March 16, 2015

Americans' Privacy Strategies Post-Snowden

Some are shifting their basic behaviors with technology, but few are making big changes using sophisticated tools. Many are not aware of the advanced strategies they could use to help them be more private – and others have just not considered those options.

FOR FURTHER INFORMATION ON THIS REPORT:

Lee Rainie, Director Internet, Science, and Technology Research

Mary Madden, Senior Researcher

202.419.4372

www.pewresearch.org

RECOMMENDED CITATION: Shelton, Martin, Lee Rainie; Mary Madden. Pew Research Center, March 15, "Americans' Privacy Strategies Post-Snowden." Available at: http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/

About this Report

This report is the second in a series of studies that examine Americans' digital privacy-related perceptions and behaviors, following the ongoing revelations of government surveillance activities introduced in 2013 by the ex-National Security Agency contractor Edward Snowden. To examine this topic in depth and over an extended period of time, Pew Research Center, Science and Technology research project conducted a survey of a representative online panel of 475 adults who are members of the GfK Knowledge Panel. These panelists have agreed to respond to four surveys over the course of one year. The findings in this report are based on a survey which was conducted in English and fielded online between November 26, 2014 and January 3, 2015. In addition, a total of 59 panelists also participated in one of six online focus groups as part of this study during December 2014 and January 2015.

This report is a collaborative effort based on the input and analysis of the following individuals:

Martin Shelton, *Research Consultant*
Lee Rainie, *Director Internet, Science and Technology Research*
Mary Madden, *Senior Researcher*
Monica Anderson, *Research Analyst*
Maeve Duggan, *Research Analyst*
Andrew Perrin, *Research Assistant*
Dana Page, *Communications Manager*

Other reports from Pew Research Center project on the topic of privacy and security online can be found at:

http://www.pewinternet.org/topics/privacy-and-safety/pages/2/

About the Pew Research Center

Pew Research Center is a nonpartisan fact tank that informs the public about the issues, attitudes and trends shaping America and the world. It does not take policy positions. It conducts public opinion polling, demographic research, media content analysis and other empirical social science research. The center studies U.S. politics and policy views; media and journalism; internet and technology; religion and public life; Hispanic trends; global attitudes and U.S. social and demographic trends. All of the center's reports are available at http://www.pewresearch.org. Pew Research Center is a subsidiary of The Pew Charitable Trusts.

© Pew Research Center 2015

Summary of Findings

It has been nearly two years since the first disclosures of government surveillance programs by former National Security Agency contractor Edward Snowden and Americans are still coming to terms with how they feel about the programs and how to live in light of them. The documents leaked by Snowden revealed an array of activities in dozens of intelligence programs that collected data from large American technology companies, as well as the bulk collection of phone "metadata" from telecommunications companies that officials say are important to protecting national security. The metadata includes information about who phone users call, when they call, and for how long. The documents further detail the collection of Web traffic around the globe, and efforts to break the security of mobile phones and Web infrastructure.

A new survey by the Pew Research Center asked American adults what they think of the programs, the way they are run and monitored, and whether they have altered their communication habits and online activities since learning about the details of the surveillance. The notable findings in this survey fall into two broad categories: 1) the ways people have personally responded in light of their awareness of the government surveillance programs and 2) their views about the way the programs are run and the people who should be targeted by government surveillance.

Some people have changed their behaviors in response to surveillance

Overall, nearly nine-in-ten respondents say they have heard at least a bit about the government surveillance programs to monitor phone use and internet use. Some 31% say they have heard a lot about the government surveillance programs and another 56% say they had heard a little. Just 6% suggested that they have heard "nothing at all" about the programs. The 87% of those who had heard at least something about the programs were asked follow-up questions about their own behaviors and privacy strategies:

34% of those who are aware of the surveillance programs (30% of all adults) have taken at least one step to hide or shield their information from the government. For instance, 17% changed their privacy settings on social media; 15% use social media less often; 15% have avoided certain apps and 13% have uninstalled apps; 14% say they speak more in person instead of communicating online or on the phone; and 13% have avoided using certain terms in online communications.

Those most likely to have taken these steps include adults who have heard "a lot" about the surveillance programs and those who say they have become less confident in recent months that the programs are in the public interest. Younger adults under the age of 50 are more likely than

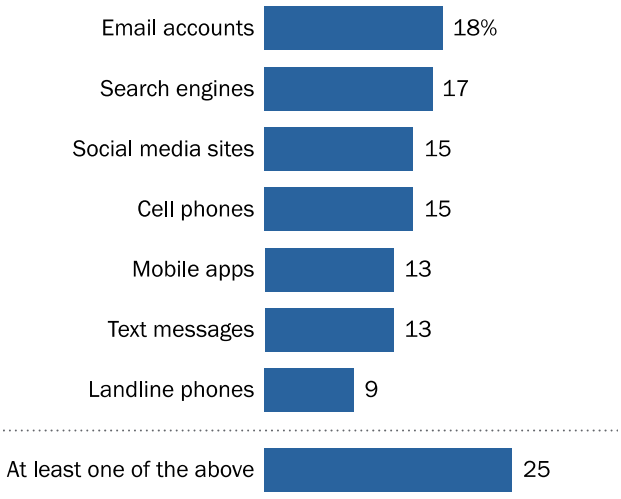
those ages 50 and older to have changed at least one of these behaviors (40% vs. 27%). There are no notable differences by political partisanship when it comes to these behavior changes.

25% of those who are aware of the surveillance programs (22% of all adults) say they have changed the patterns of their own use of various technological platforms "a great deal" or "somewhat" since the Snowden revelations. For instance, 18% say they have changed the way they use email "a great deal" or "somewhat"; 17% have changed the way they use search engines; 15% say they have changed the way they use social media sites such as Twitter and Facebook; and 15% have changed the way they use their cell phones.

Those who are more likely to have changed at least one of their behaviors include the people who have heard a lot about government surveillance (38% say they have changed a great deal/somewhat in at least one of these activities), those who are at least somewhat concerned about the programs (41% have changed at least one activity), and those who are concerned about government monitoring of their use of social media, search engines, cell phones, apps, and email.

Surveillance Programs Prompt Some to Change the Way They Use Technology

Among the 87% of U.S. adults who have heard of the government surveillance programs, the percentage who have changed their use of ... "a great deal" or "somewhat"



Source: Survey of 475 adults on GfK panel November 26, 2014-January 3, 2015.

PEW RESEARCH CENTER

There are no partisan differences when it comes to those who have changed their use of various technologies.

Additionally, a notable share of Americans have taken specific technical steps to assert some control over their privacy and security, though most of them have done just simple things. For instance, 25% of those who are aware of the surveillance programs are using more complex passwords.

Many have not considered or are not aware of some of the more commonly available tools that could make their communications and activities more private

One potential reason some have not changed their behaviors is that 54% believe it would be "somewhat" or "very" difficult to find tools and strategies that would help them be more private online and in using their cell phones. Still, notable numbers of citizens say they have not adopted or even considered some of the more commonly available tools that can be used to make online communications and activities more private:

- 53% have not adopted or considered using a search engine that doesn't keep track of a user's search history and another 13% do not know about these tools.
- 46% have not adopted or considered using email encryption programs such as Pretty Good Privacy (PGP) and another 31% do not know about such programs.
- 43% have not adopted or considered adding privacy-enhancing browser plug-ins like DoNotTrackMe (now known as Blur) or Privacy Badger and another 31% do not know such plug-ins.
- 41% have not adopted or considered using proxy servers that can help them avoid surveillance and another 33% do not know about this.
- 40% have not adopted or considered using anonymity software such as Tor and another 39% do not know about what that is.

These figures may in fact understate the lack of awareness among Americans because noteworthy numbers of respondents answered "not applicable to me" on these questions even though virtually all of them are internet and cell phone users.

The public has divided sentiments about the surveillance programs

This survey asked the 87% of respondents who had heard about the surveillance programs: "As you have watched the developments in news stories about government monitoring programs over recent months, would you say that you have become more confident or less confident that the programs are serving the public interest?" Some 61% of them say they have become less confident the surveillance efforts are serving the public interest after they have watched news and other developments in recent months and 37% say they have become more confident the programs serve the public interest. Republicans and those leaning Republican are more likely than Democrats and those leaning Democratic to say they are losing confidence (70% vs. 55%).

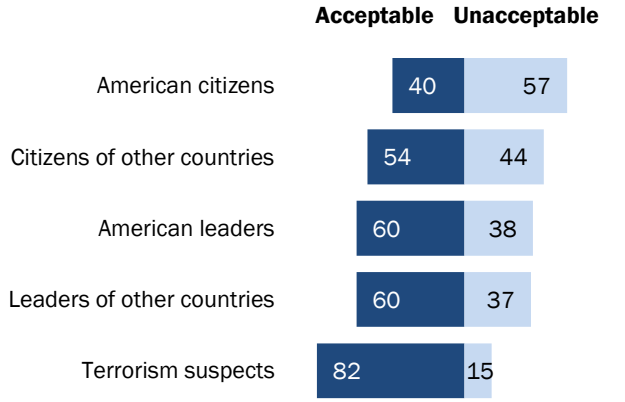
Moreover, there is a striking divide among citizens over whether the courts are doing a good job balancing the needs of law enforcement and intelligence agencies with citizens' right to privacy: 48% say courts and judges are balancing those interests, while 49% say they are not.

At the same time, the public generally believes it is acceptable for the government to monitor many others, including foreign citizens, foreign leaders, and American leaders:

- 82% say it is acceptable to monitor communications of suspected terrorists
- 60% believe it is acceptable to monitor the communications of American leaders.
- 60% think it is okay to monitor the communications of foreign leaders
- 54% say it is acceptable to monitor communications from foreign citizens

Most Americans Believe It Is Acceptable to Monitor Others, Except U.S. Citizens

% of U.S. adults who say it is acceptable or unacceptable for the American government to monitor communications from ...



Source: Survey of 475 adults on GfK panel November 26, 2014-January 3, 2015.

PEW RESEARCH CENTER

Yet, 57% say it is *unacceptable* for the government to monitor the communications of U.S. citizens. At the same time, majorities support monitoring of those particular individuals who use words like "explosives" and "automatic weapons" in their search engine queries (65% say that) and those who visit anti-American websites (67% say that).

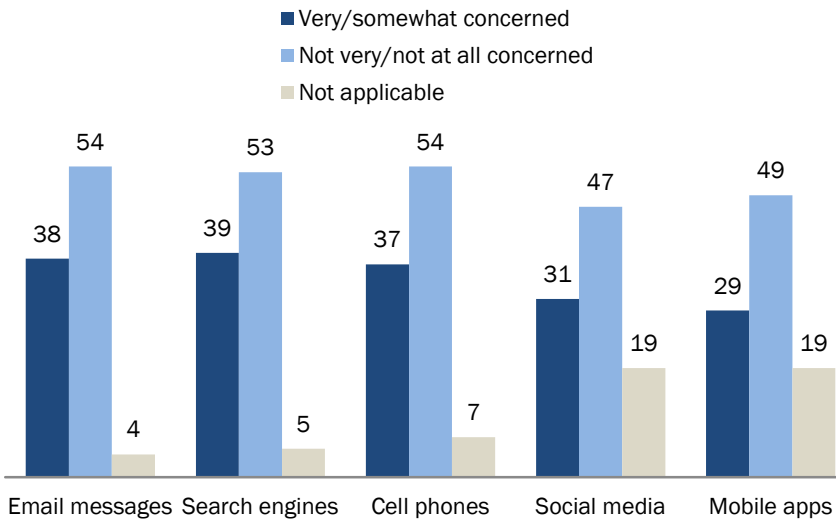
Americans are split when it comes to being concerned about surveillance programs

Overall, 52% describe themselves as "very concerned" or "somewhat concerned" about government surveillance of Americans' data and electronic communications, compared with 46% who describe themselves as "not very concerned" or "not at all concerned" about the surveillance. When asked about more specific areas of concern over their *own* communications and online activities, respondents expressed somewhat lower levels of concern about electronic surveillance in various parts of their digital lives:

- 39% describe themselves as "very concerned" or "somewhat concerned" about government monitoring of their activity on search engines.
- 38% say they are "very concerned" or "somewhat concerned" about government monitoring of their activity on their email messages.
- 37% express concern about government monitoring of their activity on their cell phone.
- 31% are concerned about government monitoring of their activity on social media sites, such as Facebook or Twitter.
- 29% say they are concerned about government monitoring of their activity on their mobile apps.

Americans Have More Muted Concerns about Government Monitoring of their Own Digital Behavior

% of U.S. adults who say they are "very/somewhat" or "not very/not at all concerned" about government surveillance of their own data and electronic communications



Source: Survey of 475 U.S. adults on GfK panel November 26, 2014-January 3, 2015.,

PEW RESEARCH CENTER

More about this survey

The analysis in this report is based on a Pew Research Center survey conducted between November 26, 2014 and January 3, 2015 among a sample of 475 adults, 18 years of age or older. The survey was conducted by the GfK Group using KnowledgePanel, its nationally representative online research panel. GfK selected a representative sample of 1,537 English-speaking panelists to invite to join the subpanel and take the first survey in the fall of 2014. Of the 935 panelists who responded to the invitation (60.8%), 607 agreed to join the subpanel and subsequently completed the first survey (64.9%) whose results were reported in November 2014. This group has agreed to take four online surveys about "current issues, some of which relate to technology" over the course of a year and possibly participate in one or more 45-60-minute online focus group chat sessions. For the third survey whose results are reported here, 475 of the original 607 panelists participated. A random subset of the subpanel receive occasional invitations to participate in online focus groups. For this report, a total of 59 panelists participated in one of six online focus groups

conducted during December 2014 and January 2015. Sampling error for the total sample of 475 respondents is plus or minus 5.6 percentage points at the 95% level of confidence.

For more information on the GfK Privacy Panel, please see the Methods section at the end of this report.

Introduction

Edward Snowden's release of internal National Security Agency documents in June 2013 has catapulted government surveillance issues and privacy policy questions to a new level of national and scholarly discourse.

The documents Snowden leaked about the NSA suggest that large American information technology companies are compelled to share data with the government about foreign individuals as part of a program called PRISM. Data about Americans' use of communications and search engine tools may be collected "incidentally" when related to foreign intelligence. Under the same authority, the government can tap directly in to fiber optic cable networks that transfer data about virtually everything a user does on the Web and other internet-based platforms.

The NSA's documents also showed that American phone companies are required to provide the government with citizens' phone records on a daily basis. The NSA and its British equivalent, the Global Communications Headquarters, can collect identifying data about a phone's user through mobile apps, including age, gender, location, and other information.

The Western intelligence agencies have argued in courts that bulk collection programs including data about Americans are crucial to its national security efforts. Still, the Privacy and Civil Liberties Oversight Board, an independent panel appointed by the White House, suggested that bulk surveillance did not help prevent any attacks in the United States, and recommended discontinuing bulk collection of American phone metadata.

A recent report from the Pew Research Center showed that the American public is concerned about surveillance by government and businesses and lacks confidence in the security of their information on several key communications channels. Partly in response to concerns like these, President Obama has promised reform to limit the collection of American communications, and that of foreign individuals unrelated to a terrorist investigation.

At the policy and scholarly level, the Snowden leaks have become a touchstone for debate about the role of "big data" in modern society, the legality and ethics of bulk surveillance and how to consider what people's electronic records say about who they are. At the same time, civil liberties and human rights groups have been arguing that electronic surveillance chills speech, driving some journalists, writers, law professionals, and ordinary citizens to self-censor their digital communications instead of speaking openly. A recent Pew Research Center survey of investigative reporters showed that some report they have changed their engagement with their sources and their use of technology in light of the Snowden disclosures.

The ongoing public dialogue about surveillance comes alongside a growing awareness of large-scale breaches of consumer data. The earlier research from the Pew Research Center found that 91% of American adults "agree" or "strongly agree" that they have lost control over how their information is collected and used by companies. While Americans value their personal privacy, they often feel ill-equipped to take steps to manage their personal data. When they want to have online anonymity, only 24%"agree" or "strongly agree" with the statement, "it is easy for me to be anonymous when I am online." And some 61% say they "would like to do more" to manage their personal information online. In a climate of growing awareness of surveillance, we set out to examine what privacy strategies Americans have been adopting since learning of the Snowden disclosures.

To continue exploration of these and other surveillance-related issues, Pew Research created an online panel of adults who agreed to respond to four surveys and participate in focus groups related to digital privacy over the span of one year. In this survey, we find there are often serious fissures in the public about the way the surveillance programs work and how they are overseen. At the same time, a number of adults have been taking some simple steps to manage their digital privacy online and by using communication channels that they perceive are more secure. However, despite widespread concern about their privacy, many are not aware of a variety of tools that would help to secure their personal data and communications.

Americans' Views on Government Surveillance Programs

Most are familiar with U.S. surveillance programs

The vast majority of Americans in this survey say they have heard about the surveillance programs to collect information about telephone calls, emails, and other online communications as part of the government's efforts to monitor terrorist activity. Overall, 31% have heard a lot about government surveillance of telephone calls, emails, and other online communications as part of efforts to monitor terrorist activity, and another 56% have heard "a little."

Men (37%) are more likely than women (26%) to have heard "a lot" about the NSA revelations. College graduates (40%) are also more likely than those who have a high school degree (25%) to have heard a lot about government surveillance. Both of these demographic trends echo findings from the first survey in this series. However, when considering other demographics, this issue was likely to be familiar to many Americans in comparable numbers.

Many of the questions in this survey about behavior change were asked of the 87% of respondents who said they were aware of the programs and an analysis of their answers is in the section following this one.

Americans are divided in their concerns about government surveillance of digital communications

In this survey, 17% of Americans said they are "very concerned" about government surveillance of Americans' data and electronic communication; 35% say they are "somewhat concerned"; 33% say they are "not very concerned" and 13% say they are "not at all" concerned about the surveillance. Those who are more likely than others to say they are very concerned include those who say they have heard a lot about the surveillance efforts (34% express strong concern) and men (21% are very concerned).

When asked about more specific points of concern over their *own* communications and online activities, respondents expressed somewhat lower levels of concern about electronic surveillance in various parts of their digital lives:

- 39% say they are "very concerned" or "somewhat concerned" about government monitoring of their activity on search engines.
- 38% say they are "very concerned" or "somewhat concerned" about government monitoring of their activity on their email messages.
- 37% express concern about government monitoring of their activity on their cell phone.

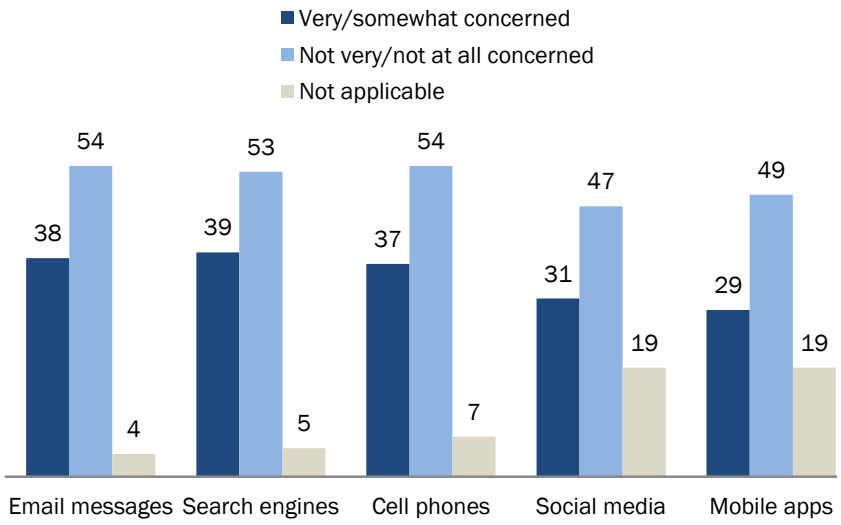
- 31% are concerned about government monitoring of their activity on social media sites, such as Facebook or Twitter.
- 29% say they are concerned about government monitoring of their activity on their mobile apps.

In addition, notable numbers of respondents said that some of these questions were not applicable to them.

In general, men are more likely than women to say that they are "very concerned" about government surveillance of Americans' data and electronic communications (21% vs. 12%). Men are also more likely than women to be "very concerned" about surveillance over their *own* activities on mobile apps and search engines.

Americans Have More Muted Concerns about Government Monitoring of their Own Digital Behavior

% of U.S. adults who say they are "very/somewhat" or "not very/not at all concerned" about government surveillance of their own data and electronic communications



Source: Survey of 475 U.S. adults on GfK panel November 26, 2014-January 3, 2015.,

PEW RESEARCH CENTER

When asked to elaborate on their concerns, many survey respondents were critical of the programs, frequently referring to privacy concerns and their personal rights.

Q: Could you please explain briefly why you have this level of concern about government surveillance of Americans' personal data and electronic communications?

"Every citizen should have the right to their own privacy inside there [sic] own homes and who they talk with. I feel this gives the government too much control."

"The fourth [amendment] originally enforced the idea that each man's home is his castle, secure from unreasonable search and seizure by the government."

"What happened to privacy?"

At the same time, others suggested that the programs could be helpful for prevention of criminal activity and terrorism, and they are not personally concerned because they have "nothing to hide":

"Law-abiding citizens have nothing to hide and should not be concerned."

"I am not doing anything wrong so they can monitor me all they want."

"Small price to pay for maintaining our safe environment from terrorist activities."

References to "terror" or "terrorism" also appeared in many of the open-ended responses, and others pointed to conflicts between personal privacy, individual rights, and national security:

"If in the event I do something unacceptable to the government or country, they have the right to investigate me. Otherwise they are taking away my privacy as an American citizen."

"Monitoring is okay for potential suspects but not every American."

A majority say they are losing confidence that the public interest is being served by the surveillance programs

Those who are aware of the government surveillance programs say they are becoming increasingly skeptical of U.S. surveillance programs. The 87% of the respondents who say they have heard of the programs were asked, "As you have watched the developments in news stories about government monitoring programs over recent months, would you say that you have become more confident or less confident that the programs are serving the public interest?" Some 61% of these respondents said they were less confident and 37% said they were more confident.

Those more likely than others to say they are less confident include those very/somewhat concerned about government surveillance (80%) and those who have heard a lot about the surveillance programs (71%). In addition, those who say they are less confident include those who say they are very/somewhat concerned about government monitoring of their activities on social media, search engines, mobile apps, cell phones, and email.

Republicans and those leaning Republican are more likely than Democrats and Democratic leaners to say they are losing confidence (70% vs. 55%).

The public is evenly split about the capacity of the judicial system to balance privacy rights with intelligence agency and law enforcement needs

Many Americans are split on the effectiveness of the judicial system in balancing privacy and national security. Some 48% agree and 49% disagree when asked if they think "the courts and judges do a good job balancing the public's right to privacy with the needs of law enforcement and intelligence agencies to collect information for investigations."

Those who are more likely to say they agree the courts are striking an appropriate balance include: those who have heard only a little about the surveillance programs (56%), those who are not very/not at all concerned about the programs (63%), and those whose confidence in the surveillance programs has grown over time (83%).

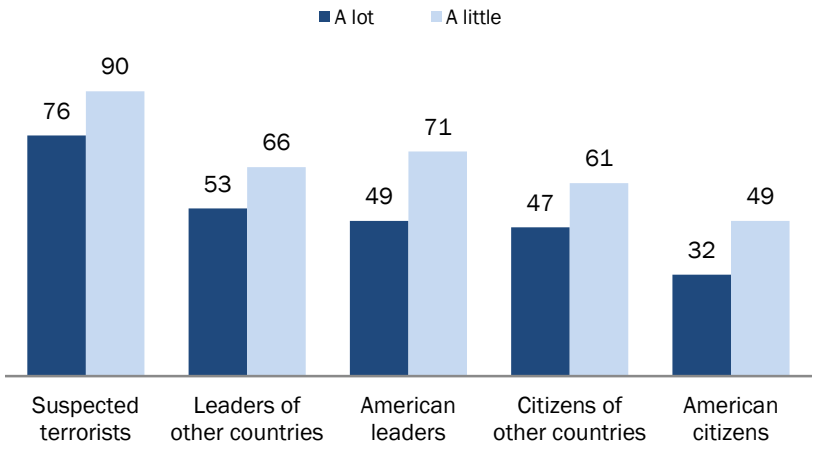
However, there are no notable partisan differences on this question.

Americans are comfortable targeting others for surveillance, but not themselves

Even as they express some concern about the reach of government surveillance programs, majorities of Americans think such monitoring is acceptable in certain instances, as long as the targets are not average Americans. Those in positions of power are not seen as exempt; for instance, 60% of all adults say it is acceptable for the American government to monitor communications from America's leaders. Here is the breakdown:

Those Who Have Heard a Lot about Surveillance Programs Are Less Likely to Support Monitoring Others

Among those who have heard "a lot" or "a little" about gov't surveillance programs, the % who say it is acceptable to monitor the communications of ...



Source: Survey of 475 U.S. adults on GfK panel November 26-2014-January 3, 2015.

PEW RESEARCH CENTER

- 82% say it is acceptable to monitor communications of suspected terrorists
- 60% believe it is acceptable to monitor the communications of American leaders.
- 60% think it is okay to monitor the communications of foreign leaders

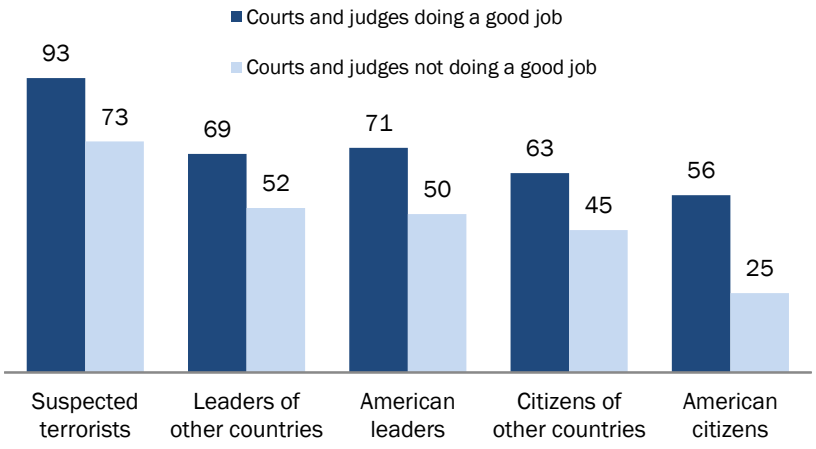
- 54% say it is acceptable to monitor communications from foreign citizens

At the same time, only a minority of Americans — 40% — feel it is acceptable to monitor ordinary American citizens. Some 57% say it is unacceptable for the government to monitor their communications.

There are several consistent patterns in people's answers to these questions: Those who have heard a lot about the government surveillance programs are *less likely* than others to feel that monitoring others, including terrorists, is acceptable. Similarly, those who are concerned about the surveillance programs are less likely to feel that monitoring others is acceptable. And younger adults under the age of 50 are less likely than their elders to think monitoring others is acceptable.

Those Who Think the Judicial System is Doing a Good Job Balancing People's Privacy Rights with Law Enforcement Needs Are More Likely to Support Monitoring Others

Among those who think the courts and judges are doing a good job/not a good job, the % who say it is acceptable for the American gov't to monitor the communications of …



Source: Survey of 475 U.S. adults on GfK panel November 26-2014-January 3, 2015.

PEW RESEARCH CENTER

At the same time, those who are more confident that the public interest is being served by these surveillance programs are also more likely to think it is acceptable to monitor others. And those who think the courts and judges are doing a good job balancing the interests of intelligence agencies and law enforcement are also more likely to support monitoring others.

Interestingly, there are no statistically meaningful partisan differences in answers to these questions about which kinds of individuals are acceptable to monitor.

Many think it is acceptable to monitor others in a variety of other situations

In specific circumstances, Americans also generally support the use of surveillance to investigate criminal activity, as well as circumstances when a person's digital activity may cause some

suspicion of potential involvement with terrorism or violent acts. These respondents are split on a number of causes for suspicion, including unusual bank withdrawals, the use of encryption to hide software, and situations where individuals are connected to social media users used hateful language about American leaders.

- 77% of adults believe it is acceptable for the government to monitor communications of a U.S. citizen when the person has visited a child pornography website.
- 68% believe it is okay to monitor someone who exchanged emails with an imam who preached against infidels.
- 67% back the idea that the government can monitor a person has visited websites connected to known anti-American groups.
- 65% believe it is acceptable to monitor a person who made search engine queries for keywords related to explosives and automatic weapons.
- 51% support the idea of monitoring individuals reported by their bank for making unusual withdrawals.
- 49% believe it is okay to monitor a person who used encryption software to hide files.
- 49% think it is acceptable to monitor a person who had friends or followers on social media who used hateful language about American leaders.

Americans ages 50 and older were more likely than those in younger groups to say surveillance is acceptable across many of these specific scenarios. In addition, those who are not concerned about the surveillance programs are more likely to say that monitoring in these situations is acceptable. And those who are confident that surveillance programs are in the public interest are more likely than others to back monitoring people in all of these circumstances, as are those who think the judicial system is balancing the needs of law enforcement with people's right to privacy.

Again, it is noteworthy that there are no partisan differences on these questions.

How People are Changing Their Own Behavior

The 87% of respondents in this sample who say they had heard at least a little about the government's surveillance programs were asked a series of questions about whether they had changed some of the ways they use technology. This section of the report covers their answers.

Some are altering their use of information and communication technologies

The respondents to this survey who knew about the government monitoring programs were asked if they had changed the way they used a variety of communications and information tools since they had learned about the government's programs.

- 18% of the Americans who are aware of the surveillance programs say they have changed the way they use their email accounts "somewhat" or a "great deal."
- 17% say they have changed the way they use search engines.
- 15% say they have changed the way they use social media.
- 15% say they have changed the way they use their cell phones.
- 13% say they have changed the way they use mobile apps.
- 13% say they have changed the way they use text messages.
- 9% say they have changed the way they use their landline phone.

In all, 12% of those who are aware of the programs say they changed their behavior in at least one of these activities a "great deal" and 25% have changed their behavior in at least one of these activities a "great deal" or "somewhat." That amounts to 22% of all adults who say they have changed their use of various technology platforms since the Snowden revelations.

Those who are more likely to have changed their behaviors include the people who have heard "a lot" about government surveillance (38% say they have changed a great deal/somewhat in at least one of these activities), those who are at least somewhat concerned about the programs (41% have changed at least one activity), and those who are concerned about government monitoring of their use of social media, search engines, cell phones, apps, and email. Similarly, those who say they are now less confident that the programs serve the public interest and those who believe the courts are not doing a good job balancing the interests of privacy and law enforcement are also more likely than others to say they have changed these behaviors.

There are no significant demographic traits that stand out among those who say they have changed their behaviors with these tools. In addition, there are no partisan differences when it comes to those who have changed their use of various technologies.

The respondents who say they modified their behavior were asked in an open-ended follow-up question to explain why they changed the way they communicate since learning about the programs. Some suggested that they were concerned about how their communications would be interpreted by third parties:

"I don't search some things that I might have before."

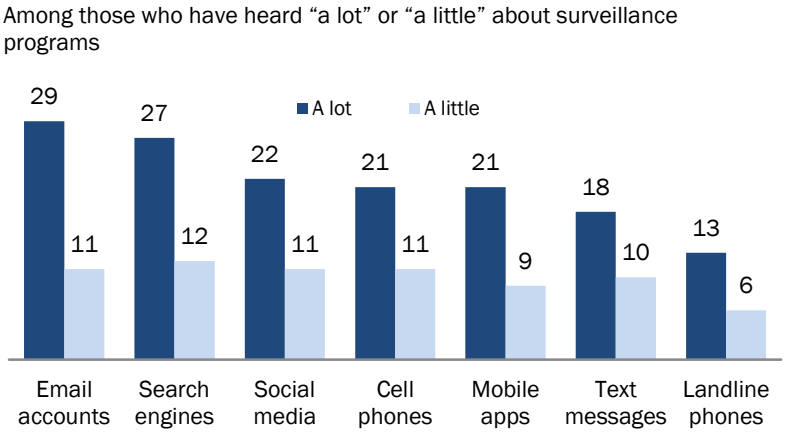
"Somewhat concerned to look up certain information on search engines, since it may appear suspicious, even if my reason is pure curiosity."

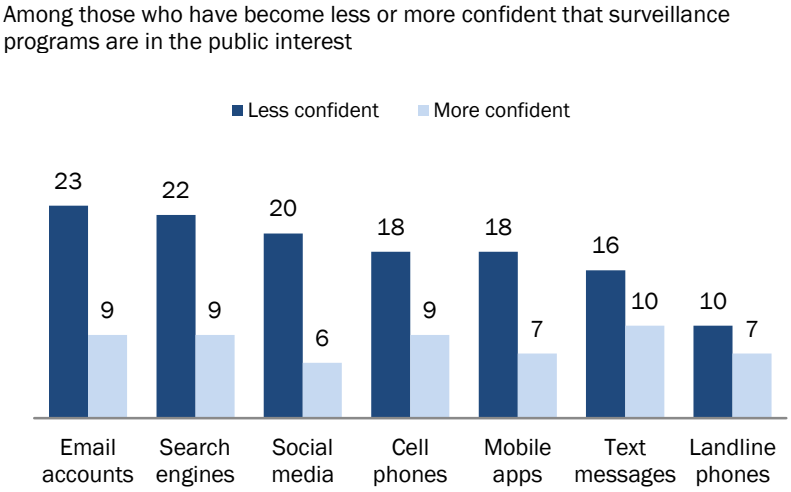
"I used to be more open to discussing my private life online with my select friends. Now I don't know who might be listening."

"Can't joke about stuff that could be taken as a threat."

Those Most Likely to Have Changed Their Behavior on Technology Have Heard a Lot about the Surveillance Programs and Are Less Confident the Programs Are in the Public Interest

Among each subgroup, the % who say they changed their use of these technologies "a great deal" or "somewhat" since they learned of the phone and internet monitoring programs





Source: Survey of 475 U.S. adults on GfK panel November 26-2014- January 3, 2015.

PEW RESEARCH CENTER

The respondents who said they had not changed their behavior in any notable way were asked why and some of the answers included:

> *"I really don't worry about government monitoring since they would have no interest in what I'm doing. I'm more cautious about what I post and say for personal reasons."*
>
> *"I actually haven't changed anything, at least consciously. I forget that I might be monitored, to be honest."*
>
> *"I haven't changed it much simply because I don't feel it's worth the effort."*

Some Americans are adopting specific online strategies to hide their information from the government

The respondents who say they have heard something about the government surveillance programs were asked about a number of offline and online activities and whether they had done anything to hide or shield their information from the government in response to learning about it.

A majority say they have not changed any communications or online activities since learning of the phone and internet monitoring programs. Still, 34% of those who have heard about the programs say that they have changed at least one of the following:

- 17% of the adults who have heard about the government surveillance programs say they have changed their privacy settings on social media in an effort to hide their information from the government.
- 15% have avoided certain apps.
- 15% have used social media less often.
- 14% have spoken more in person instead of communicating online or over the phone.
- 13% have uninstalled certain apps.
- 13% have avoided using certain terms in online communications.
- 13% have unfriended or unfollowed people on social media.
- 11% have not used certain terms in search engine queries they thought might trigger scrutiny.
- 8% have deleted social media accounts.
- 8% have made more phone calls instead of communicating online.

Those Most Likely to Shield Their Information from the Government Are Those Who Have Heard a Lot About Surveillance Programs and Who are Less Confident the Programs are in the Public Interest

% of U.S. adults who say they have used these strategies to shield themselves from surveillance since they learned of the phone and internet monitoring programs

	Among those who have heard "a little" or a "lot" about surveillance programs		Among those who are "less" or "more" confident that surveillance programs are in the public interest	
	A lot	*A little*	*Less Confident*	*More Confident*
Use social media less often	26	10	23	4
Change social media privacy settings	25	13	25	6
Spoken more in person rather than on phone or online	23	10	20	6
Avoided certain apps	22	11	17	11
Unfriended people on social media	19	10	18	6
Uninstalled certain apps	18	11	18	6
Avoided terms in online communications	18	11	18	6
Avoided using certain search terms	16	9	15	5
Made more phone calls instead of communicating online	15	4	11	3
Deleted social media accounts	14	5	12	3

Source: Survey of 475 U.S. adults on GfK panel November 26-2014- January 3, 2015.

PEW RESEARCH CENTER

Those most likely to have taken these steps include adults who have heard a lot about the surveillance programs and those who say they have less confidence since the Snowden revelations that the programs are in the public interest.

Some have taken relatively simple steps to make their activities more private, but just a fraction have taken more sophisticated steps

Those who said they had heard about the government surveillance programs were asked whether they had used any of a number of available tools to make their communications more private since they had learned about the U.S. phone and internet monitoring programs. Some 25% said they used more complex passwords and 19% said they had changed the privacy settings on their social media accounts such as Facebook or Twitter.

In both cases, younger adults under the age of 50 were much more likely than older adults to say they had used at least one of these strategies. And those with at least some college education were

more likely than others to have done the same. At the same time, those most likely to say they have *not* used these tools are the respondents who say they are not concerned about the surveillance programs and those who say they do have confidence the programs are serving the public interest. There are no notable partisan differences in people's responses to questions about these tools.

Sophisticated tools and techniques are widely available and can help online Americans increase the privacy and security of their online activities and personal data sharing. However, thus far, fairly few have adopted these tools since learning about the programs. Among those who have heard about the government surveillance programs:

- 10% say they have used a search engine that doesn't keep track of their search history.
- 5% have added privacy-enhancing browser plug-ins like DoNotTrackMe (now known as Blur) or Privacy Badger.
- 4% have adopted mobile encryption for calls and text messages.
- 3% have used proxy servers can help them avoid surveillance.
- 2% have adopted email encryption programs such as Pretty Good Privacy (PGP).
- 2% have used anonymity software such as Tor.
- 1% have used locally-networked communications such as FireChat.

A substantial number have not considered or do not know about some relatively common tools that could make their activities more private

One potential reason some have not changed their behaviors is that 54% believe it would be "somewhat" (35%) or "very" (19%) difficult to find tools and strategies that would help them be more private online and using their cell phones. Another 44% believe it would be "very easy" (9%) or "somewhat easy" (35%) to find tools and strategies that would help them be more private. Even those with college educations are evenly split on this issue of how easy or hard it would be to find such tools.

The vast majority of citizens say they have not adopted or even considered some of the more commonly available tools that can be used to make online communications and activities more private:

- 53% have not adopted or considered using a search engine that doesn't keep track of a user's search history and another 13% do not know about these tools.
- 46% have not adopted or considered using email encryption programs such as Pretty Good Privacy (PGP) and another 31% do not know about such programs.

- 43% have not adopted or considered adding privacy-enhancing browser plug-ins like DoNotTrackMe (now known as Blur) or Privacy Badger and another 31% do not know such plug-ins.
- 41% have not adopted or considered using proxy servers that can help them avoid surveillance and another 33% do not know about this.
- 40% have not adopted or considered using anonymity software such as Tor and another 39% do not know about what that is.

These figures may in fact understate the lack of awareness among Americans because noteworthy numbers of respondents answered "not applicable to me" on these questions even though virtually all of them are internet and cell phone users.

As a rule, older Americans and those who have a high school diploma or less are more likely to say they have not heard of many of the tools on our list when compared with those who are younger or have higher education levels. Interestingly, both heavy and light technology users are equally likely to say they do not know of these tools.

When asked for their reasons for changing privacy behaviors by embracing these tools and strategies, respondents described a variety of motivations, ranging from a principled defense of privacy, to guarding their information from criminals:

> *"Because it's no one's business whom I talk to [or] what I talk about."*

> *"I have employed stronger passwords, not because of government monitoring, but more because of the recent retailer hacks. I'm more afraid of cyber-crime [and] identity theft than government monitoring."*

> *"To encrypt my financial data from hackers."*

> *"To keep anyone, not just the government, from having access to my personal information online."*

Others who did not adopt the above tools or strategies said that it takes significant time and effort to learn about privacy-protecting measures:

> *"I do not know anything about some of them and do not have the time to research them at this time."*

"I do not feel expert enough to know what to do to protect myself, and to know that the protection chosen is effective. Technology changes very fast."

Still, others said they avoid taking more advanced privacy measures because they believe that taking such measures could make them appear suspicious:

"There's no point in inviting scrutiny if it's not necessary."

"I didn't significantly change anything. It's more like trying to avoid anything questionable, so as not to be scrutinized unnecessarily."

"[I] don't want them misunderstanding something and investigating me."

Methods

About this survey

The analysis in this report is based on a Pew Research Center survey conducted between November 26, 2014 and January 3, 2015 among a sample of 475 adults, 18 years of age or older living in the United States. The survey was conducted by the GfK Group using KnowledgePanel, its nationally representative online research panel. GfK selected a representative sample of 1,537 English-speaking panelists to invite to join the subpanel and take the first survey in the fall of 2014. Of the 935 panelists who responded to the invitation (60.8%), 607 agreed to join the subpanel and subsequently completed the first survey (64.9%) whose results were reported in November 2014. This group has agreed to take four online surveys about "current issues, some of which relate to technology" over the course of a year and possibly participate in one or more 45-60-minute online focus group chat sessions. For the third survey whose results are reported here, 475 of the original 607 panelists participated. A random subset of the subpanel receive occasional invitations to participate in online focus groups. For this report, a total of 59 panelists participated in one of six online focus groups conducted during December 2014 and January 2015. Margin of sampling error for the total sample of 475 respondents is plus or minus 5.6 percentage points at the 95% level of confidence.

KnowledgePanel members are recruited through probability sampling methods and include both those with internet access and those without. KnowledgePanel provides internet access for those who do not have it and, if needed, a device to access the internet when they join the panel. A combination of random digit dialing (RDD) and address-based sampling (ABS) methodologies have been used to recruit panel members (in 2009 KnowledgePanel switched its sampling methodology for recruiting panel members from RDD to ABS). The panel comprises households with landlines and cellular phones, including those only with cell phones, and those without a phone. Both the RDD and ABS samples were provided by Marketing Systems Group (MSG).

KnowledgePanel continually recruits new panel members throughout the year to offset panel attrition as people leave the panel. Respondents were selected randomly from eligible adult household members of the panel. All sampled members received an initial email on November 26, 2014 to notify them of the survey and included a link to the survey questionnaire. One standard follow-up reminder was sent three days later to those who had not yet responded.

The final sample for this survey was weighted using an iterative technique that matches gender, age, education, race, Hispanic origin, household income, metropolitan area or not, and region to parameters from the March 2013 Census Bureau's Current Population Survey (CPS). In addition, the sample is weighted to match current patterns of internet access from the October 2012 CPS

survey. This weight is multiplied by an initial base or sampling weight that corrects for differences in the probability of selection of various segments of the sample and by a panel weight that adjusts for any biases due to nonresponse and noncoverage at the panel recruitment stage (using all of the parameters mentioned above as well home ownership status).

Sampling errors and statistical tests of significance take into account the effect of weighting at each of these stages. Sampling error for the total sample of 475 respondents is plus or minus 5.6 percentage points at the 95% level of confidence. The following table shows the unweighted sample sizes and the error attributable to sampling that would be expected at the 95% level of confidence for different groups in the survey:

Group	Unweighted sample size	Plus or minus …
All adults	475	5.6 percentage points
Men	241	7.9 percentage points
Women	234	8 percentage points
18-49	245	7.8 percentage points
50+	230	8 percentage points

Sample sizes and sampling errors for other subgroups are available upon request. The margins of error reported and statistical tests of significance are adjusted to account for the survey's design effect, a measure of how much efficiency is lost from the weighting procedures. In addition to sampling error, one should bear in mind that question wording and practical difficulties in conducting surveys can introduce error or bias into the findings of opinion polls.

Pew Research Center is a nonprofit, tax-exempt 501(c)3 organization and a subsidiary of The Pew Charitable Trusts, its primary funder.

PEW RESEARCH CENTER/GFK PRIVACY PANEL
SURVEY #3 TOPLINE
NOVEMBER 26, 2014-JANUARY 3, 2015
TOTAL N=475 ADULTS, AGES 18 AND OLDER
SURVEY CONDUCTED ONLINE

MARGIN OF ERROR FOR ALL ADULTS IS +/- 5.6 PERCENTAGE POINTS

In this survey we'd like to explore your views about some important issues.

First, we'd like to learn about some activities you might pursue in your daily life.

AMONG ALL ADULTS [N=475]
Q1. How often do you use your cell phone?

65	Several times a day
9	About once a day
10	A few times a week
7	A few times a month
2	A few times a year
6	Never
1	Refused
75	**NET Daily**
24	**NET Less often / Never**

AMONG CELL PHONE USERS [N=444]
Q2. How often do you send and receive text messages on your cell phone?

54	Several times a day
8	About once a day
10	A few times a week
6	A few times a month
5	A few times a year
12	Never
5	Refused/Not asked
63	**NET Daily**
33	**NET Less often / Never**

AMONG ALL ADULTS [N=475]
Q3. How often do you use the internet either on a computer or on a mobile device like a smartphone or tablet?

68	Several times a day
12	About once a day
7	A few times a week
3	A few times a month
2	A few times a year

6 Never
2 Refused
81 NET Daily
17 NET Less often / Never

AMONG ALL ADULTS [N=475]
Q4. How often do you send and receive email?

55 Several times a day
13 About once a day
17 A few times a week
5 A few times a month
2 A few times a year
6 Never
1 Refused
69 NET Daily
31 NET Less often / Never

AMONG ALL ADULTS [N=475]
Q5. How often do you use social media such as Facebook, Twitter, Pinterest, or LinkedIn?

31 Several times a day
14 About once a day
16 A few times a week
7 A few times a month
3 A few times a year
28 Never
2 Refused
45 NET Daily
54 NET Less often / Never

AMONG ALL ADULTS [N=475]
Q6. How often do you use apps on a mobile device such as a smartphone or tablet computer?

38 Several times a day
12 About once a day
8 A few times a week
5 A few times a month
3 A few times a year
33 Never
1 Refused
50 NET Daily
49 NET Less often / Never

AMONG MOBILE APP USERS [N=320]

Q7. When an app on your smartphone or tablet seeks your permission to use your location, how often you allow it to use your location?

22	Frequently
36	Sometimes
28	Hardly ever
11	Never
3	Refused/Not asked

AMONG ALL ADULTS [N=475]
Q8. How often do you use search engines to look up information?

37	Several times a day
15	About once a day
20	A few times a week
12	A few times a month
6	A few times a year
8	Never
1	Refused
52	**NET Daily**
20	**NET Weekly**
26	**NET Less often / Never**

AMONG ALL ADULTS [N=475]
Q9. Which of these statements more accurately describes you:

65	I am generally a private person and like to keep to myself
34	I am generally an open person who enjoys sharing with others
1	Refused

AMONG ALL ADULTS [N=475]
Q10. How much, if anything, have you heard about the government collecting information about telephone calls, emails and other online communications as part of efforts to monitor terrorist activity?

31	A lot
56	A little
6	Nothing at all
6	Don’t know
1	Refused

According to news reports, the American government has been monitoring communications, such as emails and phone calls, in the U.S. and many other countries.

AMONG ALL ADULTS [N=475]
Q12. In your opinion, is it acceptable or unacceptable for the American government to monitor communications from individuals suspected of terrorist activities?

82 Acceptable
15 Unacceptable
2 Refused

AMONG ALL ADULTS [N=475]
Q13. In your opinion, is it acceptable or unacceptable for the American government to monitor communications from American leaders?

60 Acceptable
38 Unacceptable
2 Refused

AMONG ALL ADULTS [N=475]
Q14. In your opinion, is it acceptable or unacceptable for the American government to monitor communications from American citizens?

40 Acceptable
57 Unacceptable
3 Refused

AMONG ALL ADULTS [N=475]
Q15. In your opinion, is it acceptable or unacceptable for the American government to monitor communications from citizens of other countries?

54 Acceptable
44 Unacceptable
2 Refused

AMONG ALL ADULTS [N=475]
Q16. In your opinion, is it acceptable or unacceptable for the American government to monitor communications from leaders of other countries?

60 Acceptable
37 Unacceptable
3 Refused

AMONG ALL ADULTS [N=475]
Q17. Overall, how concerned are you about government surveillance of Americans' data and electronic communications?

17 Very concerned
35 Somewhat concerned
33 Not very concerned
13 Not at all concerned
2 Refused
52 NET Concerned
46 NET Not concerned

AMONG ALL ADULTS [N=475]
Q18. Could you please explain briefly why you have this level of concern about government surveillance of Americans' personal data and electronic communications?

[LARGE TEXTBOX – UNLIMITED CHARACTER LIMIT]

OPEN-END RESPONSES NOT SHOWN

AMONG THOSE WHO HEARD A LOT OR A LITTLE ABOUT GOV'T COLLECTING INFO [N=417]
Q19. As you have watched the developments in news stories about government monitoring programs over recent months, would you say that you have become more confident or less confident that the programs are serving the public interest?

37 More confident
61 Less confident
2 Refused

AMONG ALL ADULTS [N=475]
Q20. Do you generally think that the courts and judges do a good job balancing the public's right to privacy and the needs of law enforcement and intelligence agencies to collect information for investigations?

48 Yes
49 No
3 Refused

AMONG ALL ADULTS [N=475]
Q21N (Q21). How concerned are you about government monitoring of your activity on social media websites such as Facebook or Twitter?

14 Very concerned
17 Somewhat concerned
24 Not very concerned
24 Not at all concerned
19 Not applicable
2 Refused
31 NET Concerned
47 NET Not concerned

AMONG ALL ADULTS [N=475]
22N (Q22). How concerned are you about government monitoring of your activity on search engines?

15 Very concerned
24 Somewhat concerned
30 Not very concerned
23 Not at all concerned
5 Not applicable
2 Refused
39 NET Concerned
53 NET Not concerned

AMONG ALL ADULTS [N=475]
24N (Q24). How concerned are you about government monitoring of your activity on your cell phone?

17 Very concerned
20 Somewhat concerned
30 Not very concerned
24 Not at all concerned
7 Not applicable
3 Refused
37 NET Concerned
54 NET Not concerned

AMONG ALL ADULTS [N=475]
26N (Q26). How concerned are you about government monitoring of your activity on your mobile apps?

12 Very concerned
17 Somewhat concerned
28 Not very concerned
22 Not at all concerned
19 Not applicable
3 Refused
29 NET Concerned
49 NET Not concerned

AMONG ALL ADULTS [N=475]

27N (Q27). How concerned are you about government monitoring of your email messages?

19	Very concerned
19	Somewhat concerned
31	Not very concerned
23	Not at all concerned
4	Not applicable
3	Refused
38	**NET Concerned**
54	**NET Not concerned**

AMONG THOSE WHO ARE VERY / SOMEWHAT CONCERNED ABOUT GOV'T MONITORING [N=225]

Q22 (Q28). Would you explain a little more what concerns you? What kinds of problems you are concerned might arise because of government monitoring of your communications activity?

[LARGE TEXTBOX – UNLIMITED CHARACTER LIMIT]

OPEN-END RESPONSES NOT SHOWN

[RANDOMIZE RESPONSE OPTIONS A-G]

AMONG THOSE WHO HEARD A LOT OR A LITTLE ABOUT GOV'T COLLECTING INFO [N=417]

Q23 (Q29). Since learning about U.S. phone and internet monitoring, how much, if at all, would you say you have changed the way you use any of the following:

		A great deal	Somewhat	Not much	Not at all	Not applicable	Refused	**NET Great deal / somewhat**	**NET Not much / not at all**
a.	Social media websites such as Facebook or Twitter	7	7	18	45	22	1	**15**	**63**
b.	Search engines	7	10	23	56	4	1	**17**	**79**
c.	Your landline phone	5	4	17	51	23	<1	**9**	**68**
d.	Your cell phone	7	7	23	57	5	1	**15**	**80**
e.	Text messages	7	6	19	53	15	0	**13**	**72**
f.	Mobile apps	8	6	17	49	21	<1	**13**	**66**
g.	Your email accounts	8	10	23	57	2	1	**18**	**80**

[IF Q23A-G=1-3]
[LARGE TEXTBOX – UNLIMITED CHARACTER LIMIT]
AMONG THOSE WHO CHANGED THEIR BEHAVIOR [N=187]
Q24 (Q30). Could you explain a bit more about the behavior you changed and why you changed the way you communicate with others since learning about government monitoring programs?

[LARGE TEXTBOX – UNLIMITED CHARACTER LIMIT]

OPEN-END RESPONSES NOT SHOWN

[SP]
AMONG ALL ADULTS [N=475]
Q25 (Q31). If you wanted to be more private while you were using the internet or your cell phone, how easy do you think it would be for you to find tools and strategies that would help you?

9	Very easy
35	Somewhat easy
35	Somewhat difficult
19	Very difficult
3	Refused
44	**NET Easy**
54	**NET Difficult**

[IF Q10=1-2]
[RANDOMIZE RESPONSE OPTIONS A-K]
[GRID, SP ACROSS]
AMONG THOSE WHO HEARD A LOT / LITTLE ABOUT GOV'T COLLECTING INFO [N=417]
Q26 (Q32). Since learning about the government's phone and internet monitoring programs, have you done any of the following in an effort to hide or shield your information from the government?

		I have done this	I have not done this, but have considered it	I have not done this and have not considered it	Not applicable	Refused	**NET Have not done this**
a.	Unfriended or unfollowed people on social media	13	8	52	26	1	**60**
b.	Deleted social media accounts	8	9	58	24	1	**67**
c.	Used social media less often	15	9	50	24	<1	**60**
d.	Changed your privacy settings on social media	17	10	47	24	1	**57**
e.	Made more phone calls instead of communicating online	8	10	70	11	1	**80**
START NEW SCREEN							
f.	Avoided using certain terms in online communications	13	10	67	9	1	**77**
g.	Avoided certain apps	15	6	56	22	1	**62**
h.	Uninstalled certain apps	13	5	57	25	1	**62**

i.	Used pseudonyms	8	6	68	16	1	**75**
j.	Not used certain terms in search engine queries you thought might trigger scrutiny	11	13	64	11	1	**77**
k.	Spoke more in person instead of communicating online or over the phone	14	9	67	9	1	**76**

[LARGE TEXTBOX – UNLIMITED CHARACTER LIMIT]
AMONG THOSE WHO HEARD A LOT / LITTLE ABOUT GOV'T COLLECTING INFO [N=417]
Q27 (Q33). Please explain if you have made any other changes since learning about U.S. phone and internet monitoring programs that we haven't mentioned.

[LARGE TEXTBOX – UNLIMITED CHARACTER LIMIT]

OPEN-END RESPONSES NOT SHOWN

[IF Q26A-K=1-2]
[LARGE TEXTBOX – UNLIMITED CHARACTER LIMIT]
AMONG THOSE WHO HAVE CHANGED THEIR BEHAVIOR OR CONSIDERED IT [N=185]
Q28 (Q34). Could you explain a bit more about why you changed some of your behaviors and activities?

[LARGE TEXTBOX – UNLIMITED CHARACTER LIMIT]

OPEN-END RESPONSES NOT SHOWN

[IF Q10=1-2]
AMONG THOSE WHO HEARD A LOT / LITTLE ABOUT GOV'T COLLECTING INFO [N=417]
Q29 (Q35). Since learning about U.S. phone and internet monitoring, have you adopted any of the following tools or strategies to make your communications and activities more private?

		I have adopted this	I have not adopted this, but have considered it	I have not adopted this and have not considered it	I don't know what this is	Not applicable to me	Refused	**NET Have not adopted this**
a.	Used a search engine that doesn't keep track of your search history	10	12	53	13	12	1	**64**
b.	Adopted email encryption, such as PGP	2	10	46	31	11	1	**55**
c.	Adopted mobile encryption for calls or text messages	4	8	48	24	15	2	**56**
d.	Used more complex passwords	25	12	48	6	8	1	**60**
e.	Proxy servers	3	7	41	33	13	2	**49**

f.	Added a privacy-enhancing browser plugin like DoNotTrackMe or Privacy Badger	5	7	43	31	13	1	**50**
g.	Changed your privacy settings on social media such as Facebook or Twitter	19	6	44	4	26	1	**50**
h.	Used locally-networked communications such as FireChat	1	4	42	37	14	1	**47**
i.	Used anonymity software such as Tor	2	5	40	39	13	1	**45**
j.	Used another software or network tool to make your activities more private	3	9	60	14	12	1	**69**

AMONG THOSE WHO ADOPTED PRIVACY TOOLS OR CONSIDERED IT [N=200]

Q30 (Q36). Could you explain a bit more about why you felt it was important to adopt or consider one of those tools or strategies?

OPEN-END RESPONSES NOT SHOWN

[RANDOMIZE A-G]
[GRID, SP ACROSS]
AMONG ALL ADULTS [N=475]

Q37 Is it acceptable or unacceptable for the government to monitor the communications of U.S. citizens if the person…

		Acceptable	Unacceptable	Refused
a.	Visited a child pornography site	77	19	4
b.	Was reported by a bank to be making unusual withdrawals	51	45	4
c.	Made such engine queries for the keywords “explosives” and “automatic weapons”	65	30	4
START NEW SCREEN				
d.	Visited websites of known anti-American groups	67	29	4
e.	Exchanged emails with an imam who preached against infidels	68	28	4
f.	Used encryption software to hide files	49	47	4
g.	Had friends and followers on social media who used hateful language about American leaders	49	47	4

[RANDOMIZE RESPONSE OPTIONS 1 AND 2]
AMONG ALL ADULTS [N=475]
PARTY.
In politics TODAY, do you consider yourself a Republican, Democrat, or independent?

24	Republican
36	Democrat
33	Independent
6	Something else
2	Refused