PewResearchCenter

NUMBERS, FACTS AND TRENDS SHAPING THE WORLD

JANUARY 14, 2016

Privacy and Information Sharing

Many Americans say they might provide personal information, depending on the deal being offered and how much risk they face

BY *Lee Rainie* **AND** *Maeve Duggan*

FOR FURTHER INFORMATION ON THIS REPORT:

Lee Rainie, Director Internet, Science and Technology Research
Dana Page, Senior Communications Manager
202.419.4372
www.pewresearch.org

RECOMMENDED CITATION: Rainie, Lee, Duggan, M. "Privacy and Information Sharing" Pew Research Center, December 2015. Available at: http://www.pewinternet.org/2016/01/14/2016/Privacy-and-Information-Sharing/

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.

Privacy and Information Sharing

Many Americans say they might provide personal information, depending on the deal being offered and how much risk they face

Most Americans see privacy issues in commercial settings as contingent and context-dependent. A new Pew Research Center study based on a survey of 461 U.S. adults and nine online focus groups of 80 people finds that there are a variety of circumstances under which many Americans would share personal information or permit surveillance in return for getting something of perceived value. For instance, a majority of Americans think it would be acceptable (by a 54% to 24% margin) for employers to install monitoring cameras following a series of workplace thefts. Nearly half (47%) say the basic bargain offered by retail loyalty cards – namely, that stores track their purchases in exchange for occasional discounts – is acceptable to them, even as a third (32%) call it unacceptable.

Still, while many Americans are willing to share personal information in exchange for tangible benefits, they are often cautious about disclosing their information and frequently unhappy about what happens to that information once companies have collected it. For example, when presented with a scenario in which they might save money on their energy bill by installing a "smart thermostat" that would monitor their movements around the home, most adults consider this an unacceptable tradeoff (by a 55% to 27% margin). As one survey respondent explained: *"There will be no 'SMART' anythings in this household. I have enough personal data being stolen by the government and sold [by companies] to spammers now."*

In online focus groups and in open-ended responses to a nationally representative online survey, many people expressed concerns about the safety and security of their personal data in light of numerous high-profile data breaches. They also regularly expressed anger about the barrage of unsolicited emails, phone calls, customized ads or other contacts that inevitably arises when they elect to share some information about themselves. In response to a question about having their online behavior tracked in exchange for getting access to a free online service , one survey respondent wrote: "*I want control over what ads are being 'pushed back' to me: I have no interest in 'puppy portraits' but I may be interested in cameras, equipment, etc. In an effort to 'target' my preferences, my inbox gets full of [expletive] that is not relevant to me."*

These findings suggest that the phrase that best captures Americans' views on the choice between privacy vs. disclosure of personal information is, "It depends." People's views on the key tradeoff of the modern, digital economy – namely, that consumers offer information about themselves in exchange for something of value – are shaped by both the conditions of the deal and the

circumstances of their lives. In extended comments online and through focus groups, people indicated that their interest and overall comfort level depends on the company or organization with which they are bargaining and how trustworthy or safe they perceive the firm to be. It depends on what happens to their data after they are collected, especially if the data are made available to third parties. And it also depends on how long the data are retained.

The scenarios obviously did not comprehensively cover the vast range of possibilities where people would consider sharing personal information in return for a benefit. But it is interesting to note that 17% of adults say they wouldn't take any of the deals described in the six scenarios and 4% say they would accept all of the deals. The substantial majority indicate that at least one of these transactions is potentially acceptable to them.

Furthermore, notable shares of the public say their consideration of each individual scenario is conditional: Their answer depends on the circumstances of the offer, their trust in those collecting and storing the data, and their sense of what the aftermath of data-sharing might look like.

The survey findings that form the basis of this report are different in some respects from conventional public opinion polling. In this study, respondents were presented with six hypothetical scenarios, each of which involved sharing some level of personal data in exchange for using a product or service. They were then asked whether the bargain they were offered in return for sharing that information was acceptable, not acceptable, or if "it depends" on the context of the choice. Upon making their selection, they were then asked to describe in their own words what factors contributed to making their selection.

The nearby chart runs down the six different scenarios that were examined in this study.

Many Americans are in an "it depends" frame of mind when they think about disclosing personal information or keeping it private when considering different scenarios

% of adults who would find these different scenarios acceptable or not acceptable

Office surveillance cameras

Several co-workers of yours have recently had personal belongings stolen from your workplace, and the company is planning to install high-resolution security cameras that use facial recognition technology to help identify the thieves and make the workplace more secure. The footage would stay on file as long as the company wishes to retain it, and could be used to track various measures of employee attendance and performance.

Sharing health information

A new health information website is being used by your doctor's office to help manage patient records. Your participation would allow you to have access to your own health records and make scheduling appointments easier. If you choose to participate, you will be allowing your doctor's office to upload your health records to the website and the doctor promises it is a secure site.

Retail loyalty cards

A grocery store has offered you a free loyalty card that will save you money on your purchases. In exchange, the store will keep track of your shopping habits and sell this data to third parties.

Auto insurance

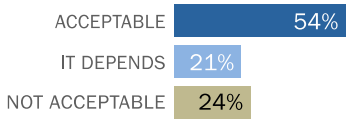
Your insurance company is offering a discount to you if you agree to place a device in your car that allows monitoring of your driving speed and location. After the company collects data about your driving habits, it may offer you further discounts to reward you for safe driving.

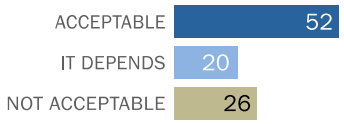
Free social media

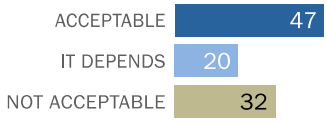
A new social media platform is being used by your former high school to help manage communications about a class reunion. You can find out the basic information about the reunion over email, but your participation on the social media site would reconnect you with old friends and allow you to communicate more easily with those who are attending. If you choose to participate, you will be creating a profile using your real name and sharing a photo of yourself. Your access to the service is free, but your activity on the site would be used by the site to deliver advertisements it hopes will be appealing to you.

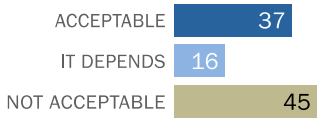
Smart thermostat

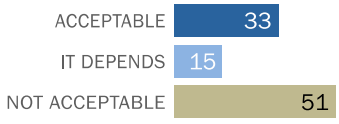
A new technology company has created an inexpensive thermostat sensor for your house that would learn about your temperature zone and movements around the house and potentially save you on your energy bill. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house like when people are there and when they move from room to room.

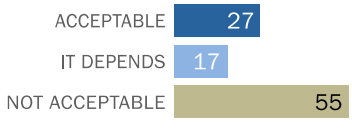












Source: Survey conducted Jan. 28 – Feb. 16, 2015.

Note: Refused responses not shown.

PEW RESEARCH CENTER

Some issues people ponder as they consider privacy tradeoffs include the likelihood of getting spam, the risk of data breaches, the special intimacy tied to location data and overdone customer profiling

Contingency permeates the reactions to each of these different scenarios, but a number of other themes emerged as well – especially when it comes to tradeoffs that people find not acceptable. Some of the common themes that came across in the open-ended answers and focus group responses include:

- ***The initial bargain might be fine, but the follow-up by companies that collect the data can be annoying and unwanted.*** People repeatedly expressed anger at the barrage of unwanted emails that often comes after the initial transaction. One survey respondent wrote: *"I would take the deal, as long as my personal information is not shared with the third party, such as my name and contact information. If it's just my demographics – age, city, what I buy – that's OK. If they want to print coupons at the checkout that target me as a consumer, that's OK, but not contacting me personally (mail, email, phone, etc.) with advertising. I hate hate hate that stuff."*
- ***Scammers and hackers are a constant threat.*** There is widespread worry that people's information is vulnerable, even when the companies that collect it do their best to keep it safe. As one respondent summarized: "*The 'secure' sites are continually making the news when they are hacked. We can have our information stolen from banks, credit card companies, hospitals … all secure … all hacked in the past. The more I 'put it out there,' the more likely my information will go somewhere hazardous to my well-being."*
- ***Location data seems especially precious in the age of the smartphone***. Some of the most strongly negative reactions came in response to scenarios involving the sharing of personal location data. One respondent put it as follows: "*I continually deny location services on my phone because I don't want the chance of ads coming up."* A focus group participant said she doesn't worry about most personal data collection *"except where I am, especially in my home. If anything involves the use of cameras, including on my phone or computer, that's the worst privacy invasion for me."*
- ***Profiling sometimes seems creepy.*** The words "creepy" and "Big Brother" and "stalking" were used regularly in the answers of those who worry about their personal information. One focus group participant summed up this view: *"Some of the marketing tracking things are creepy. I look at one thing online and then see it on every single site for weeks. At first – intriguing. Then creepy."* Another argued: *"Perhaps we need to teach the younger generations about BIG BROTHER. It seems he has been forgotten."* To which another group member added: *"Orwell was a prophet."*

- ***People are not happy when data are collected for one purpose but are used for other, often more invasive purposes.*** Many Americans express suspicion that data collectors (from employers to advertisers) have ulterior motives in their pursuit of personal data. One respondent put it this way: "*I do not trust insurance companies, and I feel they could use this data to increase my rates under whatever pretend excuse. Insurance companies are in the risk management business, and they cannot reduce that risk at the cost of their customers. The more they know, the less risk for them and the higher cost for customers.*"

The potential benefits of sharing personal information include saving money, gaining access to useful services or information, and facilitating commercial and social encounters

Yet even as they worry about the negative downstream consequences of sharing their personal information, these findings also illustrate that consumers understand and appreciate the benefits of sharing – at least under certain circumstances. The key themes here include:

- ***Free is a good price.*** The social media scenario, in particular, drew a number of short answers that made clear people like no-cost services. One focus group participant explained why he was comfortable letting a technology company know about him in return for free email service: "*To be honest, I don't really care. That is especially the case when I voluntarily use a service in return for giving up some information. For example, I use Gmail for free, but I know that Google will capture some information in return. I'm fine with that.*"
- ***Sharing helps lubricate commercial and social interactions.*** People often need convenient and inexpensive access to information, goods and services. Moreover, they generally understand that disclosing personal information makes those transactions possible – and in fact, can make them more desirable to consumers. One survey participant found the loyalty card scenario acceptable and explained: "*If the store shares information that would pertain to the type of things I would purchase, it would be OK.*"
- ***Certain realms are not inherently private and different rules about surveillance and sharing apply.*** Certain physical spaces or types of information are seen as inherently less private than others. One survey respondent noted how these norms influence his views on the acceptability of workplace surveillance cameras: "*It is the company's business to protect their assets in any way they see fit.*"

Interestingly, there are no consistent demographic patterns to people's answers on different scenarios. Sometimes people's views vary by age, household income or education, and other times they do not. And at times when there are differences, they are not always either consistently protective of privacy or consistently willing to disclose information. For instance, those under age

50 are more likely than those 50 and older to find the scenario involving a new social media site acceptable (40% to 25%). Yet those 50 and older are more likely than those who are younger to find the online medical records scenario acceptable (62% to 45%). Clearly, people place different value on different kinds of information-sharing exchanges.

There are no statistically meaningful differences in women's and men's answers to any of these scenarios.

Where does this leave Americans? Many focus group participants are uncertain, resigned and annoyed – or worse. Still, some accept this is part of modern life and others are hopeful that technological and legal solutions can be found

In nine online focus groups tied to these issues, the 80 participants gave voice to a range of emotions about the state of privacy and its future. While the focus groups cannot be seen as representative of the whole adult population, it was often the case that given the choice, people are often much more likely to speak of the darker side of personal information tradeoffs than they are to reference the benefits. As one focus group participant put it: *"I think the [chances for achieving privacy] are getting more hopeless as technology advances."*

One of the most unsettling aspects of privacy issues to many of the focus group participants is how hard they feel it is to get information about what is collected and uncertainty about who is collecting the data. A sampling of those views:

> *"In my opinion, there is a woeful lack of disclosure on how personal information is used by companies. If you read some of the terms of service, you are essentially giving the company the right to do almost anything with your personal information."*

> *"I have no idea how I'd investigate what info is collected about me in places like Google and Facebook, other than the information I've provided them, such as my profile info."*

Asked whether changes in the basic state of privacy were a "huge harm" to society or something more like an "annoyance that could be accommodated," people's answers ranged widely:

> *"It feels hopeless. Information retrieval is a way of life, but it inhibits human interaction."*

> *"For me it's not so much 'hopeless,' as it is 'resigned.'"*

> *"It's an annoyance, but inevitable."*

"I don't feel hopeless. I just feel that I need to remain vigilant."

"I don't think things are hopeless, some genius will figure out how to get around all this."

"Does any annoyance ever stop there? There are always those that want to capitalize on knowledge of others and will stretch that envelope to collect more and more data. If not more than an annoyance [now], it will become more than that [in the future]."

Asked what would it take to turn them into privacy activists? One focus group participant said: *"If I found out that a company had been negligent in putting in reasonable controls to protect my information and then refused to help me, that would be the tipping point for me."*

When it comes to the future of privacy, most of the focus group participants were downbeat. Many cited the trend towards surveillance and data capture that to them seemed inexorable. Many also said they think younger Americans are not sensitive about personal privacy and that will shape the future. One focus group respondent spoke for many of the older members of the group in asserting: *"The next generation will say 'privacy? … What is that?"* Another quickly added: "*I really think that the next generation will not even understand the value of privacy. Privacy will be a thing of the past."*

Another focus group member argued that trends in technology drive changes that compromise privacy: "*Information retrieval is a way of life, but it inhibits human interaction."*

Another asserted: *"[The loss of privacy is] a huge harm – an impoverishment of our culture. Probably most great scientific and artistic achievements occur in privacy."*

And another gave voice to a commonly voiced theme that privacy changes are subtle and cumulative: *"I think privacy will be stripped away [from us], because people are permitting it – one trade at a time. The cameras for security evolve into cameras to ensure compliance. And once those are in, the next thing is easier to get in."*

1. The state of privacy

Americans frequently face choices about whether or not to share information about themselves in return for getting something that is potentially valuable to them. From retail stores that track customers' shopping behavior in exchange for discounts to online applications that offer free services in exchange for serving personalized ads to users, Americans regularly face the choice: Is it worth it to hand over my personal information in exchange for something else?

Of course, in some cases, people have little control over whether personal information about them is collected. As one respondent in the survey summarized:

> *"I share data every time I leave the house, whether I want to or not. Every time I use a credit card, every time I walk in 80% of the commercial establishments in the nation, every time I drive down streets in most any city or town in the nation, I'm being recorded in some fashion. The data is there, and it's being used, and there isn't a damn thing most of us can do about it, other than strongly resent it. The data isn't really the problem. It's who gets to see and use that data that creates problems. It's too late to put that genie back in the bottle."*

Another made the point that bargaining over personal information seems a perpetual part of modern life: *"I continually have to decide how much personal information to share in return for prizes/money."* Another added: *"Every day, the chance that your data is shared increases. All data are ultimately digitized."*

For the past two years, Pew Research Center surveys have mapped this complicated landscape and Americans' nuanced feelings about privacy and surveillance.

The surveys have found that Americans conjure an array of ideas when they think about privacy. They feel privacy is important in their daily lives in a number of essential ways, starting with the idea of not being under surveillance all the time and the appeal of being able to share ideas and secrets with others in a way that is unobserved. Yet, they have a pervasive sense that they are under surveillance when in public. Very few feel they have a great deal of control over the data that is collected about them and how it is used.

Moreover, Americans have low levels of trust in the government and business sectors that they associate with data collection and monitoring. They are not sure their core communications channels are secure, and they have exceedingly low levels of confidence in the privacy and security

of the records that are maintained by a variety of institutions in the digital age. Indeed, noteworthy numbers of them have suffered privacy breaches, especially younger adults.

While some Americans have taken modest steps to stem the tide of data collection, few have adopted advanced privacy-enhancing measures. They are divided about the value of government surveillance programs aimed at thwarting terrorists. And majorities expect that a wide range of organizations should have limits on the length of time that they can retain records of their activities and communications. Additionally, they say it is important to preserve the ability to be anonymous for certain online activities.

In the online focus groups for this study, the theme of contingency came up in responses to each scenario. Asked about the acceptability of surveillance cameras at a workplace where some thefts had occurred, one respondent said:

> *"It depends if the cameras are in public areas (i.e. hallways, public gathering areas, lobbies, etc.) and in storage areas where supplies or personal belongings are kept (i.e. closets, locker rooms, supply rooms) this would seem to be sufficient. Cameras that monitor personal work spaces would be invasive even to the most diligent employee with absolutely nothing to hide except perhaps a sneeze, a scratch, a clothing adjustment or just bending over wrong in front of the camera."*

Another respondent, explaining his answer about his physician inviting him to use an online medical records system, wrote:

> *"It depends if I think the site is secure enough to put my information on. If it was a weak site with low development I would not use it. If it was high security like a bank site I would use it."*

And yet another respondent, asked whether she would allow a tracking device placed on her car to monitor her driving habits perhaps leading to lower insurance payments, explained how these factors would shape her judgment:

> *"It depends on how much the discount would be and what their privacy policy would be. I would not agree to it if the data is shared with anyone at all, and I would want it to be stored only temporarily and securely."*

What's the public's mood? People's level of anxiety and hopefulness are all over the place

In light of these current and future concerns, participants in the focus groups were asked how much dismay or even anger they felt at the current state of things, and they offered a range of answers trying to pinpoint their level of concern.

> *"It's hopeless."*
>
> *"No, they are as bad as we make it sound."*
>
> *"I'm not hopeless, just resigned."*
>
> *"Loss of privacy is inevitable. I've accepted that."*
>
> *"Nothing is completely safe. That's just life in these times."*
>
> *"[Loss of privacy] is a major annoyance."*
>
> *"Not hopeless, necessarily – I think that the landscape has so fundamentally shifted that we have an entirely new paradigm to deal with."*
>
> *"I think people are not happy with everyone in their business."*
>
> *"It's bleak about privacy – the more controls the government enables the less privacy we have. We have lost a lot of privacy in the U.S. since 9/11 and are losing more every day, and it appears no one cares. The less freedom we have the less privacy we should expect."*

Some focus group participants tried hard to wrestle with the complexities of the subject, moving it beyond a binary situation of privacy or no privacy and speaking instead about how they tried to live out their views about privacy. A woman in one of the groups said: *"Monitoring in public places is completely different from being monitored in your own home, or in your bank accounts, and god knows what else. I went off Facebook for several years just because I assumed everything was being collected about me, and I wanted to avoid that. And, of course, there's also the matter of leaving a record behind of your political and other views that could be detrimental in certain cases. For instance, if you apply for a job, and the employer thinks your opinions are too liberal."*

Some are concerned about the future of privacy; some have hope for a technological fix

In online focus groups tied to the most recent Pew Research Center survey, people were often downcast about the future of privacy, as were many experts who participated in a wide and diverse canvassing by the Center last year about the long-term fate of privacy. A sampler of some of the participants' views from the most recent research:

> "*Our life has become an open book. What are you gonna do?"*
>
> *"Privacy as we knew it in the past is already gone. Privacy in the future will be very different. We will have very little about our daily lives kept private. Our important records such as banking and medical will become tighter, likely through biometric access, but I expect the hackers to keep up with even that technology to obtain what they want."*
>
> *"I think that there will be less and less privacy."*
>
> *"It's an annoyance that will mostly be fixed."*
>
> *"I think that the concept of 'privacy' no longer exists. I think it is more about 'informed consent.'"*
>
> *"I think law abiding citizens sit back way too much. There are a multitude of things we should be demanding legislation about as it is."*
>
> *"The future generation will ABSOLUTELY see privacy different. Millennials put EVERY aspect of their life on social media [and, have no] for the personal or financial safety. I feel that we are in a place where we can decide how to keep our information private, but the more and more companies require information from us for access to an app, our email accounts or even our bank accounts, it will be unavoidable to not release some of our information. IT is nothing to be hopeless about rather we need to continue to be vigilant with whom we share our information and for those we do share our information with, we need to ask questions and ensure our own safety first. People need to get on board that privacy of information is a thing of the past."*
>
> *"The law is way behind technology. Privacy was written for a non-digital world. Don't expect any privacy in the future."*

"I think a backlash is coming against too much intrusion. Privacy services will become popular."

The scenarios are explored in depth

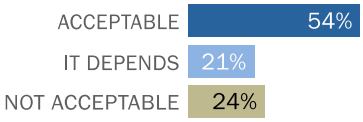
This report now turns to the individual scenarios and people's responses about whether they feel it is acceptable or not to agree to share personal information in return for a product, service or benefit that is being offered.

2. Scenario: Workplace security and tracking

Office surveillance cameras

Several co-workers of yours have recently had personal belongings stolen from your workplace, and the company is planning to install high-resolution security cameras that use facial recognition technology to help identify the thieves and make the workplace more secure. The footage would stay on file as long as the company wishes to retain it, and could be used to track various measures of employee attendance and performance.

Would this be acceptable to you or not?



Source: Survey conducted Jan. 28 – Feb. 16, 2015.

Note: Refused responses not shown.

PEW RESEARCH CENTER

One of the most important and persistent debates about surveillance involves the tradeoff between personal security and privacy. In previous research about national surveillance tied to terrorism-related investigations, Pew Research Center has found that a majority of Americans support the idea of government surveillance of others, including monitoring of American leaders, but oppose surveillance of Americans themselves.

One scenario in this survey places this tradeoff in the context of a workplace setting:

Several co-workers of yours have recently had personal belongings stolen from your workplace, and the company is planning to install high-resolution security cameras that use facial recognition technology to help identify the thieves and make the workplace more secure. The footage would stay on file as long as the company wishes to retain it, and could be used to track various measures of employee attendance and performance.

By a two-to-one margin (54% to 24%) a majority of Americans would find the installation of surveillance cameras and corresponding retention of data to be acceptable, while one fifth (21%) of adults say their consideration of this tradeoff would depend on the circumstances.

There are no statistically significant differences in people's answers to this question by different demographic groups: Men and women, young and old, and relatively well off and relatively poor are all equally likely to say this scenario is acceptable.

When asked to elaborate on their answers in an open-ended follow-up question, a number of those who felt the tradeoff was acceptable argued that companies have the right to install the cameras on property they own and to make it more secure for workers:

> *"The job has the right to do this already so I expect it. I just don't want them to get carried away."*
>
> *"My employer could choose to do this, but I might be unhappy about it. The boss is the boss."*
>
> According to one focus group participant: *"It would keep the workplace safe and may also get the employees to perform at their best."*

Others thought the idea was acceptable, as long as it applied to everyone:

> *"[It is OK with me] as long it involves all departments and employees, not just a particular group."*

Still others were anxious to know where the cameras would be placed, how persistent the surveillance would be and how long the records might be retained:

> *"Cameras to track people coming in and out of a building, locker room area or entering an office area are just fine and actually a good thing for security. Cameras tracking places where there is public involved are fine for security, such as lobby areas. Cameras tracking employees who handle sensitive data and money are fine, such as cash registers and those who handle data such as social security numbers, but the cameras should only be used for honesty issues, not performance. Cameras in non-cash/sensitive data areas in any workplace are just intrusive, such as in office areas. Cameras should never be used for performance issues. They should only be used for security issues such as like the ones I described."*
>
> *"It would depend on where in the workplace the cameras are installed. How will the footage be destroyed? If they have to track employees' attendance and performance this*

way, it seems the company does not trust its employees to come to work and do their jobs."

"It depends on whether I would be watched and filmed every minute of the day during everything I do."

"The information is not being used for what was the original purpose in collecting it. It's not clear employees would be told how long the data would be saved and who would have access. In any case, the original purpose would be OK with me, but then the monitoring should be stopped once the issue has been resolved."

"Security cameras = yes. Cameras to track attendance and performance = no way. That is just ridiculous. I find it dishonest the company says it's to make the workplace 'more secure.' That is a lie."

"Who would have access to the footage and how securely it would be stored?"

Still others felt that any scheme of this type is too intrusive:

"No Big Brother spying is good. Corporate America is screwing American citizens enough."

"Monitoring work by camera is insane."

Some were suspicious of the motives of any firm that would seek this kind of surveillance:

"This could very easily be abused and would hinder performance if every employee felt surveilled all the time."

"They say that it will only be used to see who has been stealing, but the reality is we all know that is not the truth."

"Because some employers are very abusive of their power to check on you."

"Because the company could save a lot of different feeds and then use them all at once to make a person look bad so they could just terminate them."

"It could come back and bite YOU. [I] used to be a union steward when I worked, and management already monitors everything you do. It sent to management when I clocked onto my computer in the morning, I got written up because I logged on before 8 a.m. All of our e-mails were monitored every day by an IT [information technology] company. Cameras were everywhere."

"The total use of the system is unacceptable. Identifying thieves is one thing, but this would be used in ways not intended."

"This idea just bothers me. The workplace should not feel like a prison in which you have everyone watching your every move, basically breathing down your neck at all times."

The possible long-term retention of the surveillance camera records made some respondents uncomfortable:

"There should be limits on how long the employer can keep the records or what they are allowed to do with the records. Additionally, the feeling of constantly being watched/monitored would not make for a good work environment. There are less intrusive means of preventing theft. This seems more like an excuse to install video performance monitoring."

"The company would be able to use it for situations that have nothing to do with the theft and they could keep and use the info as long as they like."

"One problem has nothing to do with the other. Use of cameras to deter theft is one thing, but to track employee is another. Fake excuse."

Some simply argued that the installation of surveillance cameras would not solve the problem:

"Because it's not for a limited purpose/time. Once cameras installed [it is] very difficult to go back. Over-intrusive in terms of capturing everyone's facial recognition and under-inclusive in terms of actually taking steps to identify and stop the thieves."

"This is not going to reduce people stealing. This is just going to cause good employees to be more micro-managed."

And the final word on this subject comes from someone who accepted the premise of the scenario, yet still would seek a job elsewhere:

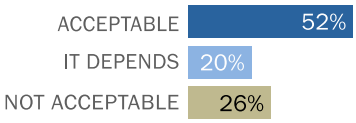
"When you accept employment you accept the fact that while you are on premises the company has the right to know how you are spending their paid time. That being said, facial recognition would most likely have me looking for another job. Petty theft happens in all facets of society. A total nanny state is not the answer. I will not give up my freedom and privacy for a false sense of security."

3. Scenario: Health information, convenience and security

Sharing health information

A new health information website is being used by your doctor's office to help manage patient records. Your participation would allow you to have access to your own health records and make scheduling appointments easier. If you choose to participate, you will be allowing your doctor's office to upload your health records to the website and the doctor promises it is a secure site.

Would this scenario be acceptable to you, or not?



Source: Survey conducted Jan. 28 – Feb. 16, 2015.

Note: Refused responses not shown.

PEW RESEARCH CENTER

Previous Pew Research surveys have found that Americans are quite sensitive about their personal health information and worry about how this information might be used in ways that negatively impact their ability to secure insurance, access credit or find jobs.

Still, the convenience of accessing one's health records or interacting with one's physician online has a relatively strong appeal. By a two-to-one margin (52% to 26%), more Americans would accept the following scenario:

A new health information website is being used by your doctor's office to help manage patient records. Your participation would allow you to have access to your own health records and make scheduling appointments easier. If you choose to participate, you will be allowing your doctor's office to upload your health records to the website and the doctor promises it is a secure site.

Some 20% say their response to a scenario like this would depend on the particular circumstances.

Those ages 50 and older are more likely than adults ages 18 to 49 to say this tradeoff would be acceptable to them (62% vs. 45%). Furthermore, those with some level of college education are

more likely than those whose education stopped at high school to find the deal acceptable (59% vs. 44%).

Very few of those who indicated this tradeoff was acceptable gave any additional explanation for their answer. Some argued that it was self-evident why easier access to their medical records and more convenient interactions with providers' offices would be appealing to them.

Others indicated their view on this tradeoff would be contingent on who could access their data, as well as how vulnerable they feel the doctor's website is.

> *"If it was with my current doctor and he showed me the site and how it was secure I may do it, because I trust him."*
>
> *"Well, it would probably be like any website. Look at all the ones that have been hacked so far. If I'm going to get hacked I would rather it be my medical records than my banking information. It would be nice to be able to know what your lab works are and not have to wait 2-3 weeks to go back to doctor to get results."*
>
> *"It's OK if it's my own HMO [health management organization] (Kaiser Permanente), but a third party website is unnecessary and unacceptable, [because] I want my health info kept confidential."*
>
> According to one focus group participant: *"I have Kaiser Permanente insurance. Kaiser has everything available. I can look up my cholesterol results going back 10 years and more. But that is not a public website, and I trust Kaiser Permanente, and they do very valuable research. I am even in a genetics study with them – they've got my DNA. But this is totally different from going through some third party website."*
>
> *"It depends on exactly what records are shared. It would have to be a very secure site for me to trust it. Scheduling appointments online wouldn't bother me though."*
>
> *"I need to know that my medical information will be encrypted and secure from online hackers."*
>
> *"My question is: Would there be any discount for me if helped them do their job? I want my records to stay personal, not on the internet."*

"Other than just the doctor's promise, I would want a document that contained the promise and was signed by the doctor."

"It would need to be HIPAA [Health Insurance Portability and Accountability Act, a law governing how patient privacy is protected] compliant and very few servers meet those guidelines."

"They would have to prove it's a secure site. Also there should be some sort of a major fine if it's not secure at all times."

"[It] depends on my approval of who would get this information in the future."

"I would want to better understand the actual security of the site and the true benefit to me vs. him/her."

A considerable number of those who found the tradeoff unacceptable went on to explain their responses. For many it was simply a matter of the security of the information – or lack thereof:

"There is no such thing as a secure site. Hackers are always finding entry points into databases. Insurance companies can afford to hire hackers. The gleaned database information would allow insurance companies to deny coverage to the patients whose information was compromised. Doctors charge excessive fees to patients to use and access this online record tool. Many patients cannot afford the online record service."

"My health records are my business and no one else's. No website is totally secure."

"No matter how safe you think the site is, it's not. Hackers can bypass anything if they choose to."

"Nothing is truly secure online. I don't go to the doctor very often nor do I like them, and I don't want my personal info on the WWW [World Wide Web] secure or not!"

"Do not trust doctors."

"What am I going to do if it turns out not to be a secure website? Sue the doctor???"

According to one focus group participant: *"With the government in charge of health care now, I am no longer allowing my doctors to put my information on the patient portals. I*

> *definitely don't like the kind of control the health industry is trying to gain in my personal life. I am offended by many of the seemingly 'none of your business' questions they are now asking at my doctor [appointments]. I refuse to answer them, and I tell them I am offended."*

Some worried that exposure of their health data would make them targets of customized pitches to buy more medicine or unnecessary treatments:

> *"My health records are confidential. I don't want them in the hands of someone unscrupulous or marketing companies possibly trying to recommend a drug or something based on a condition I may have."*

Others made references to the social problems that might result from unauthorized disclosure of the records:

> *"If these records ever leaked it could be devastating to people with certain diseases. I'm specifically thinking about stigmatized diseases like AIDS."*

And at least one respondent's medical records had been hacked in the past:

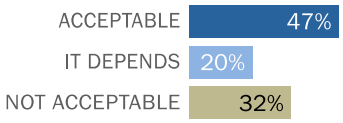
> *"My records were stored by USPS [United States Postal Service]. The system was hacked! Now my information – all of it – is out there."*

4. Scenario: Consumer loyalty cards and profiling

Retail loyalty cards

A grocery store has offered you a free loyalty card that will save you money on your purchases. In exchange, the store will keep track of your shopping habits and sell this data to third parties.

Would this scenario be acceptable to you, or not?



Source: Survey conducted Jan. 28 – Feb. 16, 2015.

Note: Refused responses not shown.

PEW RESEARCH CENTER

This is a scenario anchored in a familiar bargain that is offered in many existing retail environments. Many consumers already allow their shopping preferences to be tracked and sold to other companies in return for discounts on products, and some 47% of adults say they would be comfortable with the following scenario:

A grocery store has offered you a free loyalty card that will save you money on your purchases. In exchange, the store will keep track of your shopping habits and sell this data to third parties.

By comparison, 32% say it would not be acceptable, and another 20% say it would depend on the circumstances of the offer.

Those ages 50 and older are somewhat more likely than younger adults to say that this arrangement would not be acceptable: 39% of those 50 and older say this deal would not be acceptable, compared with 27% of those ages 18 to 49. In addition, those in households earning less than $30,000 per year are more likely than those in higher-income households to say this deal would be acceptable: 56% of those in lower-income households say the loyalty card bargain is acceptable vs. 43% of those in higher-earning households.

A number of those who find this scenario acceptable indicate that they are familiar with loyalty cards and/or already use these cards themselves. Yet even this group expresses concerns about how and under what circumstances their data are passed along to third parties:

"I use loyalty cards. As far as I can tell, the information is not being used inappropriately or specifically tied to me by third-parties, which I'm OK with."

"Well, they do this now. If [my data are] secure and I get the deals, it's OK."

"The 'selling to third party' part makes me worry. OTOH [On the other hand], I have and frequently use a Safeway rewards card, which I suspect has just such an agreement."

"I already participate in many 'loyalty' programs, but use pseudonyms so that I can determine the origin of the third-party contacts and trace back which store sold my consumer information."

"I want to choose who emails information to me."

"I would take the card to get discounts or coupon, but I wouldn't want them selling my information to third parties. That would be a violation of my rights."

Some of those who answered "it depends" to this scenario have different levels of trust depending on the company asking for their personal data. Others wanted more details about the specific bargains being offered:

"Sharing it with a third party generally indicates that you will be inundated with unwelcome email offers and you may even get unwanted calls. If they use the data for themselves I am fine with that since I use their services/products."

" [It depends on] whether I trust the company."

"Having the ability to control the information being sent would influence my decision."

"How much money would I be saving, and how much personally identifying information will be shared?"

"How many third parties will you be sharing with? Can I control what info is shared? Is it just my anonymous shopping data, or is my personal info attached?"

"[I would consider this] only if I could opt out on sharing with third parties."

"[It depends] on the type of store."

"I'm not sure what kind of stipulation would be acceptable, but if I had choice and knowledge of what companies would receive the information, I may be OK with it."

"I don't want to be personally identified – I am OK if I am an anonymous shopper."

"It depends on whether those third parties would contact me via phone, email or snail mail. If they just want to use my data, I suppose that's fine, but I don't want to be contacted or receive anything from those third parties. Keep it a one-way street. The only exception is if the grocery store gave me coupons based on what I bought."

"If the 'identifying info' on me is just my purchase habits and my loyalty card number – OK. If it includes phone, address, credit or debit card info, not too interested."

Those who said this arrangement was unacceptable took particular exception to the idea that data about their purchasing behavior might be sold to third parties after being collected by the retailer. Others expressed concern about how many unsolicited telemarketing calls might be generated by these personal shopping data:

"Third party selling is not acceptable. If I want one company to have my information, that's my choice, but not a bunch of other random companies."

"I don't want anything sold to third parties, because then I always get emails and mail that I didn't want."

"If I am spending my money in that store, they have no right to sell any information about me."

"First, I don't want you keeping track of what I buy, and second, I don't want what I do to be sold to a third party."

"Too many telemarketers are involved."

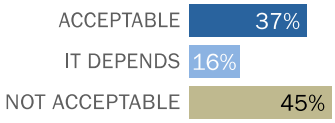
"My shopping habits are my own business unless I choose to sell the information to another party. Why should a different party benefit from personal info that they've 'gathered' about me?"

5. Scenario: Auto insurance discounts and monitoring

Auto insurance

Your insurance company is offering a discount to you if you agree to place a device in your car that allows monitoring of your driving speed and location. After the company collects data about your driving habits, it may offer you further discounts to reward you for safe driving.

Would this be acceptable or not?



Source: Survey conducted Jan. 28 – Feb. 16, 2015.

Note: Refused responses not shown.

PEW RESEARCH CENTER

As mobile devices, GPS systems and sensors proliferate there are more and more opportunities for people to be offered goods and services at rates that are tied to their behaviors. For instance, since 1998 Progressive insurance has been offering people the chance to install telematics devices that track their driving behavior and offering discounts to those who perform well. For many years, the monitoring was only tied to discounts for good driving, but starting in 2013, the company began a system that charged poor drivers with higher rates.

Some 45% say they would find the following tradeoff of personal information for benefits to be not acceptable:

Your insurance company is offering a discount to you if you agree to place a device in your car that allows monitoring of your driving speed and location. After the company collects data about your driving habits, it may offer you further discounts to reward you for safe driving.

An additional 37% say it would indeed be acceptable, while 16% say their decision would depend on the circumstances. There are no major differences by gender, age or household income in people's answers about this scenario.

Those who find this tradeoff acceptable sometimes justified their answer by their view that their current behavior is something worth rewarding:

"My driving is local and I am a safe driver."

"[This] sounds like a good deal."

According to one focus group participant*: "Driving is a privilege and not a right. With all the monitoring going on while you drive it is only a matter of time until all these vehicles on the road report direct to your insurance agent."*

Those whose answer was "it depends" expressed concerns about the specific types of driving data that might be collected, as well as the time frame for data retention:

"The recording of location seems unnecessary. Speed is fine [to collect]."

"I am not comfortable having my location tracked. I feel this is an invasion of my privacy and a safety risk."

"Monitoring driving habits might be fine to allow insurance discounts, but do they really need to know where you are? No privacy. I am an honest person, but I don't like to be checked up on and the whole world knowing what I do."

"It would depend on what else they do with the information. As long as the information was kept private, in house and used to offer legitimate discounts – not sold to third parties for exploitation."

"I would have to know more. I like the part about the speed. But, as far as where a person goes, it is their private personal business. I would agree to allow them to track distance or mileage, but, not actual location."

"I don't like the idea of someone tracking my driving destinations and knowing my whereabouts all the time. At the same time, I like saving money. It would depend on how much money I could save."

"Depends on what security measures are taken to ensure no one but the insurance could have access to the information."

"Depends on how much money I would save and that it could not increase my cost of insurance if they did not deem me a 'perfect' driver."

"It needs to be for a limited time."

Those saying this bargain would not be acceptable to them offered a wide range of justifications. Some of these justifications related to their own behavior; others related to their concerns about potential behaviors by their insurance company:

"I speed. …"

"I don't drive safely."

"The discounts aren't worth it."

"I do not like to be constantly watched and judged."

"Because I drive like a crazy lady."

"Because if they know that I drive fast, roll through stop signs and red lights, they would do the opposite and raise my rates. I live in the fast lane and want to keep it a secret."

"They may be describing it as a benefit to me, but it really feels more like they would be gathering data to deny claims or raise rates – by claiming speeding or some other such trumped-up charge with which there would be no way to defend me as an individual against a giant insurance company."

"I don't like anything attached to my car monitoring me."

"A person cannot control potential driving scenarios. Drivers will get punished when they are encumbered by construction zones in their area and are faced with stop-and-go traffic. Some drivers have no alternative routes to use to avoid these situations. Devices such as 'Snapshot' by Progressive punish drivers for driving defensively. These devices punish rather than reward the driver using the device."

"The insurance company should offer my coverage based upon my driving record/history/demographics, not by playing big brother."

"I am a safe driver and have not even been in an accident in over 35 years, much less been at fault in an accident. My record should qualify me for a discount, regardless of whether I occasionally exceed the speed limit."

"Afraid prices would go up."

"How I drive is my own business."

"I am a safe driver, but I tend to speed on the highway. I wouldn't want that to cost me more for insurance."

"I feel like this information would be used against me if I got into an accident. For example, the insurance agency will look at the data and say that I was speeding right before the accident and claim that the accident was my fault. I also feel as though law enforcement would attempt to use this information in the event of a criminal case."

"I do not trust insurance companies to do anything good."

"It's inappropriate for other parties to be able to track where I am. It's bad enough that it's traceable via cellular technology."

"I pay for insurance at the established rate given my driving record (one speeding ticket in 1967, 48 years ago, at a speed trap in Ohio). I don't need to have anyone (who I pay) monitor my activities while driving!"

"How long will they keep these records? And could there be legal ramifications if these systems prove that the client has in some way broken the law? It just sounds like an easy way to police the public even more for the sake of a 'deal.'"

"The speed is fine. But if they hike my rates due to location; for example, if they perceive an area to be unsafe, I wouldn't think that is fair. Lots of people work/live in high crime areas, and I don't think they should be penalized for that."

"I know it would encourage drivers to be safer and that is good, but that is too much like '1984' for me."

Some people gave answers tied to their particular circumstances with their auto insurance companies:

"They could potentially charge me a premium for exceeding their arbitrary standards of safety, as well. My insurance company already pulls my credit worthiness (how the hell does my FICO relate to my driving ability?) and tracks the VINs [vehicle identification

*numbers], drivers and driver's records of all my cars/drivers. My rates just went up 30% in January with *no* explanations as to why. I am changing insurance companies as of the 30th and will be saving $500/year."*

"I actually evaluated such a device offered by my insurance. Unfortunately, the device was easily removed in case the car was stolen, and also the device was not that easily secured under the dashboard. I decided that the reward was not worth the effort."

"I tried that once. I am a good driver, and I don't drive very much at all, and they still did not give me a discount so that makes you wonder!"

"I had one of those and only got $1 discount."

"This option was presented to me by my insurance company. If they can identify how I drive, they can identify where I am, next what I am doing every moment. … I am responsible, doing what is considered appropriate, but I do not have to prove that every moment. Also data can be misinterpreted. If I accelerate to avoid a bad situation, how will it be perceived by a computer chip? If I am driving way under the speed limit and making many stops, am I a poor driver or am I in gridlock or traffic emergency?"

"The idea of monitoring just my driving isn't true, it would do more than that and it's the 'more' that I can't be sure of."

"Its use could be applied in so many other ways. Insurance company should base their rates on claim/accident data alone. They should not directly control my driving or freedom of movement with collecting that kind of data."

"Allowing the insurer to define what is considered 'safe' is like hiring the fox to guard the hen house."

"If by not having this device your rates would raise dramatically I would do it, but my rates are pretty low already because of my driving record, so I don't know that it would be necessary."

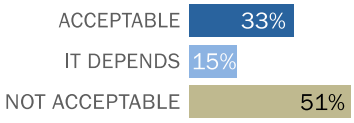
"My insurance rates should only be based on no accidents, not penalized by how I choose to drive, based on some set of criteria they deem acceptable."

6. Scenario: Personal details and advertisements

Free social media

A new social media platform is being used by your former high school to help manage communications about a class reunion. You can find out the basic information about the reunion over email, but your participation on the social media site would reconnect you with old friends and allow you to communicate more easily with those who are attending. If you choose to participate, you will be creating a profile using your real name and sharing a photo of yourself. Your access to the service is free, but your activity on the site would be used by the site to deliver advertisements it hopes will be appealing to you.

Would this scenario be acceptable to you, or not?



Source: Survey conducted Jan. 28 – Feb. 16, 2015.

Note: Refused responses not shown.

PEW RESEARCH CENTER

Today a wide range of online services offer their product free of charge in return for tracking users' activities in order to profile them for the purposes of serving them advertisements. This bargain anchors a wide range of commercial services on the web, from social media platforms to search engines to web-based email clients.

The following scenario attempted to unpack Americans' attitudes about this bargain:

A new social media platform is being used by your former high school to help manage communications about a class reunion. You can find out the basic information about the reunion over email, but your participation on the social media site would reconnect you with old friends and allow you to communicate more easily with those who are attending. If you choose to participate, you will be creating a profile using your real name and sharing a photo of yourself. Your access to the service is free, but your activity on the site would be used by the site to deliver advertisements it hopes will be appealing to you.

By a 51% to 33% margin, Americans generally do *not* find this bargain acceptable. The most striking difference in views on this question pertains to age: Some 40% of those under age 50 say this deal *would* be acceptable, compared with only 24% of those ages 50 and above.

Notably, some of the detailed responses to this question – especially among those who do not currently use social media – suggest a general dislike of social media and the information that people share on those platforms. In other words, there is a possibility that in answering this question, people's general aversion to the whole idea of social media colored their views of the "bargain" being presented in the scenario.

Those who were willing to consider this tradeoff often described their outer permissible boundary for such a deal. Some of these "it depends" respondents also noted that their preference would be to use an existing social media site for the task at hand, rather than a new one.

> *"It depends on how the ads are delivered to me."*
>
> *"Acceptable until you use my likeness or information in an advertisement. That I would never agree to."*
>
> *"What other information about me was required? If only name and picture, then OK."*
>
> *"I would only want to see advertising in that website, not in my personal email."*
>
> *"If most of the platform would be items of high interest to me, I would be willing to 'give up' a little of myself to enjoy the parts I am interested in."*
>
> *"Name is OK but no photo, and I would not like to receive advertisements."*
>
> *"If it is a new service I would not join, I would join a group on a platform which I already use."*
>
> *"I would not want the site delivering to companies I did not want to be bothered with."*
>
> *"It would depend on how secure my information is, and if my data would be sold or provided to another party."*

"I don't see this as a gross invasion of privacy, all the information that would be gathered about me is certainly already available online somewhere else. I just wouldn't care enough to create another internet profile."

"As long as the amount of email wasn't overwhelming."

"It would depend on if I could easily delete this account if I didn't like how many ads I received."

This was the scenario that elicited the greatest number of comments about the ubiquity of ads online and the annoyance they cause:

"If I have the option to suppress my email address or turn off advertisements, then I would join the site."

"I hate receiving advertisements on the internet from people and companies that do not interest me. It creates so much spam."

"Sounds like what Facebook currently does - and the ads are intrusive and non-relevant. [It] takes away from purposes of joining site to begin with."

Those who viewed this scenario as unacceptable cited a variety of reasons – often starting with their concerns about being profiled based on their personal connections and interests and having marketing campaigns tailored to those profiles:

"I do not use social media now because of this. [It is] marketing I do not like, and [I] do not participate anywhere this is used."

"Although I understand this scenario is already standard practice, it uses information collected about me in a manner not for my benefit, without my consent. It would affect how I use the reunion site or whether I even join the site at all."

"Do not want to view excessive ads and do not want to create more profiles."

"Advertised as 'free,' but it isn't. I pay, but with my attention span rather than a monetary fee. Too costly, and based on a lie."

"I wouldn't use it or I might make one post on the site about contacting me a different way so those who want to connect could in the ways I am willing to use. Then delete my account. I put as little personal information on social media sites as possible. I just don't like sharing."

For some people, the prospect of another social media platform itself was another turn off. Some expressed worry about posting information about themselves on such a semi-public platform:

"Not a big fan of social media."

"I don't use social media, I don't like that anyone can graze, or as some of the girls call it 'creep,' which is to look just because you are there."

"I dislike social media. [There are] too many ways for too many people to learn things about me."

"I would feel like I am being put on display."

"Not that attached to my high school, and can communicate with those I want through other means."

"WE CAN FIND OUR WAY EASILY TO COMMUNICATE WITH OUR OLD FRIENDS AND HAVE A CLASS REUNION WITHOUT THE NEED OF A SOCIAL MEDIA PLATFORM. WHY BOTHER TO EXPOSE OURSELVES TO THE AD COMPANY."

"I have enough social media sites to manage. I'd rather they use Facebook. The privacy settings are similar to what's described and those are fine by me. But I don't want to start using another site."

"I'll get the info at the reunion anyway. Then I can choose who I want to contact."

Some of those who balked at this arrangement felt that the supposed "benefit" of reconnecting with former classmates was not terribly enticing in the first place:

"I don't care enough about high school to go through these steps."

"I have no desire to keep in contact with people from high school."

"I have no interest in seeing my classmates ever again."

And one person felt this arrangement would defeat the whole purpose of the reunion – the delight and surprise of catching up with old friends.

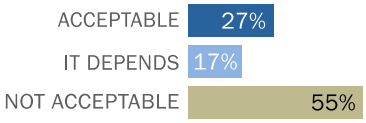
"I would rather wait until the reunion to see friends and teachers. Like it has always been before email. Or it would take the fun out of it."

7. Scenario: Home activities, comfort and data capture

Smart thermostat

A new technology company has created an inexpensive thermostat sensor for your house that would learn about your temperature zone and movements around the house and potentially save you on your energy bill. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house like when people are there and when they move from room to room.

Would this be acceptable or not?



Source: Survey conducted Jan. 28 – Feb. 16, 2015.

Note: Refused responses not shown.

PEW RESEARCH CENTER

The emergence of "smart" home devices and appliances has long been anticipated by both science-fiction writers and technology enthusiasts. In recent years, a number of firms have begun initiatives related to the Internet of Things, particularly in the realm of smart homes and appliances. A 2012 canvassing of technology experts by Pew Research Center found widely varying prophecies about whether smart systems would live up to their promise and take hold among consumers in the ways that forecasters were predicting.

Smart thermostats, which have often been promoted as a way to save energy and promote personal safety, are some of the earliest smart-home devices to gain a foothold in the marketplace. However, Americans are not generally comfortable with the implicit tradeoffs outlined in the following scenario:

A new technology company has created an inexpensive thermostat sensor for your house that would learn about your temperature zone and movements around the house and potentially save you on your energy bill. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house like when people are there and when they move from room to room.

Some 55% of adults find this a "not acceptable" scenario, while 27% say it is acceptable. Another 17% say "it depends" on the particulars of the arrangement. Those ages 50 and older are among the most likely to say it is not acceptable: 69% say this, compared with 48% of those under age 50.

Many of those who weighed this scenario were focused on what specific information is collected, who it is shared with, and what happens to their data after it is captured:

> *"[This would be OK with me] as long as others do not know my name and or location."*
>
> *"A learning thermostat is a great idea and exists already. But sharing data about my movements with someone else 'on the other end' is not acceptable. That's an invasion of privacy. Nobody needs to know my movements within my house."*
>
> *"I would be concerned that the data could be used to find out when nobody was home – I don't want anyone tracking what I do in my home."*
>
> *"It would depend more precisely on the details of the company's privacy statement. What can they use the collected information for? And do they share it with third parties? If they can use the information for anything but controlling my house's HVAC [heating, ventilation and air conditioning], I would be very hesitant to participate."*
>
> *"Movements around the house are fine (for example, only heat bedrooms at night), but I would not want it to record when people are or aren't there (potential security risk)."*
>
> *"I would be willing to use this service if they provided the thermostat for free and paid me a small amount each month to allow them to collect data on my household."*
>
> *"Distribution to 3rd parties and data security would be key. I wouldn't want just anyone knowing my habits of coming and going. Might as well leave a sign for the burglars."*

Many invoked the specter of security issues: As one respondent put it, "The security risks are not outweighed by the benefits." Others objected to their data being captured in a space – their home – that heretofore had been private:

> *"My house is too small, and/or the upgrades necessary for my house to 'zone' the HVAC for different locations would be cost-prohibitive. It is my castle, and nobody needs to know how long I or any member of my family takes a shower or makes a meal."*
> *"Knowledge is control. My utility company already chastises me for not being more*

'efficient' as compared to my neighbors; I don't need them to tell me to take quicker showers, or potentially charge me a 'shower premium!'"

"Crosses a line – too intrusive. Goes into creepy zone of being watched!"

"No need for this camel to have its nose in my tent. Too voyeuristic."

"It is creepy to think someone is following you around, but the idea is a good one. Would have to know how intrusive 'basic activities' are."

"What I do and which room I am in my home is no one's business but mine."

"Don't want others to know when the house is unoccupied."

"I don't want that info possibly hacked."

According to one focus group participant:*" I would be afraid that someone would hack into the data & use it to determine when your house is no occupied."*

Others made the case for human choice and agency over assistance from a smart gadget. If people truly cared about energy safety and remote monitoring of their security, this argument goes, they would arrange for it themselves:

"I already, cut-to-the-bone, have a low electricity bill; this thermostat will not benefit me. I don't use the heater or air conditioner."

"I control my thermostat. Nobody else needs to have any sort of control over how I cool/warm my house."

"My home. My temperatures. My control."

"All of this stuff is way too invasive of my personal space! It's like they all want to be in control of everyone at all times. Know what we are doing etc. No thank you."

"Because in your home you are not being watched or tracked and that should be your one place away from all that sensor nonsense."

Acknowledgments

This report was made possible by The Pew Charitable Trusts. It is a collaborative effort based on the input and analysis of the following individuals:

Primary researchers

Lee Rainie, *Director, Internet, Science, and Technology Research*
Maeve Duggan, *Research Associate*
Michaela Hoffman, *Research Intern*

Research team

Aaron Smith, *Associate Director, Research*
Andrew Perrin, *Research Assistant*
Claudia Deane, *Vice President, Research*
Mary Madden, *Senior Researcher*

Editorial and graphic design

Margaret Porteus, *Information Graphics Designer*

Communications and web publishing

Shannon Greenwood, *Assistant Digital Producer*
Dana Page, *Senior Communications Manager*

Other reports from Pew Research Center project on the topic of privacy and security online can be found at: www.pewresearch.org/topics/privacy-and-safety/

Methodology

The majority of analysis in this report is based on a Pew Research Center survey conducted between Jan. 27 and Feb. 16, 2015, among a sample of 461 U.S. adults ages 18 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 January 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- to 60-minute online focus group chat sessions. For the second survey whose results are reported here, 461 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 80 panelists participated in one of nine online focus groups conducted during January 2015. Sampling error for the total sample of 461 respondents is plus or minus 5.8 percentage points at the 95% level of confidence.

The detailed discussion that follows is for the primary survey of 461 adults:

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 cellphones 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 Aug. 5, 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, 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 461 respondents is plus or minus 5.8 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	461	5.8 percentage points
Men	235	8.1 percentage points
Women	226	8.3 percentage points
18-49	230	8.0 percentage points
50+	231	8.4 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.

Topline Questionnaire

PEW RESEARCH CENTER
PRIVACY PANEL SURVEY #4 TOPLINE
JANUARY 27-FEBRUARY 16, 2015
TOTAL N=461 ADULTS, AGES 18 AND OLDER
SURVEY CONDUCTED ONLINE

MARGIN OF ERROR FOR ALL ADULTS IS +/- 5.8 PERCENTAGE POINTS

Sometimes people are willing to share some personal information in exchange for certain benefits. For each of the following scenarios, please indicate whether or not you would be willing to share information about yourself in exchange for getting something you might need or enjoy…

PROGRAMMING NOTE: RANDOMIZE Q2A-Q2G SETS]

AMONG ALL ADULTS [N=461]

Q2a. A grocery store has offered you a free loyalty card that will save you money on your purchases. In exchange, the store will keep track of your shopping habits and sell this data to third parties. Would this scenario be acceptable to you, or not?

47 Yes

32 No

20 It depends

1 Refused

52 NET No/Depends

AMONG ALL ADULTS [N=461]

Q2b. A new health information website is being used by your doctor's office to help manage patient records. Your participation would allow you to have access to your own health records and make scheduling appointments easier. If you choose to participate, you will be allowing your doctor's office to upload your health records to the website and the doctor promises it is a secure site. Would this scenario be acceptable to you, or not?

52 Yes

26 No

20 It depends

1 Refused

46 NET No/Depends

AMONG ALL ADULTS [N=461]

Q2c. A new social media platform is being used by your former high school to help manage communications about a class reunion. You can find out the basic information about the reunion over email, but your participation on the social media site would reconnect you with old friends and allow you to communicate more easily with those who are attending. If you choose to participate, you will be creating a profile using your real name and sharing a photo of yourself. Your access to the service is free, but your activity on the site would be used by the site to deliver advertisements it hopes will be appealing to you. Would this scenario be acceptable to you, or not?

33 Yes

51 No

15 It depends

1 Refused

66 NET No/Depends

QUESTION 2D – NOT REPORTED

AMONG ALL ADULTS [N=461]

Q2E. YOUR INSURANCE COMPANY IS OFFERING A DISCOUNT TO YOU IF YOU AGREE TO PLACE A DEVICE IN YOUR CAR THAT ALLOWS MONITORING OF YOUR DRIVING SPEED AND LOCATION. AFTER THE COMPANY COLLECTS DATA ABOUT YOUR DRIVING HABITS, IT MAY OFFER YOU FURTHER DISCOUNTS TO REWARD YOU FOR SAFE DRIVING. WOULD THIS SCENARIO BE ACCEPTABLE TO YOU, OR NOT?

37 Yes

45 No

16 It depends

1 Refused

62 NET No/Depends

AMONG ALL ADULTS [N=461]

Q2F. SEVERAL CO-WORKERS OF YOURS HAVE RECENTLY HAD PERSONAL BELONGINGS STOLEN FROM YOUR WORKPLACE, AND THE COMPANY IS PLANNING TO INSTALL HIGH-RESOLUTION SECURITY CAMERAS THAT USE FACIAL RECOGNITION TECHNOLOGY TO HELP IDENTIFY THE THIEVES AND MAKE THE WORKPLACE MORE SECURE. THE FOOTAGE WOULD STAY ON FILE AS LONG AS THE COMPANY WISHES TO RETAIN IT, AND COULD BE USED TO TRACK VARIOUS MEASURES OF EMPLOYEE ATTENDANCE AND PERFORMANCE. WOULD THIS SCENARIO BE ACCEPTABLE TO YOU, OR NOT?

54 Yes

24 No

21 It depends

1 Refused

45 NET No/Depends

AMONG ALL ADULTS [N=461]

Q2G. A NEW TECHNOLOGY COMPANY HAS CREATED AN INEXPENSIVE THERMOSTAT SENSOR FOR YOUR HOUSE THAT WOULD LEARN ABOUT YOUR TEMPERATURE ZONE AND MOVEMENTS AROUND THE HOUSE AND POTENTIALLY SAVE YOU ON YOUR ENERGY BILL. IT IS PROGRAMMABLE REMOTELY IN RETURN FOR SHARING DATA ABOUT SOME OF THE BASIC ACTIVITIES THAT TAKE PLACE IN YOUR HOUSE LIKE WHEN PEOPLE ARE THERE AND WHEN THEY MOVE FROM ROOM TO ROOM. WOULD THIS SCENARIO BE ACCEPTABLE TO YOU, OR NOT?

27 Yes

55 No

17 It depends

1 Refused

72 NET No/Depends

[SHOW Q3A-D ON THE SAME PAGE; SP]
[RANDOMIZE ORDER OF ITEM A-D INSERTS]
AMONG ALL ADULTS [N=461]

Q3 In the course of making decisions about what personal information to share with various companies, at any point in the last **month** have you felt any of the following things?

First at any point, have you felt...

	Yes	No	Refused
a. Discouraged with the amount of effort needed to understand what would be done with your data	35	61	5

Next at any point, have you felt... ...

b. Confused by the information provided in a privacy policy	38	59	3

Next at any point, have you felt... ...

c. Confident that you understood what would be done with your data	50	47	3

Next at any point, have you felt… …

d. Impatient because you wanted to learn more but needed to make a decision right away	29	68	3