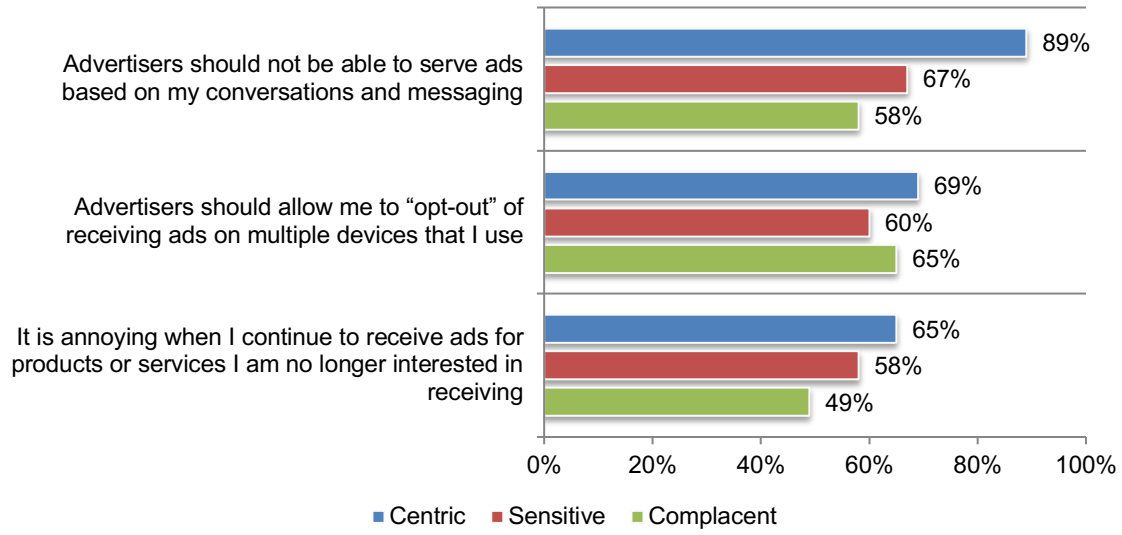
Privacy complacent consumers are not limiting their sharing of personal data when using online services. According to Figure 24, 74 percent of privacy complacent consumers do not limit providing their personal data when using online services.

Figure 24. Do you consciously try to limit providing personal data when using online services?
No responses presented



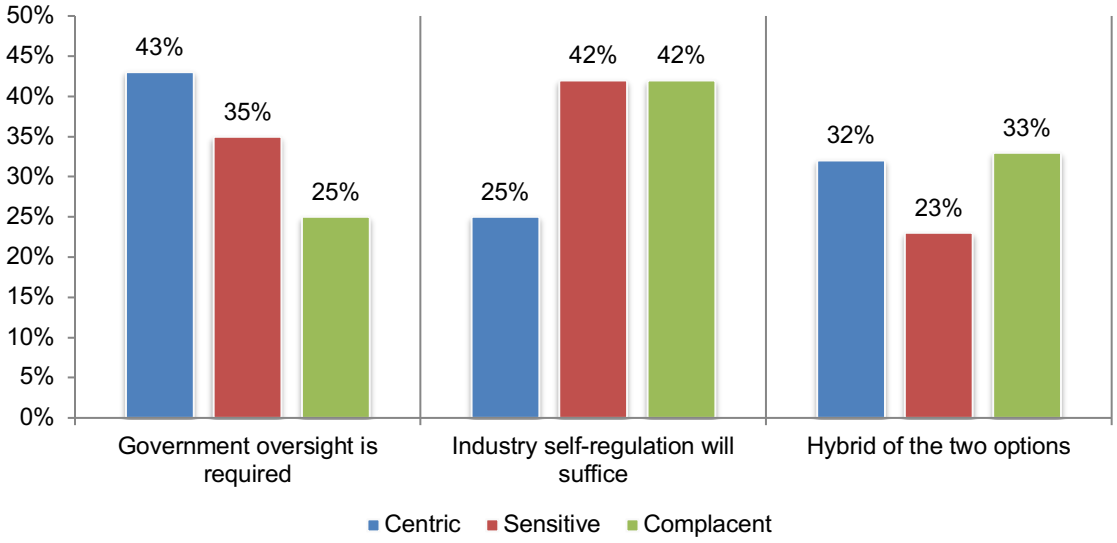
Privacy centric consumers are far more concerned about how advertisers are marketing to them. Eighty-nine percent of privacy centric consumers say advertisers should not be able to serve ads based on their conversations and messaging, as shown in Figure 25. By contrast, only 58 percent of privacy complacent consumers share this perception. 65 percent of privacy centric consumers are annoyed when they continue to receive ads for products or services they are no longer interested in receiving.

Figure 25. Perceptions about advertisers' practices
Strongly agree and Agree responses combined



Privacy centric consumers are more likely to want government oversight in order to protect their privacy rights. As shown in Figure 26, 43 percent of privacy centric consumers believe the government should intervene in protecting their privacy. Privacy sensitive and complacent consumers agree that industry self-regulation will suffice.

Figure 26. Do you believe Big Tech companies will protect your privacy rights through self-regulation or should the government step in and regulate these companies?

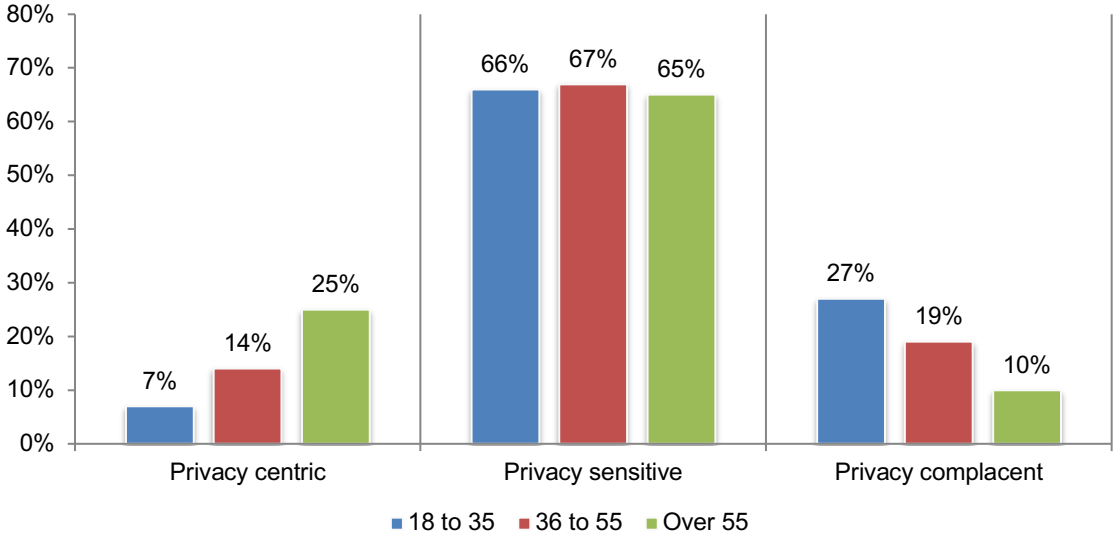


Differences in consumers' attitudes about digital privacy based on their age

In this section, we analyze the differences in consumers' attitudes about digital privacy based on their age. We organized the analysis according to three age groups as shown in the figures.

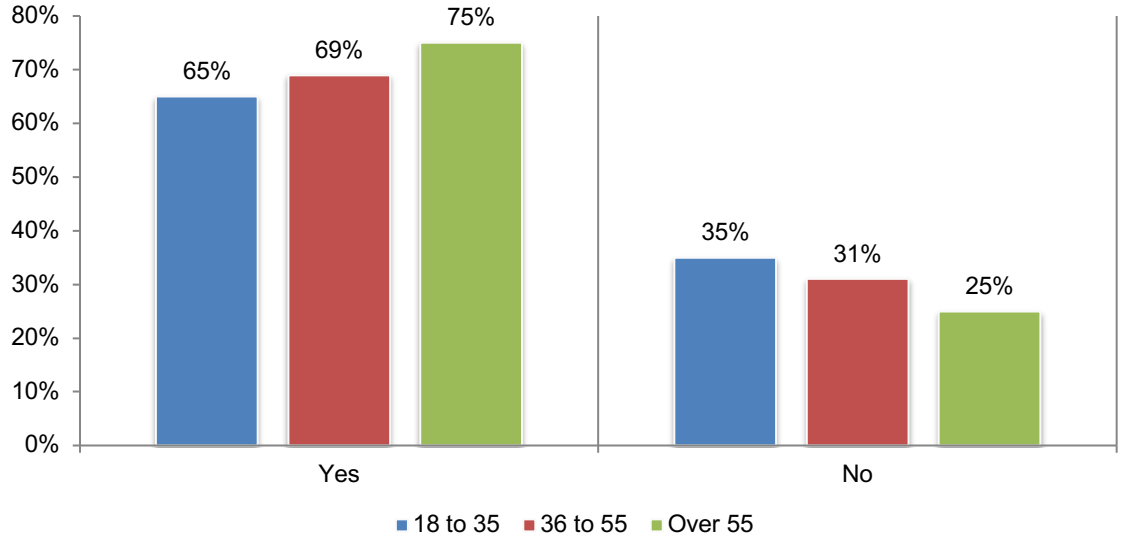
Most consumers in all age groups consider themselves privacy sensitive. Figure 27 presents the three privacy profiles based on age. It is interesting that more respondents in the 18 to 35 age group consider themselves privacy complacent.

Figure 27. What is your privacy profile?



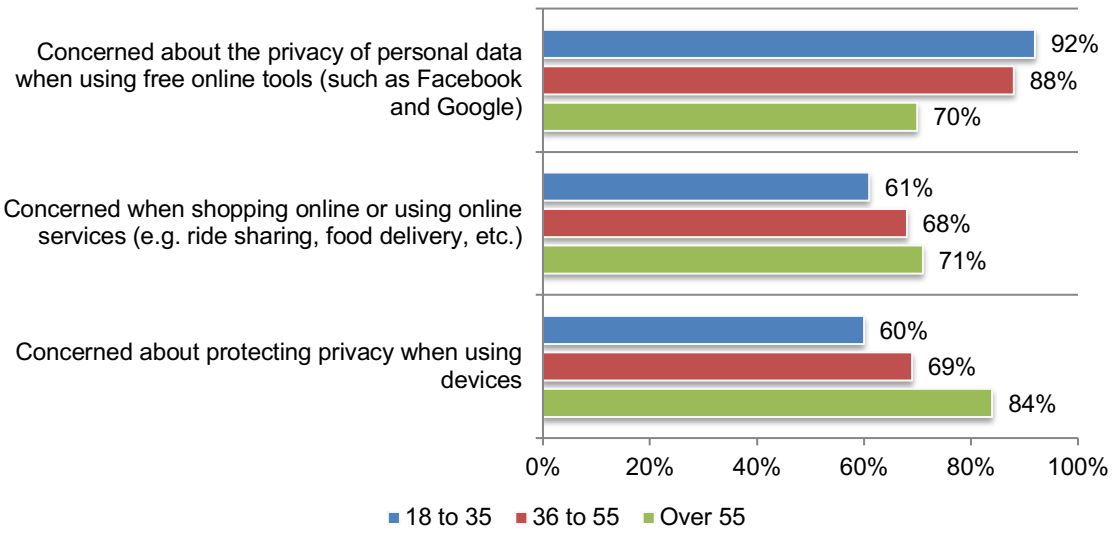
Older consumers have become more concerned about the privacy of their personal data over the past three years. According to Figure 28, 75 percent of consumers in the over 55 age group have become more concerned about their privacy. Thirty-five percent of those in the 18 to 35 age group have not become more concerned.

Figure 28. Have you become more concerned about the privacy of your personal data over the past three years?



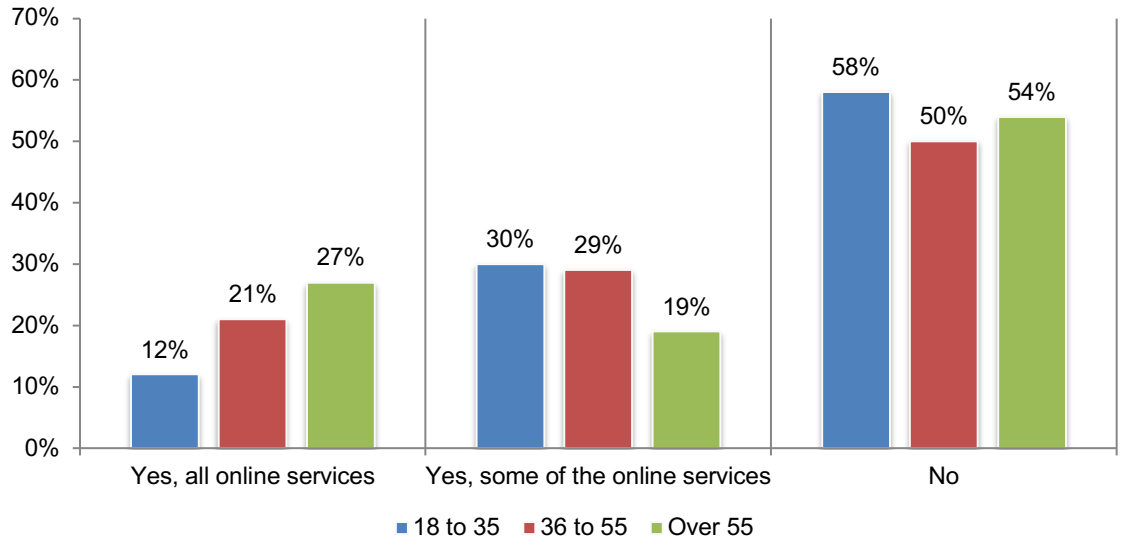
Younger consumers are most concerned about their privacy when using devices, free online tools and when shopping online or using online services. According to Figure 29, virtually all young consumers (92 percent) are very concerned about their privacy when using devices, free online tools and when shopping online or using online services, whereas 84 percent of older consumers are concerned about protecting privacy when using devices.

Figure 29. How concerned are you about privacy when using devices, free online tools and when shopping online or using online services?
1 = not concerned to 10 = very concerned (7+ responses)



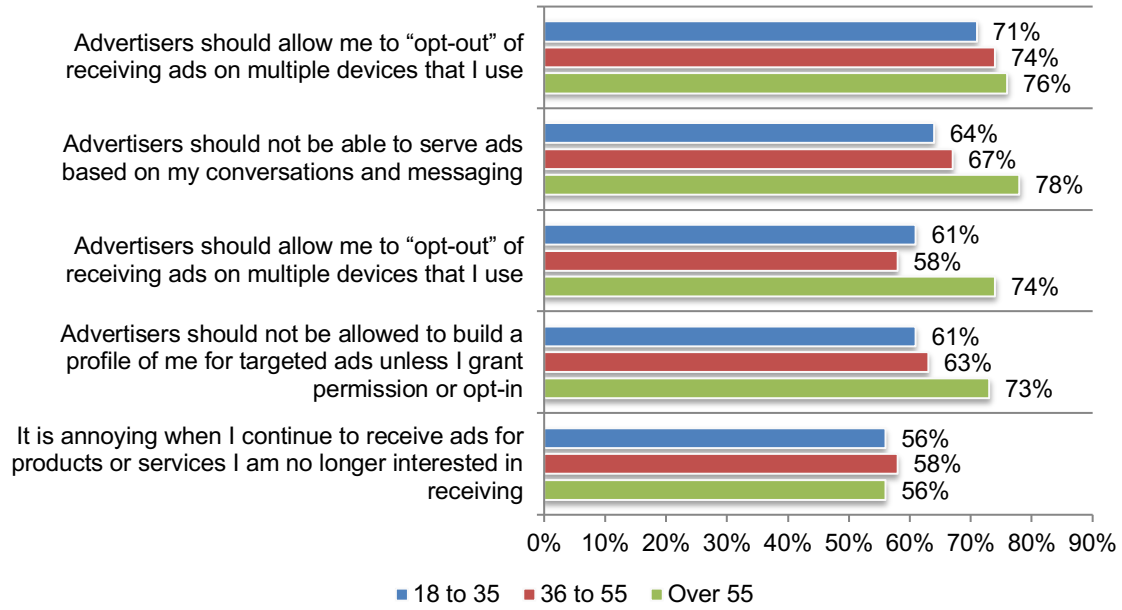
The majority of consumers in all age groups are not providing personal data when using online services, as shown in Figure 30.

Figure 30. Do you consciously try to limit providing personal data when using online services?



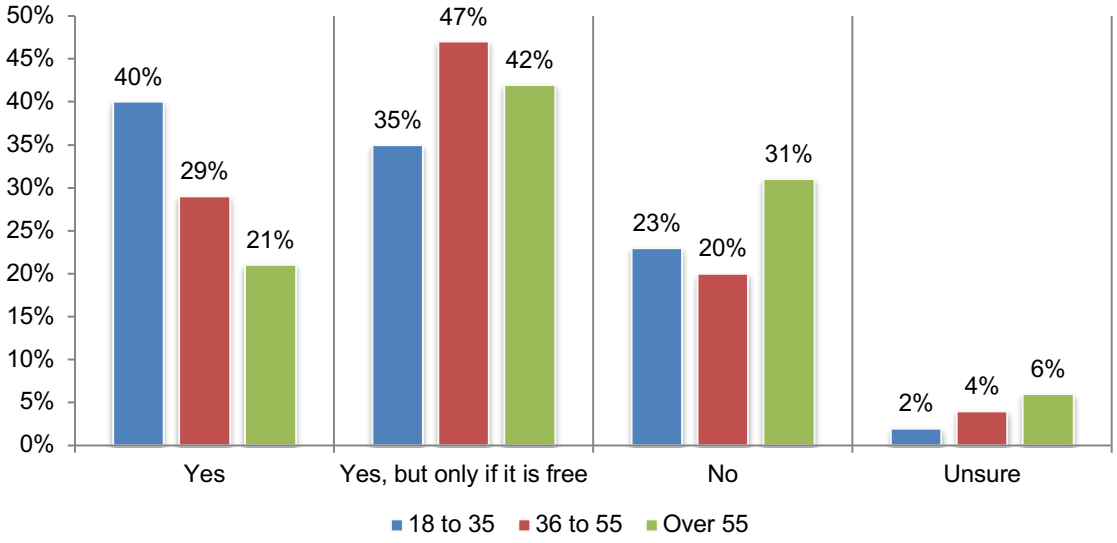
Older consumers are more concerned about the practices of advertisers. According to Figure 31, 78 percent of older consumers say advertisers should not be able to serve ads based on their conversations and messaging. They also more strongly agree that advertisers should allow them to "opt-out" of receiving ads on multiple devices they use and 73 percent say advertisers should not be allowed to build a profile for targeted ads unless permission is granted.

Figure 31. Perceptions about advertisers' practices
Strongly agree and Agree responses combined



Younger consumers are more likely to consider using or buying an online tool to protect their privacy and older consumers are less likely to use such a tool. As shown in Figure 22, younger consumers are most likely to use an online tool that would protect privacy when using sites that track, share and sell their personal data, even if it is not free.

Figure 32. Would you consider using/buying an online tool that would help you protect your privacy when using sites that track, share and sell your personal data?



Recommendations on how consumers can protect their digital privacy

To protect their privacy and security in a digital world, we recommend taking the following steps.

- **Password hygiene is key.** When setting up new accounts, use unique passwords for each new account, and try not to use the same email address for all online platforms.
- **Take control of your privacy settings.** It is also important to customize your privacy settings when setting up a new account. Take inventory of what details you have provided online through social media. How much could a hacker learn about you?
- **Consumers should think twice before consenting to sell their data to online service providers.** The more personal information you allow others to use, the more vulnerable you are to data breaches of third-party organizations and, as a consequence, the potential loss of finances and identity.
- **Use a Virtual Private Network (VPN) to secure your connection and avoid public WiFi networks that are not secured against hackers.** A VPN gives an added layer of protection between your devices and the Internet, hides your IP address and location, and encrypts your data after it leaves your device and travels to whatever website you are visiting.
- **Be aware of COVID-19 related scams, phishing and malware attacks.** At this time, you should be especially cautious when working or shopping online from home. You should be sure to use a VPN when on a potentially unsecure network and should update the firmware on your router, firewall, modem and wireless access points in your home.
- **Invest in identity protection.** Finally, subscribe to an identity protection service like MyIDCare that will help detect early signs of identity fraud for consumers.

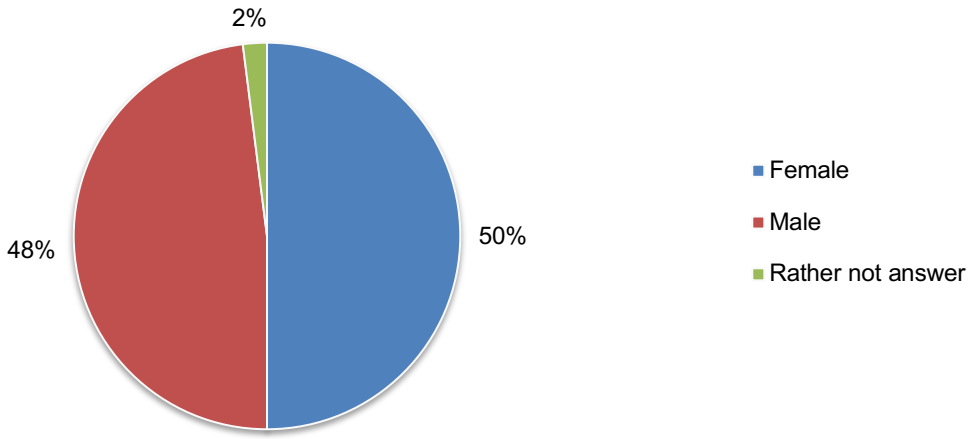
Part 3. Methods

A sampling frame of 16,751 consumers in the United States were selected as participants in this survey. Table 1 shows 708 total returns. Screening and reliability checks required the removal of 56 surveys. Our final sample consisted of 652 surveys, or a 3.9 percent response rate.

Table 1. Sample response	FY2020	Pct%
Sampling frame	16,751	100.0%
Total returns	708	4.2%
Rejected or screened surveys	56	0.3%
Final sample	652	3.9%

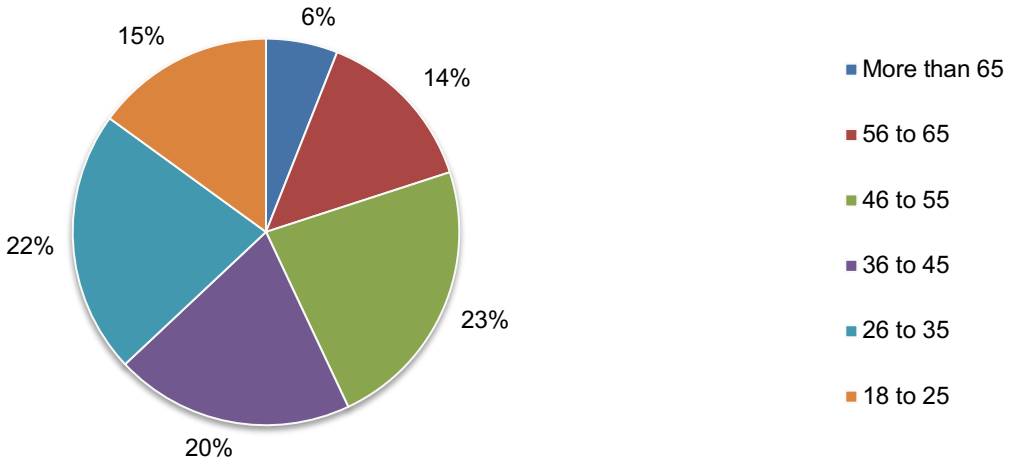
The following pie chart summarizes the gender of respondents. Fifty percent of respondents are female and 48 percent of respondents are male.

Pie Chart 1. Gender of respondents



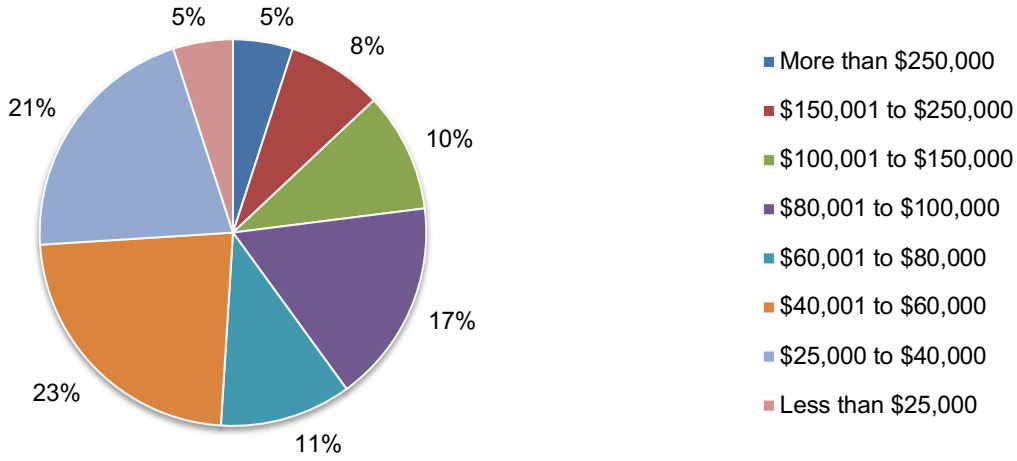
More than half (57 percent) of respondents are between the ages of 18 and 45, and 43 percent of respondents are over 45 years of age.

Pie Chart 2. Age of respondents



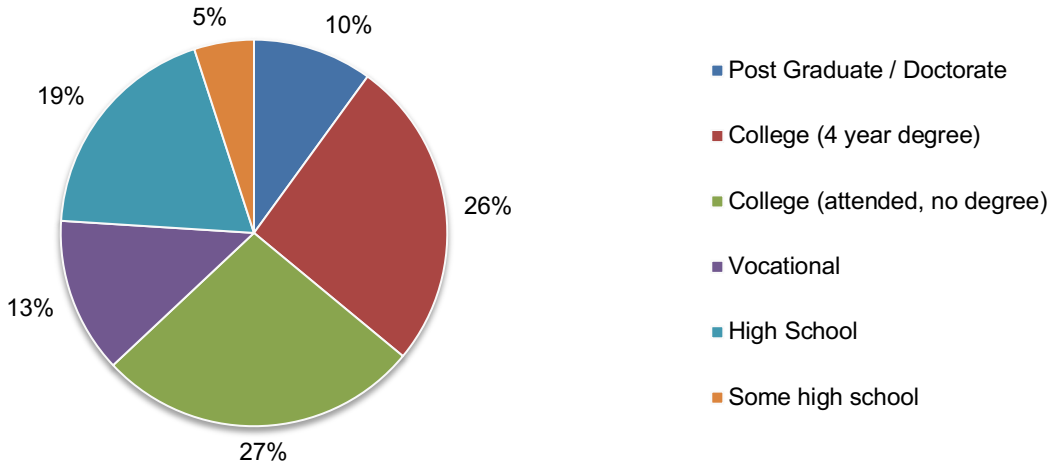
More than half (60 percent) of respondents reported their household income to be $80,0000 or less and 40 percent of respondents reported their income to be greater than $80,000.

Pie Chart 3. Household income of respondents



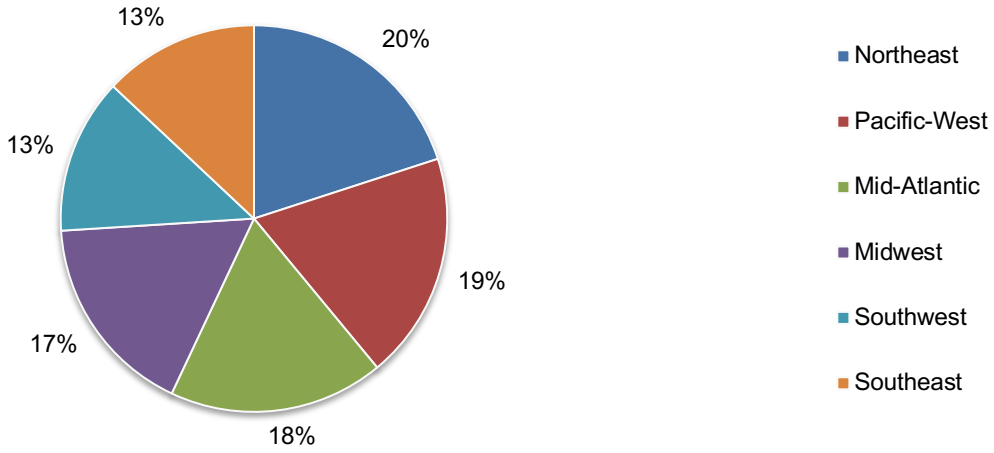
Pie Chart 4 reports the highest level of education attained by respondents. Twenty-seven percent of respondents reported having attended college, 26 percent of respondents have a 4 year college degree, 19 percent of respondents completed a high school education, 13 percent of respondents have vocational training and 10 percent of respondents have a post graduate degree.

Pie Chart 4. Highest level of education of respondents



As shown in Pie Chart 5, 20 percent of respondents are located in the Northeast, 19 percent of respondents are in the Pacific-West, 18 percent of respondents are in the Mid-Atlantic, 17 percent of respondents are in the Midwest, and 13 percent of respondents are in the Southwest and also the Southeast.

Pie Chart 5. Geographical location of respondents



Part 4. Caveats to this study

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 many consumer-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a sample of adult-aged consumers located in all regions of the United States, 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 sample is representative of individuals who are at least somewhat concerned about their online privacy. We also acknowledge that the results may be biased by external events such as media coverage at the time we fielded our survey.

  We also acknowledge bias caused by compensating respondents to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, the possibility remains that a subject did not provide accurate responses.

Appendix: Detailed Results

The following tables provide the frequency of responses to all survey questions contained in this study. All survey responses were captured in June 2020.

Survey response	Freq	Pct%
Total sampling frame	16,751	100.0%
Total returns	708	4.2%
Rejected surveys	56	0.3%
Final sample	652	3.9%

Part 1. Privacy profiles

Q1. Based on the descriptions above, what is your privacy profile **today**?	Pct%
Privacy centric	14%
Privacy sensitive	66%
Privacy complacent	20%
Total	100%

Q2. Based on the descriptions above, what was your privacy profile **three years ago**?	Pct%
Privacy centric	12%
Privacy sensitive	61%
Privacy complacent	27%
Total	100%

Q3a. Have you become more concerned about the privacy of your personal data over the past three years?	Pct%
Yes	68%
No	32%
Total	100%

Q3b. If yes, why have you become more concerned? Please select all that apply.	Pct%
I became a victim of a data breach	44%
I became a victim of identity theft	12%
I have growing concerns about government surveillance	41%
I use social media more often	56%
I am using location tracking devices more often	25%
I know someone who became a victim of a data breach	21%
I am using my mobile devices such as smartphones and tablets more often	48%
I use mobile payment methods including mobile wallet	34%
More of my personal information including medical records is being shared with third parties	27%
I became more knowledgeable about the potential threat to my digital privacy	50%
Total	388%

Part 2. Consumers' use of online devices and their concerns.
Please indicate the devices and primary platforms you have to use the Internet.

Q4a. Computer	Pct%
Yes	94%
No	6%
Total	100%

Q4b. If yes, what platform do you use?	Pct%
Mac	49%
PC	51%
Total	100%

Q5a. Tablet	Pct%
Yes	56%
No	44%
Total	100%

Q5b. If yes, what platform do you use?	Pct%
iOS	45%
Android	55%
Total	100%

Q6a. Smartphone	Pct%

Yes	67%
No	33%
Total	100%

Q6b. If yes, what platform do you use?	Pct%
iOS	61%
Android	39%
Total	100%

Q7a. Smart speakers	Pct%
Yes	32%
No	68%
Total	100%

Q7b. If yes, what platform do you use?	Pct%
Amazon Alexa	52%
Google Assistant	48%
Total	100%

Q8a. Smart watches	Pct%
Yes	21%
No	79%
Total	100%

Q8b. If yes, what platform do you use?	Pct%
Apple Watch	50%
Fitbit	35%
Other (please specify)	15%
Total	100%

Q9. What personal information do you believe is collected by the devices you use? Please check all that apply.	Pct%
Browser settings & histories	90%
Credit history	44%
Email address	96%
Health condition	31%
Hobbies, tastes & preferences	45%
Home address	19%
Marital status	21%
Name	54%
Names of friends & family members	20%
Payment account details	78%
Phone numbers	53%
Photos & videos	78%
Physical location (GPS)	54%
Purchase histories	47%
Social Security number	12%
Special dates, including date of birth	25%
Gender	46%
School or employer	29%

Q10. Listed below are common concerns if personal information is lost, stolen or wrongfully acquired by outside parties. Please check the top two concerns that you would have if your personal information was lost or stolen.	Pct%
Identity theft	54%
Stalking or spying	17%
Marketing abuses	25%
Loss of civil liberties	56%
Embarrassment because of the revealing personal secrets	15%
Inadvertent exposure of private information	33%
Total	200%

Q11. How concerned are you about protecting your **privacy** when you are using your devices? Please use the 10-point scale provided below. 1 = not concerned to 10 = very concerned.	Pct%
1 or 2	7%
3 or 4	9%
5 or 6	15%
7 or 8	26%
9 or 10	43%
Total	100%
Extrapolated value	7.28

Q12. How concerned are you about the **privacy** of your personal data when using free online tools (such as Facebook and Google)? Please use the 10-point scale provided below. 1 = not concerned to 10 = very concerned.	Pct%
1 or 2	2%
3 or 4	2%
5 or 6	10%
7 or 8	39%
9 or 10	47%
Total	100%
Extrapolated value	8.04

Q13. How concerned are you when shopping online or using online services (e.g. ride sharing, food delivery, etc.)? Please use the 10-point scale provided below. 1 = not concerned to 10 = very concerned.	Pct%
1 or 2	7%
3 or 4	9%
5 or 6	18%
7 or 8	28%
9 or 10	38%
Total	100%
Extrapolated value	7.12

Part 3. Trust in the use of online sites	
Q14. After browsing websites and/or making online purchases, do you believe you have control over how your personal data will be used?	Pct%
Yes, most of the time	11%
Yes, some of the time	15%
Rarely	24%
No	50%
Total	100%

Q15. Do you consciously try to limit providing personal data when using online services?	Pct%
Yes, all online services	19%
Yes, some of the online services	27%
No	54%
Total	100%

Q16. What types of online sites do you trust the least? Please select your top three choices only.	Pct%
Banking	12%
Shopping	52%
Healthcare/medical	36%
Airlines/hotels	15%
Music	9%
Movies/cable	12%
Gaming	30%
Ride sharing	29%
Food delivery	16%
Social media	61%
Fitness tracking	23%
Other (please specify)	5%
Total	300%

Q17. Where do you have the most trust when doing online shopping, banking and other financial activities online? Please select only one choice.	Pct%
Home	46%
Work	23%
Public WiFi	10%
Phone Internet	21%
Total	100%

Q18. Do you know if online sites are required to provide the data that they have about you if you were to request it?	Pct%
Yes	44%
No	56%
Total	100%

Q19. Are you aware that most online sites are also required to delete your personal data at your request?	Pct%
Yes,	42%
No	58%
Total	100%

Q20. Should online sites require you to explicitly opt-in to using or sharing/selling your personal data before you are able to use their service?	Pct%
Yes	70%
No	30%
Total	100%

4. Perceptions about how third parties and advertisers use information not directly provided by consumers	
Q21a. Have you received online ads that are relevant but not based on your online search behavior or publicly available information?	Pct%
Yes, it happens frequently	41%
Yes, but it happens only rarely	25%
No, I don't receive such online ads	31%
Unsure	3%
Total	100%

Q21b. If yes, do you think it is "creepy" when this happens?	Pct%
Yes	64%
No	30%
Unsure	6%
Total	100%

Q22. Do you believe that the types of websites listed below share or sell your personal data? Percentage Yes response.	Pct%
Banking	38%
Entertainment & gaming	60%
Investments	35%
News sites	52%
Shopping	63%
Search engines	92%
Social media	78%
Tech & software	54%
Travel sites	59%

Please rate the following statements using the agreement scale provided below each item. **Strongly Agree and Agree response combined.**	Pct%
Q23. Advertisers should not be able to serve ads based on my conversations and messaging.	68%
Q24. Advertisers should not be allowed to build a profile of me for targeted ads unless I grant permission or opt-in.	64%
Q25. It is annoying when I continue to receive ads for products or services I am no longer interested in receiving.	57%
Q26. Advertisers should allow me to “opt-out” of receiving ads on any specific topic at any time.	73%
Q27. Advertisers should allow me to “opt-out” of receiving ads on multiple devices that I use.	62%

Part 5. Steps consumers take to protect their privacy and what needs to change	
Q28. Are you aware that your devices have privacy controls you can use to set your level of sharing your personal information?	Pct%
Yes	55%
No (please skip to Q30)	45%
Total	100%

Q29. If yes, on which devices have you reviewed these settings and updated them to enhance your privacy and/or limit data sharing? Please select all that apply.	Pct%
Computers	60%
Tablets	43%
Smartphones	56%
Smart speakers	27%
Smart watches	23%
I have not reviewed any settings	25%
Total	234%

Q30. What protections are in place to protect your personal information? Please select all that apply.	Pct%
My data is shared only with trusted parties	33%
I can turn off tracking activities anytime	27%
The device provides strong authentication controls	35%
I can remotely disable the device if it is lost or stolen	19%
I can erase any information collected about me	15%
I can opt out of data collection and/or data sharing	52%
My personal information collected is encrypted	48%
There is someone to contact if I have concerns about privacy	19%
None of the above	5%
Total	253%

Q31. Do you use any of the privacy protections provided by the devices you use? Please select only one choice.	Pct%
I use additional authentication controls	19%
I set a more restrictive data sharing setting	25%
I use both additional authentication controls and set a more restrictive data sharing setting	21%
I don't use any of the privacy protections	30%
Other (please specify)	5%
Total	100%

Q32. Do you expect the websites you access to provide you with the following privacy tools and settings? Please check all that apply.	Pct%
Limit the collection and sharing of personal information	17%
Security features are embedded in the browser	45%
Web pages utilize HTTPS	69%
Website posts a comprehensive privacy policy	47%
Website has an ad blocker that stops tracking	33%
Website is scanned for malware, spyware and other threats	53%
I am able to have my personal data deleted	39%
Website privacy and data security practices are certified	28%
Other (please specify)	3%
Total	334%

Q33. Whom do you expect is most accountable for protecting your' privacy rights when online? Please select your top two choices.	Pct%
Federal government	40%
State & local government	9%
Online service providers	54%
Advertisers	10%
Those who sell my personal information	40%
Myself	45%
Other (please specify)	2%
Total	200%

Q34. Do you believe that Big Tech companies (like Google, Twitter and Facebook, among others) will protect your privacy rights through self-regulation, or does the government need to step in and regulate these companies?	Pct%
Industry self-regulation will suffice	40%
Government oversight is required	34%
Hybrid of the two options	26%
Total	100%

Q35. Would you ever consider using/buying an online tool that would help you protect your privacy when using sites that track, share and sell your personal data?	Pct%
Yes	31%
Yes, but only if it is free	42%
No	23%
Unsure	4%
Total	100%

Part 6. Demographics

Following are variables that will be used by us to analyze results. Please note that no personally identifiable information is being collected in this survey.	
Gender:	Pct%
Female	50%
Male	48%
Rather not answer	2%
Total	100%

Age range:	Pct%
18 to 25	15%
26 to 35	22%
36 to 45	20%
46 to 55	23%
56 to 65	14%
More than 65	6%
Total	100%

Household income:	Pct%
Less than $25,000	5%
$25,000 to $40,000	21%
$40,001 to $60,000	23%
$60,001 to $80,000	11%
$80,001 to $100,000	17%
$100,001 to $150,000	10%
$150,001 to $250,000	8%
More than $250,000	5%
Total	100%
Extrapolated value	$ 89,080

Highest Level of Education:	Pct%
Some high school	5%
High School	19%
Vocational	13%
College (attended, no degree)	27%
College (4 year degree)	26%
Post Graduate / Doctorate	10%
Other	0%
Total	100%

U.S. Regional Location:	Pct%
Northeast	20%
Mid-Atlantic	18%
Midwest	17%
Southwest	13%
Southeast	13%
Pacific-West	19%
Total	100%

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.

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.