Privacy: Risk/Benefit Survey

2019 Nationally Representative Phone Survey

Prepared by CR Survey Research Department

July, 2019

Consumer Reports | Digital Lab

INTRODUCTION

In June 2019, Consumer Reports conducted a ***nationally representative survey of 1,004 U.S. adults.*** This survey focused on consumer behaviors and attitudes regarding internet-connected devices and privacy, in particular on mobile apps.

This survey was supported by the Alfred P. Sloan Foundation (sloan.org).

REPORT HIGHLIGHTS

5

PRIVACY PRACTICES
OUT OF 10
WE ASKED ABOUT

On average, Americans say they do about half of the privacy practices we asked about, such as blocking cookies on their web browser or using a password manager.

74%

USE A STRONG PASSWORD
ON HOME WIFI NETWORK

Among the most commonly used methods to protect privacy online (of those respondents for which each method was applicable) are using a strong password on your home WiFi network (74%), not using apps that collect too much personal information (71%), and requiring a password or other lock on your smartphone (69%).

34%

USE VPN
TO ACCESS INTERNET

The least common practices that people do to protect their privacy online (of those respondents for which each method was applicable) are using a password manager (36%) and using VPN to access the internet (34%).

67%

MOBILE APPS SHOULD BE
ALLOWED TO COLLECT INFO
WHEN YOU AREN'T USING APP

Two-thirds of Americans think that mobile apps should be allowed to collect personal information from you, even when you aren't currently using the app.

90%

OF THOSE WHO THINK APPS CAN
COLLECT INFO SAY THEY NEED
PERMISSION FIRST

Nine in 10 of those who think apps should be allowed to collect personal information about you even when you aren't currently using the app think this is okay only if the app gets your permission.

62%

RISKS OUTWEIGH BENEFITS
WHEN SHARING EMAIL ADDRESS

The types of information that Americans feel risks tend to outweigh benefits most when they are shared online are their email address, access to their camera and photos, and their location information (at least six out of 10 Americans think risks outweigh benefits).

41%

BENEFITS OUTWEIGH RISKS
WHEN SHARING
SMART TV HISTORY

Four in 10 Americans think benefits outweigh the risks when sharing their smart TV watch history. When it comes to sharing their browsing and search engine history, although many believe the risks outweigh the benefits, more than half of Americans feel that the benefits exceed or are equal to the risks.

FINDINGS

Most Americans use the internet, at least occasionally (84%). ***More than three-quarters of Americans have an internet-connected smartphone***.

Actions to Protect Privacy

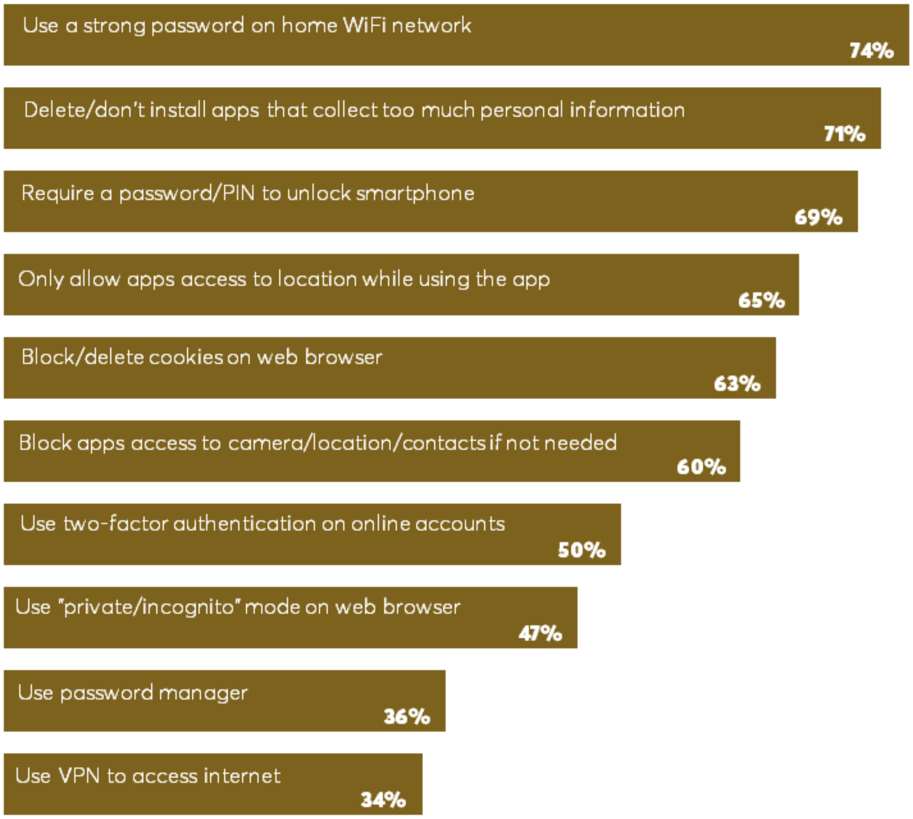
We were interested in the types of things that people do to protect their privacy or personal data when using technology. Respondents were given a list of ten practices, such as blocking cookies on their web browser or using a password manager. For each one, they were asked if it is something ***they currently do when using their personal devices*** (*respondents were told not to include practices they do only when using devices owned by an employer or solely for business purposes*).

5.1

OUT OF 10
WE ASKED ABOUT

On average, Americans say they do about half of the privacy practices we asked about. Younger individuals (aged 18 to 34) are more likely to say they do more of them (mean of 5.8 privacy practices) than older individuals (aged 55 and up; 4.3 privacy practices).

ACTIONS CONSUMERS TAKE TO PROTECT PRIVACY ONLINE



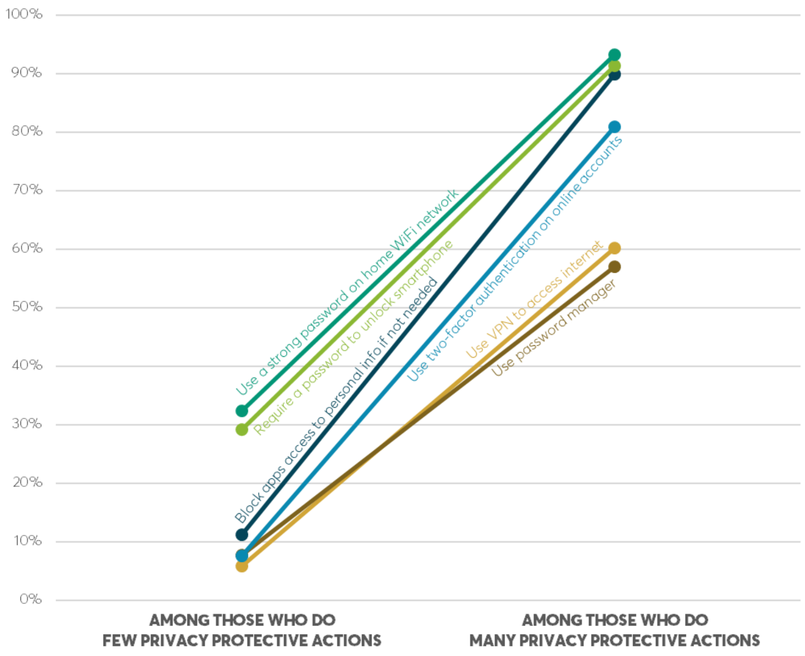
Base: All respondents, excluding those who said *'Not applicable'* or *'Don't know'*

As can be seen in the graph above:

- ***Among the most common privacy practices are:***
  - Using a strong password to access your home WiFi network (defined as at least 8 characters long, including upper and lowercase letters, numbers and symbols) (74%)
  - Deleting or choosing to not install apps on your smartphone if you think they collect too much personal information or do not protect it adequately (71%)
  - Requiring a password, PIN, or other method, such as touch or face ID, to unlock your smartphone (69%)
- ***Among the least common privacy practices are:***
  - Using a password manager that automatically creates and stores a very strong password for each of your online accounts (36%)
  - Using a "virtual private network," or VPN, to ever access the internet on your devices, for instance your laptop, smartphone, or tablet (34%)

Privacy-vigilant users set app permissions and use two factor authentication

As can be seen in the graph at the right, when comparing the group of Americans who did the least of the privacy practices we asked about to those who did the most, using a strong password on your WiFi network or having a lock set up on your smartphone are common practices consistently, just as using a password manager or VPN are more rare practices across the board.



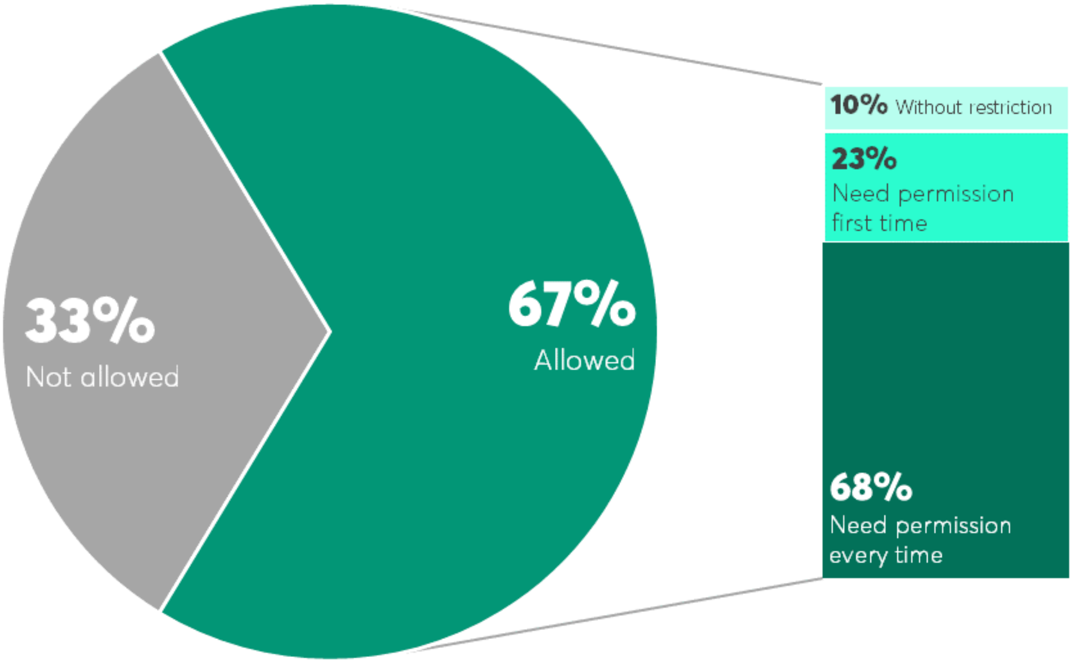
Protective action groups were created from the total number of items for which the respondent said they currently do. "Few" group, up to three actions; "Many" group, seven or more (out of 10).

When it comes to setting permissions for apps on their smartphone to block access to things like camera, location or contacts if they aren't needed for the app to function and using two-factor authentication, such as password plus phone verification, on any of their online accounts, we see an interesting pattern emerge when comparing the two groups. ***Despite only around half of Americans overall using either of these two methods, among the group who tends to use many practices to protect their privacy, this jumps up to over 80% who do these things.***

Data Collection on Mobile Apps

Mobile apps can collect information about you, such as your location, who your contacts are, what your battery level is, or what other apps you use. We asked Americans if they think this type of data collection should be allowed ***when you are not using the app***.

When you are not using the app,
data collection on mobile apps should be…



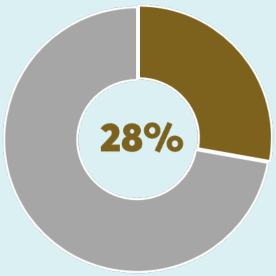
Two-thirds of Americans think that mobile apps should be allowed to collect personal information from you, even when you aren't currently using the app. However, very few of these individuals believe it should be collected without permission. When a mobile app collects information about you when you aren't using the app, **nearly seven in 10** of those who think it should be allowed only think so if the app gets your permission each time they do this.

Some groups more likely to think mobile app data collection should not be allowed

WHEN IT COMES TO MOBILE APP DATA COLLECTION THAT IS DONE WHEN THE USER IS NOT ACTIVELY USING THE APP, NOT EVERYONE IS IN AGREEMENT ABOUT WHETHER OR NOT THIS SHOULD BE ALLOWED

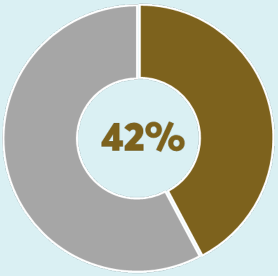
Among those aged 18 to 34:

Twenty-eight percent think this should NOT be allowed



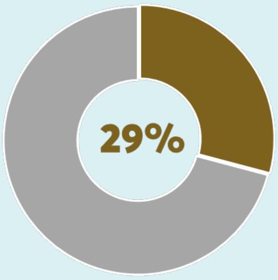
Among those aged 55 and up:

Four out of 10 think this should NOT be allowed



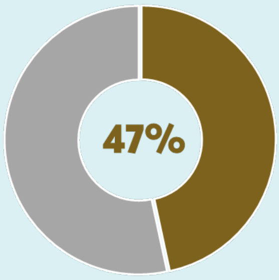
Among those who do many privacy-protective actions:

Three out of 10 think this should NOT be allowed



Among those who do few privacy-protective actions:

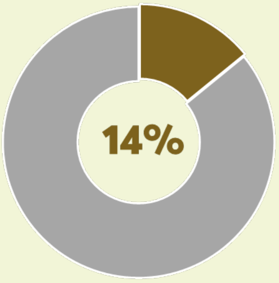
Nearly half think this should NOT be allowed



Protective action groups were created from the total number of items for which the respondent said they currently do. "Few" group, up to three actions; "Many" group, seven or more (out of 10).

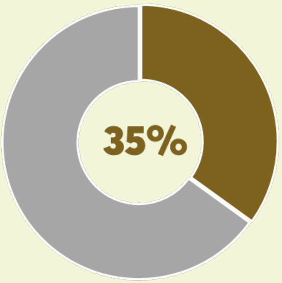
Among those who tend to think benefits outweigh risks when sharing information:

Fourteen percent think this should NOT be allowed



Among those who tend to think risks outweigh benefits when sharing information:

Over a third think this should NOT be allowed



Benefit/risk groups were created from a summary measure averaging responses across all nine scenarios presented (described in the section that follows). "Benefit" group, 1-2.74; "Risk" group, 3.26-5 (1 = Benefits strongly outweigh risks; 5 = Risks strongly outweigh benefits).

As can be seen in the charts above about mobile app data collection when the user is not using the app:

- ***Older individuals*** are more likely to say it should not be allowed than younger individuals
- People who do ***fewer of the methods we asked about to protect their privacy*** (such as using a VPN, adjusting smartphone permissions, or using private mode on their browser) tend to think it should not be allowed more than those individuals who have better control over their privacy through the use of more of these methods
- Those who ***think sharing their information online is risky*** are more likely to say it should not be allowed compared to those who think data sharing can offer convenient benefits to the user

Risks and Benefits of Sharing Personal Information

There are benefits and risks to consumers when sharing personal information in today's digital world. Sharing data about yourself and your online activities can sometimes make websites and apps feel more personalized and add convenience. But sometimes, online tracking of personal information feels too intrusive, and could have unfavorable consequences, like in the case of a data breach.

Respondents were presented with a series of scenarios presenting nine different types of information that are commonly collected about people and a potential benefit (for example, "Access to your phone's calendar is requested by a social media site. You can add events you are interested in to your calendar straight from the app."). After each scenario, we asked them to tell us if they feel the benefits outweigh the risks, or the risks outweigh the benefits when sharing each type of information.

Here are the nine scenarios that were presented to respondents:

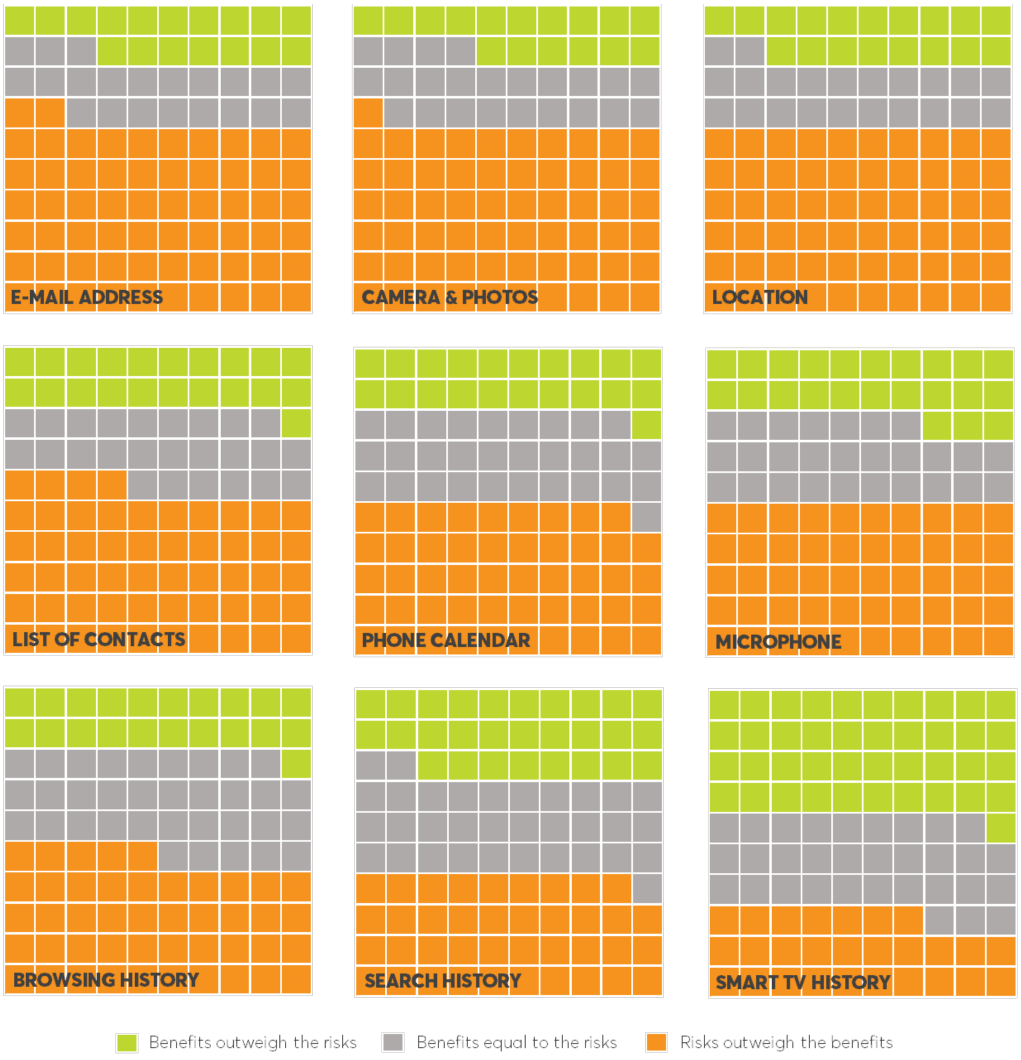
- *Your email address is required by a website before it will allow you to read an article or see other content. Your email is added to a mailing list.* (62% say risks outweigh the benefits)
- *Access to your camera and photos is requested by a shopping app. If you submit a review on a purchase, you'll be able to add photos to it from your smartphone.* (61% say risks outweigh the benefits)
- *Your location information is requested to play a game app like "Words with Friends." This allows other local players to find you when you are online.* (60% say risks outweigh the benefits)
- *Access to your list of phone contacts is requested by a navigation app. You'll be able to automatically get directions to friends' houses.* (54% say risks outweigh the benefits)
- *Access to your smartphone microphone is requested by your mobile web browser. You'll be able to submit searches using your voice.* (50% say risks outweigh the benefits)
- *Access to your phone's calendar is requested by a social media site. You can add events you are interested in to your calendar straight from the app.* (49% say risks outweigh the benefits)
- *Your browsing history of clothing websites is saved by the browser using cookies. Ads for similar stores you might be interested in pop up on your web browser.* (45% say risks outweigh the benefits)
- *What you have typed into a search engine, such as researching an illness online, is saved by the search engine. Afterwards, you receive ads for doctors or treatments you may find useful in your web browser.* (39% say risks outweigh the benefits)
- *What you've watched on your smart TV is saved. The next time you go to watch TV, there are recommended shows and movies for you.* (27% say risks outweigh the benefits)

The types of information that Americans feel risks tend to outweigh benefits most when they are shared online are their ***email address, access to their camera and photos, and their location information***.

More people say the benefits associated with sharing their ***smart TV watch history*** outweigh the risks. Further, as can be seen in the graph that follows, when it comes to sharing your ***browsing*** and ***search engine history***, although many believe the risks outweigh the benefits, more than half of Americans feel that the benefits exceed or are equal to the risks.

Do the risks outweigh the benefits when sharing personal information?

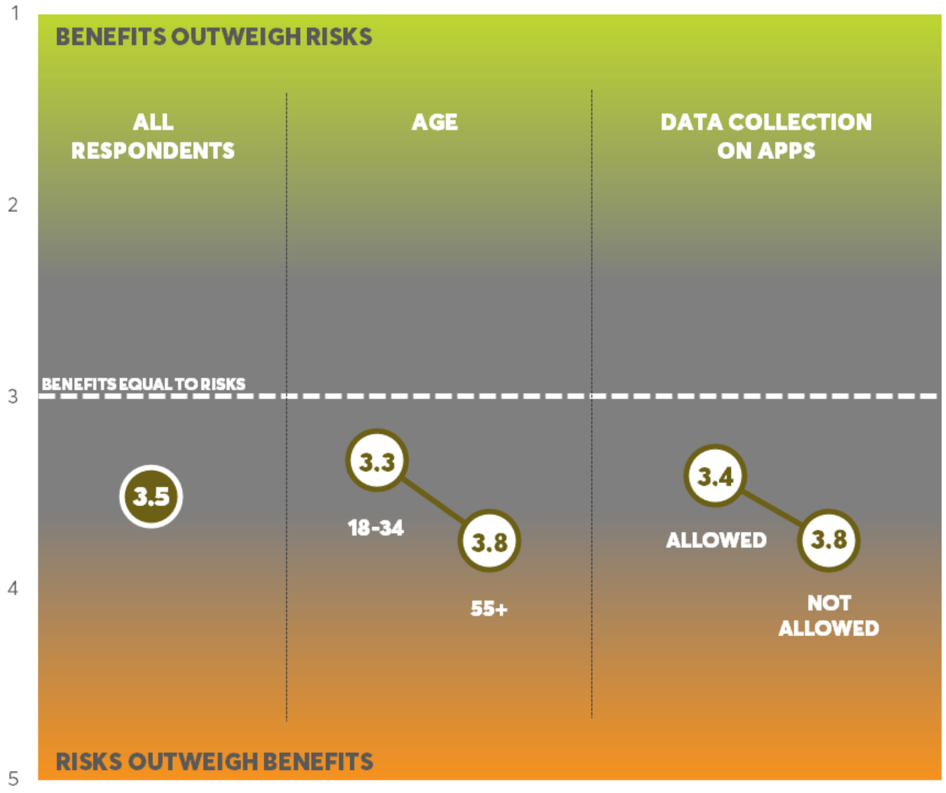
The orange cells represent Americans who think the **risks outweigh the benefits** for each type of information. ***Watch the pattern change as you move across the chart below*** – from email address (62% say risks outweigh benefits) down to smart TV history (27% say risks outweigh benefits).



The graph below shows that, overall, individuals are slightly skewed towards believing that sharing their personal information is more risky than beneficial, despite the benefits and conveniences they might gain from doing so. In other words, ***on average, people land at a 3.5 out of 5*** (where 3 represents benefits are equal to the risks, 4 represents risks somewhat outweigh the benefits, and 5 represents risks strongly outweigh the benefits). This is even more true among people aged 55 and up and those who say that mobile apps should not be allowed to collect information when you are not using the app (mean differences are statistically significant).

OVERALL FEELINGS OF RISK VS. BENEFIT WHEN SHARING INFORMATION

(Aggregated across all nine types of personal information we asked about that can be shared online)



Values represent a summary measure created by calculating the average (mean) score for each respondent across all nine scenarios presented (1 = Benefits strongly outweigh risks; 5 = Risks strongly outweigh benefits).

Base: Respondents who gave a valid answer for all nine scenarios described above.

SUMMARY

These days, there are so many ways that technology can help you out. Our web browsers give us recommendations based on things we've been searching for, we can talk directly to our phones to get them to perform a myriad of tasks for us, and important aspects of our daily lives, like our location, calendar, contacts, and photos, can be linked to many apps we use for added functionality. But what about the privacy implications of all of this? Do users feel like the benefits outweigh the risks, or the other way around? What should apps be able to do, and what do they need to get your permission for first? What kinds of things are people doing to protect themselves online?

People are concerned about giving up their privacy. They typically see the risks associated with sharing different types of information online, especially their email address, camera and photos, and location.

Interestingly, the people who take the most care to protect their privacy online, through things like using strong passwords for their WiFi network, setting up permissions on their smartphone apps, and even less common activities like using "private" mode on their browser or a VPN, are not necessarily the ones who think risks outweigh the benefits when sharing information online. Perhaps they feel that their actions mitigate their vulnerability to risk.

There are young, smartphone-using Americans who do a lot to protect their privacy online. They have come to rely on technology in their daily lives, and although they see the risks, they're used to them. They are even in favor of apps collecting their personal information, as long as the apps ask permission first. These types of users want to be in control of their online presence so they can take advantage of the benefits to be gained.

On the other hand, other individuals do very little to protect their privacy online. These individuals are more likely to want restrictions placed on what types of information mobile apps can collect about you. They would rather there be implicit regulations against these practices, and not have to personally take the time and effort learning how to adjust smartphone or browser settings, for instance.

Wherever individuals fall on the spectrum, from believing the benefits of personalized content and convenience strongly outweigh the risks when they share their information online to thinking it is just far too risky, people should know the facts about what is being collected about them and what they can do to be as safe online as possible. Any user could be vulnerable, even if they don't realize it, no matter the care they have taken to protect their privacy.

METHODOLOGY

This telephone survey was fielded by SSRS on its Omnibus survey platform using a nationally representative sample. The survey was conducted from June 18 - 23, 2019.

The SSRS Omnibus sample is designed to represent the adult U.S. population. The SSRS Omnibus uses a stratified random-digit-dialing (RDD) sample of landline telephone households, and randomly generated cell phone numbers. In total, SSRS collected 1,004 responses (969 in English; 35 in Spanish). Telephone interviews were conducted by landline (303) and cell phone (701). The margin of error for total respondents is +/-3.60% at the 95% confidence level. Smaller subgroups will have larger error margins.

The survey was conducted using a computer-assisted telephone interviewing system (CATI), which allows for computer control of questionnaire administration, automatic handling of skip pattern response editing, and range checks. Where appropriate, question order, question verbiage, and response answer choices are randomized or scales are rotated. Each unit in the sample receives as many calls as necessary in order to survey qualified respondents and to fulfill the required number of interviews within each sub-strata of the samples. Additional callback attempts follow a differential callback schedule to ensure the highest completion rate possible.

Final data is weighted by age, race, sex, region, education, and telephone type to be proportionally representative of the U.S. adult population.

Key demographic characteristics (after weighting is applied) are presented below:

- 51% female
- Median age of 46
- 63% White, non-Hispanic
- 32% 4-year college graduates
- 41% have a household income of $50,000 or more

Scale Development and Subgroup Creation

In order to compare individuals ***who do many of the privacy protective actions*** we asked about in Q1 (such as using a strong password on your home WiFi, deleting cookies on your web browser, or using a password massager for online accounts) to those ***who do few of them***, we created *Low*, *Medium*, and *High Protective Action Groups*.

To do this, we first took the sum of the total number of items for which the respondent said "Yes" in Q1 (each respondent received a score from 0 to 10). The ten items were found to have high inter-item correlations (Cronbach's alpha = 0.76), which supports their use as a scale.

Cut off points for number of protective actions were determined to make the three groups as equally sized as possible. Individuals are in the ***Low*** group if they do up to three actions, the ***Medium*** group if they do four to six actions, and the ***High*** group if they do 7 or more actions (out of 10).

The table that follows shows the percentage of respondents in each of the three groups, along with the mean number of actions taken by those in each group.

	Protective Action Group		
	Low	**Medium**	**High**
Percentage of sample in each group	28%	35%	37%
Mean total number of protective actions taken *(out of 10)*	*1.24*	*5.17*	*8.04*

We also wanted to be able to compare people ***who tend to think benefits outweigh risks*** when sharing personal information online to those ***who tend to think risks outweigh benefits***. Three groups were created based on responses to the nine scenarios in Q3. Respondents who answered all nine of these items were given a score. This score is also used to summarize respondents' opinions about sharing data in general across the nine different types of information we asked about.

For each item, respondents received 1 to 5 points, where "benefits strongly outweigh risks" is 1 and "risks strongly outweigh benefits" is 5. The responses to the nine items were averaged for a scale score that ranges from 1 to 5 (low indicates tendency to think data sharing is beneficial; high indicates tendency to think data sharing is risky). Responses to the nine scenarios had high inter-item correlations (Cronbach's alpha = 0.81), which supports their use as a scale.

Individuals are in the ***Benefit*** group if they scored under 2.75, in the ***Neutral*** group if they scored from 2.75 to 3.25, and in the ***Risk*** group if they scored above 3.25. These categories result in unevenly sized, but meaningful, groups based on the cut off points.

The table below shows the percentage of respondents in each of the three groups, along with the mean score for those in each group.

	Benefit/Risk Group		
	Benefit	**Neutral**	**Risk**
Percentage of sample in each group	14%	28%	58%
Scale score *(1 = benefits strongly outweigh risks;* *5 = risks strongly outweigh benefits)*	*2.32*	*3.01*	*4.05*