The McAfee Safety Series

Smart Home Security Guide

Table of Contents

Smarter Homes & Gardens 3

Protecting your smart devices—and your privacy 5

Steps for a more secure network and smart devices 5

Using the new Matter technology: the emerging standard for the smart home 8

Balancing your security, privacy, and your smart home 10

Shopping for smart devices the smart way 12

Plenty of smart devices, yet few standards for smart device protection 13

Shopping smarter for smart devices 14

Smart speaker privacy 17

So, are smart speakers listening in? 17

Is someone on the other end of my smart speaker listening to my recordings? 19

Setting up your smart speaker for better privacy 20

Looking forward to your connected home 21

About McAfee 23

Smarter Homes & Gardens

With your voice, you dim the lights and cue up some quiet music to close out the day. The front doorbell rings and you check to see who's there from the LCD screen on your refrigerator. In the garden, your tomatoes are looking red and ripe, ready for picking, thanks to the connected sprinkler system that monitors the weather, soil, and water usage by your plants.

Welcome to your smart home, full of connected devices and conveniences.

There's no doubt that we've seen a proverbial explosion of smart devices in the marketplace—coffeemakers, door locks, sprinkler systems, lights, refrigerators, and on and on. And there's also no doubt that people have been buying them up, to the tune of more than $33 billion a year[1] and climbing.

And very likely, with one device will come many others, to the point where some homes will largely run on a mix of apps, voice commands, and internet connectivity.

Yet wherever there's connectivity, there's a need for security.

Any device connected to the internet must be protected. Even if it's something as innocuous as a smart wall outlet. Reason is, your home network is only as strong as its weakest security link. And many smart devices don't come with the best security out of the box. Hackers know this. By compromising a device like a smart wall outlet, a hacker can gain access to the rest of the network and the devices and data on it.

But how do you protect a smart wall outlet, along with that smart coffeemaker, door lock, and refrigerator?

This guide will show you how. We'll cover the basics of protection, how to shop for more secure smart devices, plus talk specifically about smart speakers and protecting your privacy while using them.

Let's get started.

Protecting your smart devices—and your privacy

With waves of smart home devices rolling out at the rate they are, it's easy to get caught up in the rush of what's possible and bask in the cool factor. What's sometimes less easy is taking a moment to ask some questions—is this device secure, is it supported, is it something that can infringe on my privacy? After all this is your home we're talking about here. If you're connecting portions of it to the internet, you'll want assurances that it's safe from both a security and privacy standpoint.

Steps for a more secure network and smart devices

As for security, you can take steps that can help keep you safer. Broadly speaking, they involve two things: protecting your devices and protecting the network they're on. These security measures will look familiar, as they follow many of the same measures you can take to protect your computers, tablets, and phones.

Grab online protection for your smartphone

Many smart home devices use a smartphone as a sort of remote control, not to mention as a place for gathering, storing, and sharing data. So whether you're an Android owner or iOS owner, protect your smartphone so you can protect the things it accesses and controls—and the data stored on it too.

Don't use the default—Set a strong, unique password

One issue with many IoT devices is that they often come with a default username and password. This could mean that your device and thousands of others just like it all share the same credentials, which makes it painfully easy for a hacker to gain access to them because those default usernames and passwords are often published online. (Baby monitors are a classic example.[2]) When you purchase any IoT device, set a fresh password using a strong method of password creation, such as ours. Likewise, create an entirely new username for additional protection as well.

Use multi-factor authentication

Online banks, shops, and other services commonly offer multi-factor authentication to help protect your accounts—with the typical combination of your username, password, and a security code sent to another device you own (often a mobile phone). If your IoT device supports multi-factor authentication, consider using it there too. It throws a big barrier in the way hackers who simply try and force their way into your device with a password/username combination.

Secure your internet router too

Another device that needs good password protection is your internet router. Make sure you use a strong and unique password there as well to help prevent hackers from breaking into your home network. Also consider changing the name of your home network so that it doesn't personally identify you. Fun alternatives to using your name or address include everything from movie lines like "May the Wi-Fi be with you" to old sitcom references like "Central Perk." Also check that your router is using an encryption method, like WPA2 or the newer WPA3, which will keep your signal secure.

Upgrade to a newer internet router

Older routers may have outdated security measures, which may make them more prone to attack. If you're renting yours from your internet provider, contact them for an upgrade. If you're using your own, visit a reputable news or review site such as Consumer Reports for a list of the best routers that combine speed, capacity, and security.

Update your apps and devices regularly

In addition to fixing the odd bug or adding the occasional new feature, updates often address security gaps. Out-of-date apps and devices may have flaws that hackers can exploit, so regular updating is a must from a security standpoint. If you can set your smart home apps and devices to receive automatic updates, even better.

Set up a guest network specifically for your IoT devices

Just as you can offer your guests secure access that's separate from your own devices, creating an additional network on your router allows you to keep your computers and smartphones separate from IoT devices. This way, if an IoT device is compromised, a hacker will still have difficulty accessing your other devices on your primary network, the one where you connect your computers and smartphones.

Using the new Matter technology: the emerging standard for the smart home

Outfitting your smart home recently got a whole lot easier.

Figure 1. Matter logo

A new industry standard called Matter aims to remove a big barrier in smart home technology,[3] one that makes different smart home devices compatible with any smart home platform—something that wasn't possible until now.

For years, different smart home devices have run on several different competing platforms, such as Amazon Alexa, Apple Home, Google Assistant, or Samsung SmartThings. None of which were compatible with each other. For example, a doorbell camera built for one platform wouldn't work with the LCD screen on a fridge built for another platform. And that created headaches for homeowners. It forced them to pick one platform over another and only use devices built for that platform.

Matter aims to remedy that. It's hailed as a unifying technology that will make all those devices work together. With its launch in October of 2022, we may start to see the vision of the smart home come true—a place where all your connected stuff works together with just the sound of your voice or a tap on your phone, regardless of manufacturer.

With that, let's take a closer look at the new Matter protocol and what it offers, along with a look at security and privacy for smart home devices in general.

How does Matter work with connected homes?

Spearheading Matter is the Connectivity Standards Alliance, a growing body of hundreds of companies working together to create and support this new standard, which includes recognizable names like Amazon, Apple, Google, and Samsung. With Matter's version 1.0 launch, expectations look high for the industry and consumers alike.

Beyond creating cross-compatibility where there was none before, Matter also creates a more energy-efficient, secure, and reliable network for your smart home devices.

Figure 2. A smart device featuring the Matter logo

Using a networking technology known as Thread, it can run independently of your internet connection, so if your internet goes out, you can still control your smart devices locally. Likewise, if a device within the Thread network fails, it won't bring down the entire network, thanks to the way Thread meshes the devices together.

And unlike previously, owners of smart home devices won't need a dedicated hub to control them. Other devices like smart speakers can serve as a controller if they like.

Security factors into the design as well. Matter uses a combination of encryption and blockchain technology to secure transmitted data and ensure that only the devices you trust can use the network.[4] Considering that you may be heating your home, warming up your oven, or even locking your front door with your smart devices, security features like these only make sense.

Several manufacturers have announced that they will create upgrade paths for existing devices so that consumers can take advantage of Matter. From there, new devices emblazoned with the Matter logo will hit the marketplace, which will help you easily spot this new standard as you shop.

Balancing your security, privacy, and your smart home

Thinking about connected homes more broadly, a few question marks remain when it comes to privacy. And important question marks at that.

Imagine for a moment what a highly connected home might look like—and all the data those connections will generate. That data will show what time of day your front door tends to unlock and lock when family members go to and from work, school, or what have you. It'll also show when you tend to turn on your lights, cook your dinner, or turn on the house alarm for the night. And there are smart speakers to consider here as well. Your commands, searches, and requests flow through them as well.

Some of this data passes along locally on your network. Other data gets passed along the internet and into a company's cloud service for processing. Additional data may get sent to third parties as well. Joint research conducted by Northeastern University and Imperial College London found that 57% of the smart devices they studied connected with third parties.[5]

In short, a smart home generates plenty of data, which may then travel to companies and third parties in ways that you may not be aware of.

This is where data privacy policies come into play. As consumers have become increasingly aware these days, not every company treats personal data the same way. Different companies have different policies around what data they may collect and then what they do with that data. Some may sell it to data brokers for profit or share it with third parties like insurance companies, government agencies, law enforcement, and others according to findings published by some industry groups.[6] Still others may not sell that data, yet they will share it with third parties for analysis or use it to fuel their own advertising campaigns or advertising platforms they own. And of course, there are others who collect and analyze the bare minimum, and keep that data to themselves.

The United States, the United Kingdom, and the European Union have recently enacted laws protecting what data can be collected, how it is used, and what rights you have regarding any data collected about you. You can read about the different privacy laws here General Data Protection Regulation (GDPR) in the European Union (https://gdpr.eu/what-is-gdpr/) and here https://cppa.ca.gov/regulations/consumer_privacy_act.html.

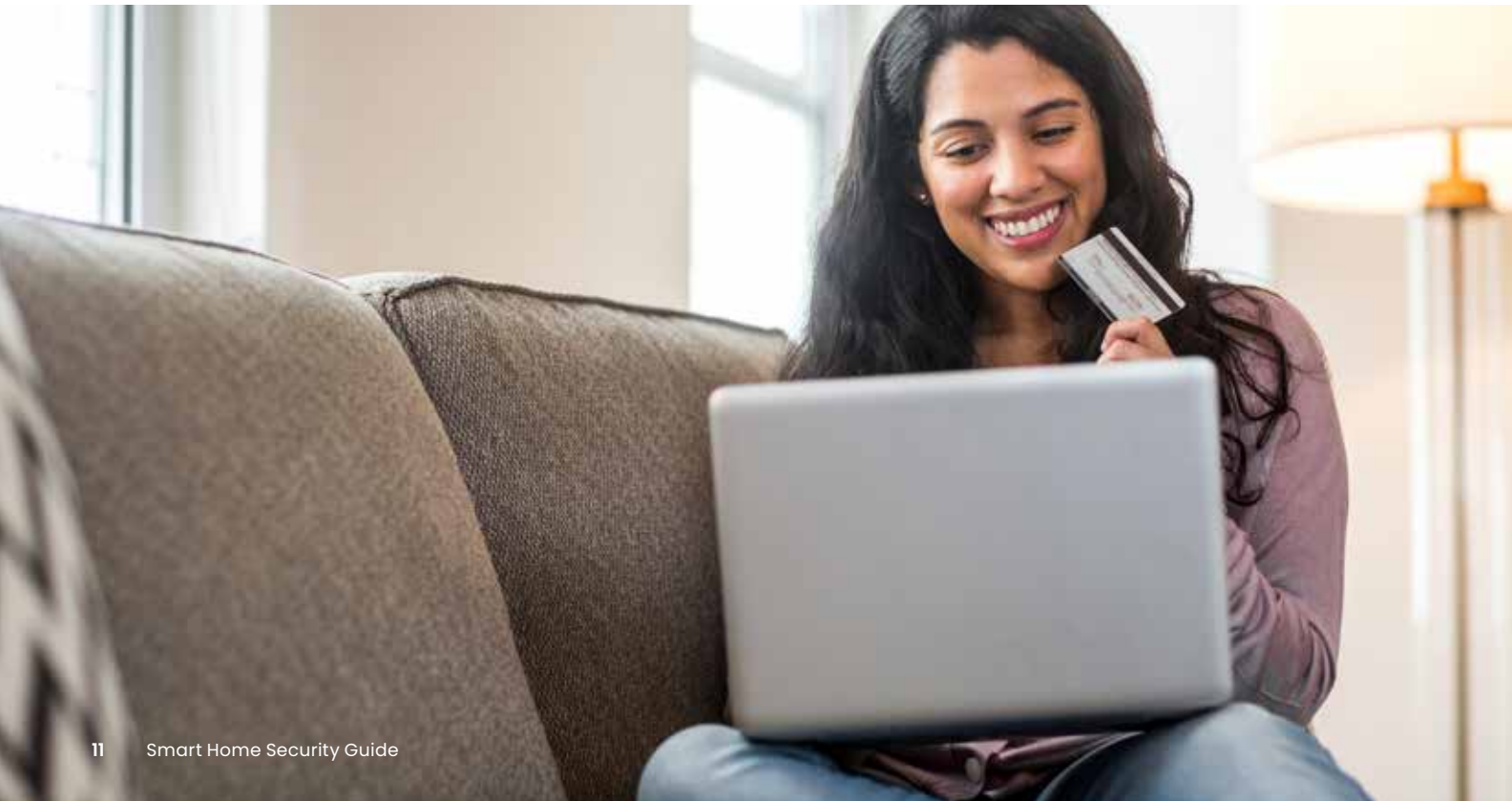
So how do smart devices factor into your security and privacy? A couple truths about connected devices can help form the answer:

- The more devices you have, the more data you create, which companies can potentially collect, share, and sell.
- And the more devices you have, the more potential weak spots you have, which hackers can use to compromise the data and devices on your network.

These truths particularly apply to smart devices.

As more and more companies enter the smart device marketplace, we're seeing some build in better security measures than others. Similarly, we're seeing some roll out better privacy policies than others. So if you have smart devices from three, five, or even a dozen manufacturers in your home, you may be well protected in some places and left exposed in others.

With that, there's one more place you can protect yourself. At the checkout. Buying devices with strong security features and a clear privacy policy can help you bring only the best devices into your home. (You can check out our privacy policy for an example: https://www.mcafee.com/en-us/consumer-support/policy/legal.html.) For certain, security and privacy should factor in when you shop for smart devices, which we'll look at next.



Shopping for smart devices the smart way

Let's do some shopping for smart devices. But with a sharp eye for privacy and security.

We've already mentioned things like refrigerators, washers, and other appliances are transforming into connected devices. Many of these things have been subject to compliance standards for years now, long before they ever became "smart." That's particularly true for appliances and nearly anything you plug into a wall. They have regulations in place for safety, efficiency, and labeling that provides consumers with information about them. (In the case of the U.S., you can see several examples of mandatory regulations listed here.)

Federal Regulatory Authorities and Technical Regulations (Mandatory)

Several U.S. federal agencies are responsible for regulations pertaining to electrical and electronic products.

Agency	Scope
Consumer Product Safety Commission (CPSC)	Children's products, hazardous substances, labeling of hazardous products, consumer product safety
Customs and Border Protection (CBP)	Country of origin for most imported products
Department of Energy (DOE)	Energy efficiency
Environmental Protection Agency (EPA)	Toxic substances, Energy Star
Federal Communication Commission (FCC)	Radio frequency and digital devices
Food and Drug Administration (FDA)	Food contact substances, medical products and devices
Federal Trade Commission (FTC)	Labeling, EnergyGuide standards, environmental claims
Occupational Safety and Health Administration (OSHA)	Occupational safety, nationally recognized testing program

Source: U.S. Department of Commerce

However, similar standards for data and device security lag behind.

In effect, a smart washing machine must meet rigorous standards to ensure it's mechanically sound and won't start a fire in your home because such regulations are in place for appliances. Yet there's little in the way of regulations to ensure that it's sound from a cybersecurity standpoint.

Plenty of smart devices, yet few standards for smart device protection

That's not to say that there's no guidance in place. Over the years, you may have seen the UL logo stickered on the back or on the electrical cord of your appliances. This mark indicates that the appliance in question has met certain standards put forward by UL, a long-standing safety certification organization. UL has put together several services and tests designed to help manufacturers create smart devices that are safer and more secure,[7] however, participation is purely voluntary. Manufacturers are not required to follow them, unlike some of the compliance standards above.

This leaves consumers in a bit of a lurch. Let's say you walk into a big box store to shop for a smart refrigerator. You can compare a couple of them side by side and see that one is Energy Star compliant for energy efficiency and the other is not. That Energy Star standard, and the consumer-friendly labeling that comes with it, can help you make a purchasing decision. Meanwhile, you have no visibility into what cybersecurity measures are built into one fridge or the other—or what their data collection and privacy policies are. There's no standard. No label. No quick and easy way to evaluate the purchase based on security and privacy.

Why does that matter? Some recent research sheds a little light on what's at stake. Last year, researchers at the Florida Institute of Technology found that the companion apps for several big brand smart devices had security flaws.[8] Of the 20 apps associated with connected doorbells, locks, security systems, televisions, and cameras they studied, 16 had "critical cryptographic flaws" that could allow attackers to intercept and modify their traffic. This could lead to the theft of login credentials and spying, or it could lead to the compromise of the connected device itself. That's unsettling, given that we're talking about things like smart door locks here.

Yet the good news is that the researchers shared their findings with the companies, which then made security improvements before the research was published. (Another good reason to keep your devices updated!)

Granted, this is just one study that examined one set of connected smart devices, yet it underscores that long-held rule of cybersecurity: it's connected, it must be protected. Unfortunately, as mentioned earlier, some smart devices are manufactured with better protection than others—and better supported by teams who continually update them for security. Needless to say, hackers have taken note of smart devices that have poor security in place and will target them accordingly.[9]

Shopping smarter for smart devices

So where does this leave us as consumers? Right now, it appears we have a bit of homework to do when it comes to shopping for smart devices—a bit of research on our part. In the absence of consumer-friendly certifications and industry standards that can help guide our decision making, we must get smart on smart devices. That way, we can enjoy all the convenience while still looking after our privacy and security.

So, as you set out, here are a few things you can keep in mind:

1) Check out trusted reviews and resources

A positive or high customer rating for a smart device is a good place to start, yet purchasing a safer device takes more than that. Impartial third-party reviewers like Consumer Reports will offer thorough reviews of smart devices and their security, as part of a paid subscription.[10] Likewise, look for other resources that account for device and data security in their writeups, such as the "Privacy Not Included" website. Run by a nonprofit organization, it reviews a wealth of apps and smart devices based on the strength of their security and privacy measures.

2) Look up the manufacturer's track record

This also calls for a bit of research. Whether you're looking at a device made by a well-known company or one you haven't heard of before, you can find out if they've had any reported privacy or security issues in the past. And just because you may be looking at a brand name doesn't mean that you'll make yourself more private or secure by choosing them. Companies of all sizes and years of operation have encountered problems with their smart home devices. What you should look for, though, is how quickly the company addresses any issues and if they consistently have problems with them. Again, you can turn to third-party reviewers or reputable news sources for information that can help shape your decision.

3) Look into permissions

As we'll cover in the next section on smart speaker privacy, some smart devices will provide you with options around what data they collect and then what's done with it once it's collected. Hop online and see if you can download some instructions for manuals for the devices you're considering. They may provide an explanation of the settings and permissions that you can enable or disable.

4) Make sure it uses multi-factor authentication

Multi-factor authentication provides an additional layer of protection that makes it much more difficult for a hacker or bad actor to compromise your device even if they know your password and username. It's quite common nowadays, where an online account will ask you to use an email or smartphone as part of your logon process. Purchase devices that offer this as an option. It's a terrific line of defense.

5) Look for further privacy and security features

Some manufacturers are more security- and privacy-minded than others. Look for them. You may see a camera that has a physical shutter that caps the lens and blocks recording when it's not in use. You may also find doorbell cameras that store the video locally instead uploading it to the cloud where others can potentially access it or create transcripts of your voice interactions on the device. (Again, more on that in our next section on smart speakers.) Also look for manufacturers that call out their use of encryption, which can further protect your data in transit.

Smart speaker privacy

So is your smart speaker really listening in on your conversations?

That's the crux of a popular privacy topic. Namely, are we giving up some of our privacy in exchange for the convenience of a smart speaker that does our bidding with the sound of our voice? As you can imagine, the answer varies based on the manufacturer, what commands you're issuing, and what settings you have in play.

For starters, let's take a look at what's going on inside of your smart speaker, how it processes your requests, and what companies do with the recordings and transcripts of your voice.

So, are smart speakers listening in?

Yes. Each smart speaker has its own "wake word" that it listens for, like *Alexa*, *Siri*, or *Google*. When the device hears that wake word, or thinks it hears it, it begins recording and awaits your verbal commands. Unless you have the microphone or listening feature turned off, your device actively listens for that wake word all the time.

Here's where things get interesting, though. There's a difference between "listening" and "recording." The act of listening is passive. Your smart speaker is waiting to hear its name. That's it. Once it does hear its name, it begins recording for a few seconds to capture your command. From there, your spoken command may go the company's cloud for processing by way of an encrypted connection—or it may get processed locally on your device. This will vary depending on the device and the command you issued.

Broadly speaking, smart speakers may process some requests locally, while other requests require processing in their cloud. Local processing means that the request goes no further than your device. It gets handled right there.

In the cases where information does go to the cloud, processing entails a few things. First, it makes sure that the wake word was heard. If it's determined that the wake word was indeed spoken (or something close enough to it—more on that in a minute), the speaker follows through on the request or command. Depending on your settings, that activity may get stored in your account history, whether as a voice recording, transcript, or both. If the wake word was not detected, processing ends at that point.

Enter the issue of mistaken wake words. While language models and processing technologies used by smart speakers are constantly evolving, there are occasions where a smart speaker acts as if a wake word was heard when it simply wasn't said. Several studies on the topic have been published in recent years.[11] In the case of research from Northeastern University, it was found that dialogue from popular television shows could be interpreted as wake words that trigger recording. For example, their findings cite:

> *"We then looked at other shows with a similarly high dialogue density (such as Gilmore Girls and The Office) and found that they also have a high number of activations, which suggests that the number of activations is at least in part related to the density of dialogue. However, we have also noticed that if we consider just the amount of dialogue (in number of words), Narcos is the one that triggers the most activations, even if it has the lowest dialogue density."*

Of interest is not just the volume of dialogue, but the pronunciation of the dialogue:

> *"We investigated the actual dialogue that produced Narcos activations and we have seen that it was mostly Spanish dialogue and poorly pronounced English dialogue. This suggests that, in general, words that are not pronounced clearly may lead to more unwanted activations."*

Research such as this suggests that smart speakers at the time had room for improvement when it comes to properly detecting wake words, thus leading to parts of conversation being recorded without the owner intending it. If you own a smart speaker, you may have had issues like that from time to time yourself.

Is someone on the other end of my smart speaker listening to my recordings?

As mentioned above, the makers of smart speakers make constant improvements to their devices and services, which may include the review of commands from users to make sure they are interpreted correctly. There are typically two types of review—machine and human. As the names suggest, a machine review is a digital analysis and human reviews entail someone listening to and evaluating a recorded command or evaluating a transcript of a written command.

However, several manufacturers let you exercise some control over that. In fact, you'll find that they post a fair share of information about their collection and review processes, along with your choices for opting in or out as you wish:

- Apple doesn't retain audio of your requests unless you opt in to help improve Siri. If you've opted in, Apple explains that process here. For more information about their overall privacy measures, visit Apple's page here.
- Amazon also explains how it uses such information and likewise how you can opt out. You can learn more about their overall privacy measures for Alexa here.
- Google states that it does not retain your audio recordings by default—and you can browse or delete your Google Assistant history here.

Setting up your smart speaker for better privacy

The quickest way to ensure a more private experience with your smart speaker is to disable listening. This keeps it from passively waiting to hear its wake word, effectively making your smart speaker unresponsive to voice commands until you enable them again. This approach works well if you decide there are certain stretches of the day where your smart speaker doesn't need to be on call.

Yet let's face it, the whole idea of a smart speaker is to have it on and ready to take your requests. For those stretches where you leave it on, there's another step you can take to shore up your privacy.

In addition to making sure you're opted out of the review process mentioned above, you can also delete your recordings associated with your voice commands.

- For Google Assistant users, Google provides the following article.
- Siri users can follow these instructions to delete their recordings.
- You can manage your Alexa recordings with these instructions as well.

Managing your voice history like this gives you yet one more way you can take control of your privacy. In many ways, it's like deleting your search history from your browser.

With privacy becoming an increasingly hot topic (rightfully so!), companies have been taking steps to make the process of managing yours easier and a more prevalent part of their digital experience. As you can see, there are several ways you can take charge of how your smart speaker uses, and doesn't use, your voice.

Given that companies like Amazon, Apple, and Google now dedicate portions of their websites to privacy, pay them a visit when you have questions or simply want to lock down your privacy. Their tutorials will guide the way and provide you with a look at the latest controls you can put in place.

Looking forward to your connected home

Smart homes show plenty of promise, laden with comforts and conveniences, while also making for time-savings and energy-savings too.

Yet outfitting your home with smart devices calls for consideration and care, given the security and privacy involved. Some manufacturers put plenty of effort into creating devices that are more secure, such as by using encryption to transmit data, regularly sending out updates for the devices, or simply designing them in ways that make them more private and secure from the start. Others, not so much.

Similarly, different manufacturers have different privacy policies and thus use people's data in different ways, which puts consumers like us in a position to understand the terms, conditions, and implications of each one. Yet with data privacy being such a hot topic for consumers, the industry, and regulators already, it remains to be seen what consumer-friendly standards are set for data collection in the years to come—both in and out of the smart home.

However, these issues shouldn't bar you from exploring smart devices for your home. With a broad understanding of how smart devices work, plus a sound understanding of how to protect them and how to shop for the safest and most private ones available, you can enjoy the benefits of a smart home today.

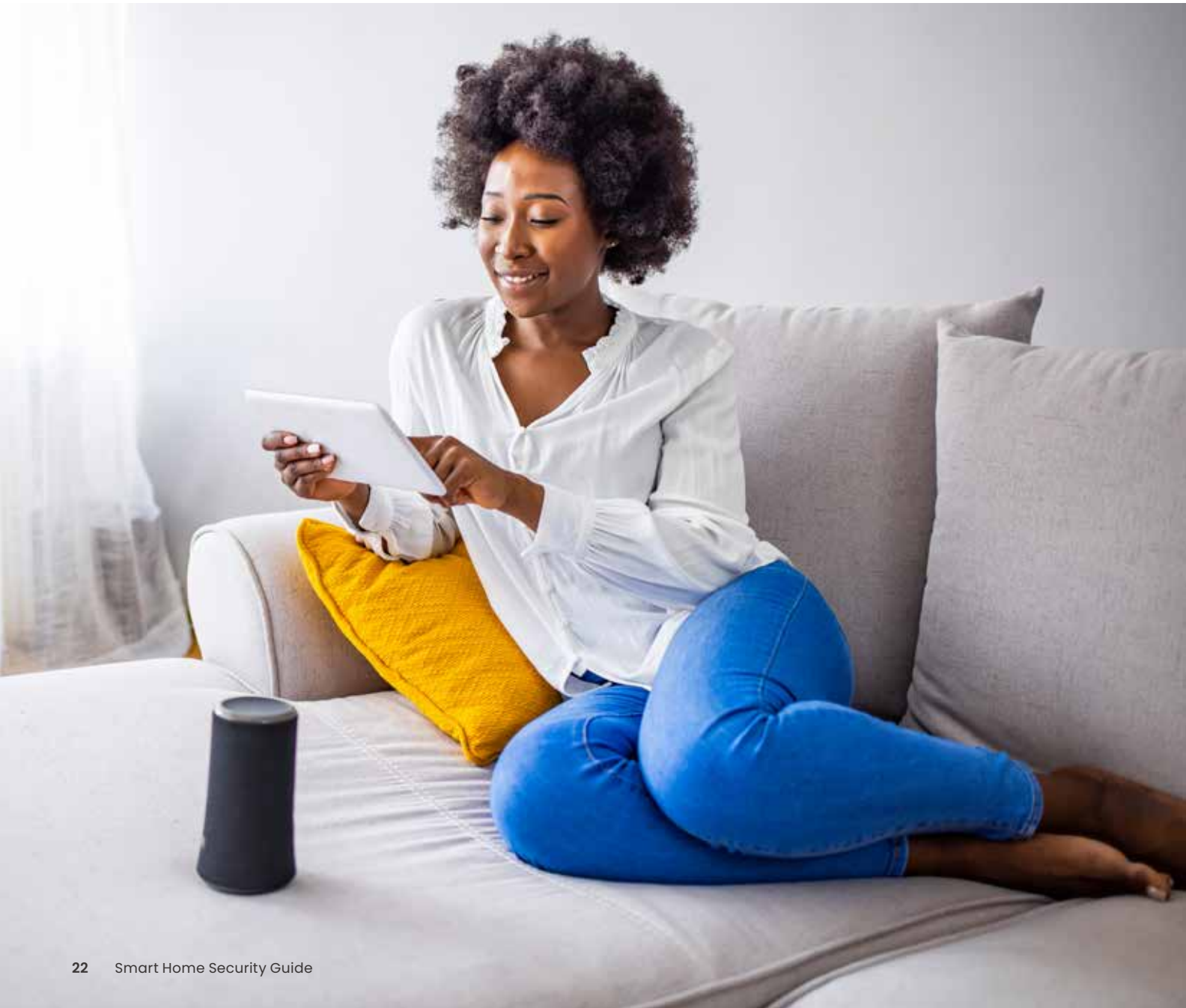
We hope that the insights and advice you've picked up here will help you build out your smart home for comfort and convenience—and for privacy and security too.

For more about staying safe and getting the most out of life online, our blog offers you and your family a terrific resource across a wide range of topics from online banking, gaming, and shopping to tough yet important topics like cyberbullying and which apps are safe for kids.

Our aim is to help you think about what's best for your family and the steps you can take to see it through so that you can make everyone's time online safer and more enjoyable.

Visit us any time!

https://www.mcafee.com/blogs



About McAfee

McAfee is a worldwide leader in online protection. We're focused on protecting people, not devices. Our solutions adapt to our customers' needs and empower them to confidently experience life online through integrated, easy-to-use solutions.

www.mcafee.com

For more information about online protection, visit us at mcafee.com/blogs

1 https://www.statista.com/outlook/dmo/smart-home/united-states
2 https://www.npr.org/sections/thetwo-way/2018/06/05/617196788/s-c-mom-says-baby-monitor-was-hacked-experts-say-many-devices-are-vulnerable
3 https://csa-iot.org/all-solutions/matter/
4 https://zigbeealliance.org/wp-content/uploads/2021/11/Matter-Security-Privacy_one-pager.pdf
5 https://moniotrlab.ccis.neu.edu/wp-content/uploads/2019/09/ren-imc19.pdf
6 https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/five-common-privacy-problems-in-an-era-of-smart-devices
7 https://www.ul.com/services/internet-things-iot-testing-services
8 https://news.fit.edu/academics-research/apps-for-popular-smart-home-devices-contain-security-flaws-new-research-finds/
9 https://news.fit.edu/academics-research/apps-for-popular-smart-home-devices-contain-security-flaws-new-research-finds/
10 https://www.consumerreports.org/smart-home/best-smart-home-devices-of-the-year-a5691424633/
11 https://moniotrlab.ccis.neu.edu/smart-speakers-study-pets20/

McAfee™

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com

gd-smart-home-security_1222 DECEMBER 2022