

TAKE CONTROL OF

HOME SECURITY CAMERAS

by GLENN FLEISHMAN

Take Control of Home Security Cameras (1.4)

Glenn Fleishman

Copyright © 2023, Glenn Fleishman. All rights reserved.

ISBN for EPUB and Mobi version: 978-1-7780439-6-3

Table of Contents

Read Me First

- Updates and More
- What's New in Version 1.4
- What Was New in Version 1.3

Introduction

Home Security Cameras Quick Start

Which Camera to Buy

Why Do You Want a Camera?

- Screen Approved Visitors and Workers
- Ding, Dong! Who's There?
- Deter and Report Crime

Rough Out Your Layout

Choose Where Video Lives

- Where a Camera Stores Your Video
- How To Retrieve Video
- Pick Your Storage Method

Consider Physical Parameters

- Pick a Brand Name?
- Choose a Network Connection
- Mull Mounts and Pick Power
- How Cameras Capture a Scene
- Pick Camera-Based Features
- Consider Extras Beyond Video

Be Alert!

- Configure Triggers
- Actions Respond to Triggers
- Receive Alerts

Secure Your System

- You Face Real Risk
- Set Up an Account or Device Password
- Secure Hardware and Data
- Share Access

Protect Privacy

- Keep Your Cameras and Video Private
- Respect Other People’s Privacy
- Are You Part of the Surveillance State?

Use Smart Home Ecosystems for Control

- What Kind of Systems Exist
- Look at Major Ecosystems

About This Book

- Ebook Extras
- About the Author
- About the Publisher

Copyright and Fine Print

Read Me First

Welcome to *Take Control of Home Security Cameras*, version 1.4, published in January 2023 by alt concepts. This book was written by Glenn Fleishman and edited by Joe Kissell.

Learn everything you need to know about home security cameras to plan, purchase, and install the best system for your needs for live access, security monitoring, alerts, privacy concerns, and affordability.

If you want to share this ebook with a friend, we ask that you do so as you would with a physical book: "lend" it for a quick look, but ask your friend to buy a copy for careful reading or reference. Discounted classroom and user group copies are available.

Copyright © 2023, Glenn Fleishman. All rights reserved.

Updates and More

You can access extras related to this ebook on the web (use the link in Ebook Extras, near the end; it's available only to purchasers). On the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy any subsequent edition at a discount.
- Access the book in both PDF and EPUB formats. (Learn about reading on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.

If you bought this ebook from the Take Control website, it has been added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually; see Ebook Extras.

What's New in Version 1.4

This update includes timely revisions to reflect current product lines and price changes, among other changes. More specifically:

- **Eufy gone:** I removed Anker's Eufy line of cameras from recommendations and discussion. A researcher discovered multiple significant security flaws, the company delayed and obfuscated its response, and even the fixes and answers are incomplete as of January 2023.

- **Logitech line-up changed:** Logitech has discontinued all but its Circle View models, which work only with Apple HomeKit Secure Video. I've updated the book to reflect that.

- **Constant model changes:** Because of the constant churn of camera models, prices, features, and availability, our rundown about models by company becomes obsolete within days or weeks of publication. As a result, I've removed the section that included a detailed rundown. It's better I refer you to manufacturers' sites and specific models that we ensure remain available through book updates.

What Was New in Version 1.3

This version incorporated the latest feature changes to home security cameras and software. Other changes included:

- **Doorbell cameras:** The section on doorbell cameras, Ding, Dong! Who's There?, was revised and expanded. I also added a sidebar that gets into the electrical issues of using analog doorbell wiring for a doorbell camera in Doorbell Cameras May Require or Allow Special Wiring.

- **Apple HomeKit Secure Video and iCloud+**: Apple changed the name of its paid tiers of storage. The free 5 GB tier is still iCloud, but the 50 GB, 200 GB, and 2 TB tiers ($0.99, $2.99, and $9.99 per month) are all called iCloud+. All three tiers now include support for HomeKit Secure Video. See Use HomeKit to Store Video and Trigger Alerts. Changes were made throughout as well.

- **Use an Apple TV:** I added a short section explaining how to use an Apple TV with tvOS 13 or later to view video from HomeKit-connected cameras. See View Video with an Apple TV.

- **Google name changes:** Google Home now refers only to the app Google offers to control their hardware; previously, Google also released smart speakers as Google Home devices, but now uses Nest for their branding. See Google Assistant, Nest, and Home.

- **Expanded encryption in transit:** I expanded the section about how data and video used by cameras is encrypted in transit to better explain the layers of options available. See Encrypt Data in Transit.

Introduction

A camera or camera system can allow you to let someone into your home when you're not there, note when packages land on your porch, check in with your child or children when you have a nanny or babysitter watching them (or uncover unauthorized parties when they're older), avoid personal contact during epidemics or other personal health events, or check in on a rental property.

And you can, of course, provide details to an insurance company when theft or accidental damage occurs, or call the police or hand over video if a burglar or other criminal is caught in the act. Sometimes the mere presence of cameras deters people from breaking in.

In this book, I'll help you figure out what your intent is for installing video monitoring, determine what it might cost in outright expense and ongoing fees, and plan a deployment. The end of the book features several chapters each devoted to a specific company's line (or sometimes, multiple lines) of products that are designed to work either solo or together.

> **Note:** Throughout this book I refer to *cameras* in the plural. Some people start with one camera and may choose to add subsequent ones; from what we can tell with the sale of bundles and systems, two or more appears quite common.

But I'll also help bring up the ethical and political challenges for each of the scenarios I suggested. Whom do you tell about having camera pointing outwards from your house or inside it (or a rental property)? What access do you offer police routinely or when crimes are believed to have occurred?

Technology is always a two-edged sword, and I hope to help you wield it safely and to your advantage.

Home Security Cameras Quick Start

This book helps you determine what kind of camera or system you need, narrow down which to purchase, and keep yourself and those around you secure and private.

Figure out the system that's right for you:

- Consider your intent in getting a camera system in the first place; see Why Do You Want a Camera?
- Draw a map of your home and where you want to cameras to be placed and what they view; see Rough Out Your Layout.
- Decide how you want to interact with live and recorded video (and audio) from your cameras; see Choose Where Video Lives.
- Learn about camera features, like resolution and angle of view; see Consider Physical Parameters.
- Consider how cameras fit into a smart home ecosystem; see Use Smart Home Ecosystems for Control.

Think about privacy, security, and surveillance:

- Uncover the implications of where your video is stored, locally or remotely; see Where a Camera Stores Your Video.
- Who should have access to your camera and stored video? See Keep Your Cameras and Video Private.
- Avoid peeping on other people; see Respect Other People's Privacy.
- Consider how law enforcement might use video you record; see Are You Part of the Surveillance State?
- Pick good passwords and lock down access; see Secure Your System.

Tweak your systems to meet your needs:

- Determine the alerts you want to receive and control how they're delivered; see Be Alert!

- Let others share access to your cameras; see Share Access.

Which Camera to Buy

For readers who want a tl;dr on best options, here are my top recommendations in three categories:

- **Highest-quality single camera with user-controlled encrypted cloud storage (Apple ecosystem only):** The Logitech Circle View ($159.99) is a good camera with up to 180° field of view that works only with Apple's HomeKit Secure Video. Apple's system provides top-notch end-to-end encryption (E2EE) that prevents anyone but you from decrypting your stored video clips or viewing the live stream. Even Apple can't. An iCloud+ subscription of $2.99 or more per month is required, but video storage isn't counted against iCloud+ storage limits. Apple keeps 10 days of clips for you. Apple devices are required for configuration, notifications, and viewing video. See Use HomeKit to Store Video and Trigger Alerts.

- **Best overall line-up for user-controlled encrypted cloud storage (cloud, Amazon Ring system):** Several of Amazon's Ring cameras now offer end-to-end encryption, which works with any combination of iPhone, iPad, or Android phone or tablet. While some cavil at Amazon's past practices, E2EE prevents the company from viewing or accidentally exposing your video. Supported cameras run the gamut, and Amazon offers two tiers of enhanced service, both of which are reasonably priced. Amazon lists supported models.

- **Cheapest camera and cloud plan (all platforms):** Wyze offers a couple of camera models that cost below $40 and are paired with a free storage plan with 14 days of clip storage. The plan can upgraded to unlimited for just $1.99 per camera per month or a more heavily discounted $15 per camera per year. It can also record video to an inserted microSD card.

Why Do You Want a Camera?

It sometimes feels like we live in a surveillance state already. Why add yourself into that mix? Reasons abound for wanting to purchase one or more home security cameras to monitor the environment around our home, a cabin or vacation house, or a home or other place we may rent or make available to others.

Let's look into the two main categories. They're not exclusive! You may have stuff snatched from your porch and want to try to put a stop to it *and* enjoy capturing video of hummingbirds paused on a feeder outside your back deck.

Screen Approved Visitors and Workers

While the field emphasizes security and I put it in the title of the book, personally controlled cameras on one's property can offer many more purposes than deterring or recording burglaries (see Deter and Report Crime, later in this chapter).

This includes a lot of distinct activities, all of which have privacy, security, health, and safety considerations:

- Know when packages are delivered to retrieve them or ask a neighbor to, in an area with a lot of porch-prowling package purloiners.
- Allow a remote face check to allow a contractor or other tradesperson into your house—or even someone delivering a package. You may have given or left them a key or have a smart lock you can use to let them in.

> **Tip:** Some camera systems automatically recognize when a package appears and remains within view and notify you.

- For personal safety, where you live alone and would prefer not opening your door to anyone, would like to come home without worrying is someone is near your home, and want greater awareness of who is around your house even while there is no current crime involved.
- Confirm a child has left the house or arrived home. Smartphones help with this, too, but not all children own one (shocking, I know).

- Monitor a baby or infant in their room.
- Monitor or communicate with a babysitter or nanny.
- Capturing footage of birds and larger wildlife in your area. This may be for appreciation—you can find hummingbird cams all over—or out of concern. In some areas, homeowners have to monitor for animals they view as pests—munchers of vegetables or potential spreaders of disease—like bunnies, deer, rodents, and other small animals. You might also need to be aware of or beware predators like coyotes, wolves, mountain lions, cougars—oh my!
- Capture people letting their dogs poop on your lawn and not picking it up. Seriously, I imagine that's a top ten, if not top five purpose.

Warning! Privacy considerations abound—and criminal and civil liability issues—when you record people you have invited into your house. Read up on privacy issues of recording other people in and around your home in Respect Other People's Privacy.

There's no single camera model that's perfect for all these purposes. But there are four general considerations that overlap, and you may want to fulfill one or more of these:

- **Need to greet someone at the door without being there or opening it:** To this end, you almost always want a doorbell cam with a button someone can press. The camera may be paired with facial recognition, which can even be used to unlock the door for known parties if also paired with a smart lock. But it's always set to activate an alert on your smartphone or another device, allows two-way audio communication, and is optimized (often with a fish-eye lens) to show the entire area around the door. Long-term storage of video is rarely an issue.
- **Need to monitor what's happening inside your house:** Aspects of this kind of monitoring can be creepy; others times, it's necessary or appropriate oversight. If you have employees (like a nanny) or contractors in your house routinely, you may want a camera both to tune in live or to review video if something goes wrong when it's not criminally wrong. The presence of a camera might deter improper actions, too. A huge array of indoor models meet this need.

  On the storage front, you may want to record continuously and retain that for a period of time, which limits camera choices. Motion-triggered clips may be less useful because of the constant movement in some spaces.

Two Non-Creepy Monitoring Examples

A sub-contractor hired by your contractor swings a hammer poorly, knocks a hole in the wall, and then hides it. You later discover the hole, and can show your general contractor who was at fault. Second, a child knocks over a lamp. You ask the babysitter about it, and they disclaim knowing how it happened. The video confirms it's your kid's fault—not the sitter's!

- **Need to monitor goings on in front of your house:** For contractor work, the coming and going of people to a porch, and even checking up on kids playing in the front lawn, you want either an outdoor battery-powered camera—possibly with a solar panel to avoid having to recharge the battery—mounted in a position that is hard to get at; or, an indoor camera mounted directly onto a window. Motion-triggered short video clips are typically the most useful approach, and all camera systems support them.

- **Need to communicate with people inside your house:** Most indoor cameras include two-way audio, like an intercom. Check specs on cameras to make sure the feature is present, and read reviews for how well it works. This is often a feature reviewers call out. This sort of communication rarely needs to be stored.

Ding, Dong! Who's There?

A doorbell camera can be a great technological aid to let you screen visitors without going to the door or having to open it when it's someone you don't know. You can see them, talk to them, and hear them. If you pair the doorbell camera with a smart door lock, you can even let people in remotely.

Tip: This was great during the early phases of the pandemic, when many people avoided all direct contact with people outside their households, but it is also generally useful.

One of the easiest paths is to replace an existing wired, analog doorbell with a model that can use its electrical wiring. This avoids recharging a battery and the limitations of battery-powered cameras. To install, you might need an electrician if you're not comfortable with turning off a circuit breaker and doing some rewiring, too.

Tip: If you don't have old-style wiring, you can purchase an electrical adapter, but this probably isn't the right option for you. Pick a battery-powered model instead.

Here are the best options in two scenarios for replacing an existing powered doorbell:

- **Store video end-to-end encrypted in the cloud; Apple ecosystem:** The Logitech Circle View Doorbell ($199.99, chime sold separately) relies on Apple's iCloud+ paid subscription service for end-to-end encrypted HomeKit Secure Video storage only you can access. You must have an iPhone, iPad, or Mac plus a HomeKit hub (iPad, HomePod, or

Apple TV). You can buy Logitech's chime kit, wire it into an existing chime, or receive notifications just on your devices. iCloud+ includes unlimited clips that don't count against your storage limits for each tier. The $0.99 per month (50 GB) tier allows 1 camera; $2.99 per month (200 GB) supports up to 5; and the $9.99 per month (2 TB) pays for unlimited cameras. See Use HomeKit to Store Video and Trigger Alerts for the full set of requirements.

- **Add an externally mounted doorbell camera:** You have many choices, but Amazon's Ring brand has the most options. Consider the simplest model that can tie into existing doorbell wiring, the Ring Video Doorbell Wired ($59.99; bundled with chime, $79.99), and which offers end-to-end video encryption as an option. Ring cameras can also work without a subscription for live interactions and alerts. Monthly storage subscriptions start at $3.99 per month (one camera) or $10 per month (unlimited cameras) for cloud-based clip storage and other features.

Ring and a handful of others offer battery-powered versions of doorbell cameras, too. However, depending on the model, the camera might store shorter clips or lack options that a continuously powered model can provide.

Peephole without a Doorbell

If you have an existing security peephole, you may be able to replace it with a Ring Peephole Camera ($129.99), which is compatible with many styles of optical peepholes. If you're a renter, your landlord might allow you to install it, too, as it doesn't add holes or require modifications to the door. It's also the most appropriate option for most people in live in a building of apartments, condos, or co-ops. See above for storage options.

Deter and Report Crime

Property crime has plummeted in most of the developed world in the last decade. In many countries, fewer than half as many break-ins with the intent to steal occurred per 100,000 residents in 2016—the most current year for statistics—as in 2005. That includes the United States, whose rate dropped nearly in half even with population growth of 11%; and places like the Netherlands, with 75% fewer burglaries alongside a stable population.

Of course, it's certainly not down to zero. And you may live—as I do—in a pocket in a city that for whatever geographic, socioeconomic, or topographical reasons has a measurably higher property crime rate than the rest of your area.

That can be because your house or street is tucked out of the way or views are obscured by hills or valleys—or your area is perceived as or actually is more conspicuously wealthy than regions around you, even if you're not a participant in displays of or possession of affluence!

Whatever the reason, if your primary or one of your reasons for installing a camera is to capture video (and audio), there are five components to consider:

- **Deterrent:** The presence of a camera may scare off potential thieves or miscreants from engaging in crime in the first place.
- **Alerts and alarms:** If someone appears outside or inside your home, you want to be alerted to it and be able to see what's going on so you can take action, like calling the police, or have an automatic action occur, like flood lights turn on and a siren go off.
- **Video for criminal charges:** If a crime is committed in or near your home, your cameras may have captured it. (See Is Video Admissible in Criminal Cases? below.) You may have varying feelings about that, so also read Are You Part of the Surveillance State?
- **Video for civil lawsuits:** If someone engages in vandalism, steals from you, or otherwise causes damages, video can be an effective tool in a lawsuit in which you are suing to recover money or obtain other relief.
- **Monitoring crime in the area:** You may be an area with enough general lawlessness that you use a camera to help as part of neighborhood efforts, such as monitoring for car thefts or break-ins at other houses. You might also want to make this readily available to other neighbors and the police; see Are You Part of the Surveillance State? for more on this, too.

For each of these prospects, the kinds of camera specs you need are fairly straightforward:

- **1080p, 2K, or 4K recording:** Modern cameras start at 1080p, while higher-end cameras record in 2K or even 4K. The more detail you want, especially of people's faces and of things farther away, the higher the resolution you want. See Resolution and Quality.

> **2K or not 2K? Let's Resolve It**
>
> When you compare resolution, 1080p and 4K are clearly different: 1,920 by 1080 pixels versus typically 3,840 by 2,160—though sometimes 4,096 by a proportional amount. Not so for 2K, which varies among makers from rounding up 1,920 pixels to 2,000, or might be a true 2,048 by roughly 1,152.
>
> Even if it's "true" 2K, multiplication and division reveal that's only a 13% greater number of pixels than 1080p, and typically not worth a large price jump above 1080p cameras unless other, more important features are included.

- **Night vision:** Most camera models feature infrared LEDs to illuminate indoor and outdoor scenes. However, because crimes often occur with low or no lighting, you might opt for a camera that requires a power source instead of a battery to allow for higher-intensity infrared LEDs and a more sensitive image capture sensor. Some newer cameras use better

image sensors, brighter LEDs, and image processing to upgrade the normal grayscale night vision to full color, too. See Night Mode and read the specs on cameras.

- **Wide aperture:** A more recent trend has seen camera makers advertise cameras with big apertures, the openings that pass light through to expose onto a sensor. With well-designed optics, the bigger the aperture, the less light required to capture clear images and video. When paired with newer, higher-quality sensors that are better at reducing noise in low-light conditions, you may not need lighting or night vision at all if there's enough ambient light.

- **System integration:** Most cameras offer smartphone or other alerts when certain triggers set off recording, such as motion or a camera being unplugged. If you're concerned about a break-in or other actions, you likely want a camera tied into an alarm system that may trigger a siren, call a monitoring company, and even turn on flood lights. Depending on the camera, you might be able to get an all-in-one service plan that includes cloud storage, full-time monitoring, and alarm-style features, as with Amazon's Ring series. See Use Smart Home Ecosystems for Control.

- **Full capture:** It's a more niche need, but if you have constant problems with crime, you may want to retain a continuous video feed and for a long period of time. It used to be that you had to turn to an integrated multi-camera system that includes or supports a network video recorder (NVR). However, newer service plans from several companies let you stream continuously to cloud storage, sometimes as part of the basic price of the service and sometimes through an add-on option.

- **Storage:** Because you may not discover a crime has occurred until later, you likely want longer-term storage of continuous video or trigger-based clips than a day—sometimes 24 hours' storage of clips is included free with a camera's purchase. Instead, look for cameras that offer 7-day to 30-day storage plans or cameras that you can configure with your own storage. See Choose Where Video Lives.

- **Third-party access:** Some systems let you share video directly with law-enforcement officers or provide it to neighbors who can then choose what to do with it. If this is an ongoing concern, consider that factor in which camera you purchase. Ring offers these features, but they're controversial. See Are You Part of the Surveillance State? for more on that.

Is Video Admissible in Criminal Cases?

You might be recording video to use as evidence of a crime. But can that video be used to charge someone or be introduced in a trial? (Let me preface this, as I will repeat a few times in the book, by noting I am not a lawyer and this does not constitute legal advice.)

For people without permission to be on your property or inside your home, the answer generally appears to be yes. However, police have to follow an investigative process in obtaining the video from you, document a camera's position, and make sure they can prove the date and time and location of the recording.

Simply emailing a video won't work as evidence in court! In fact, police relying on video without following the rules could lead to any other evidence they collect on the basis of that video being thrown out—the so-called fruit of the poisoned tree.

Defense attorneys may be able to block a video on many grounds or destroy its credibility if all the niceties aren't followed—if a camera's clock is set incorrectly and the timestamp on the video is inaccurate.

However, an increasing number of cases rely on video recorded by someone of a crime against them or their property, or by video given by neighbors or nearby businesses or subpoenaed by police.

If you have video evidence of someone you invited into your home or whom you hire to be there, like a babysitter or plumber, and your cameras are hidden, not every judge or state will admit the evidence.

Audio is covered by different rules; see Is It Legal To Record Audio?.

Defendants, by the way, are often allowed more leeway to introduce into evidence video that might exonerate them, as the balance of power in a criminal proceeding favors defendants providing evidence that casts doubt.

Rough Out Your Layout

This book offers criteria for the kinds of things you want in cameras or an integrated system. But before we dig into the particulars, you should make a rough diagram of your house, condo, apartment, or other setting to figure out exactly what you want to see and hear.

Draw a map by hand or in simple-to-use software—you can use the drawing tools in Word or Pages. It doesn't have to be to scale at all (**Figure 1**). The idea is to get you thinking about spaces, directions, and coverage. If you have multiple floors, draw a layout for each one.

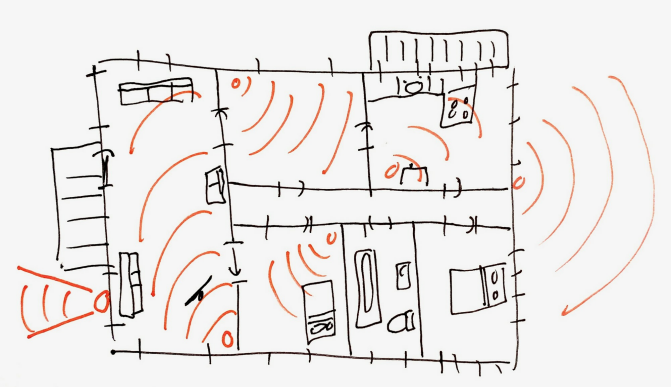


Figure 1: A rough drawing of a house floor plan with desired cameras and directions sketched in.

If you doubt your basic drawing abilities or want more precision, you can use inexpensive smartphone software that lets you walk around your house and tap on walls to build an amazingly accurate house layout. As one suggestion, RoomScan Pro comes in a trial version you can test and then unlock for $8.49 a year (**Figure 2**).

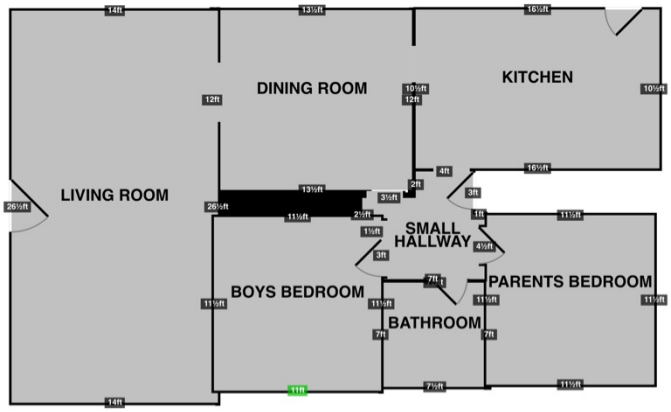


Figure 2: A precise set of measurements offers more detail than you need, but it's simple to generate, too. (Generated in RoomScan Pro)

Now mark up potential locations and directions for cameras, as I did in **Figure 1**. Don't limit yourself initially: mark every spot in and around your home you want to capture video (or audio) from.

For a camera capturing views outside, consider whether you'd locate it attached to a window pane or pointed from a location inside that encompasses a window, or mounted somewhere outside (see Indoors and Outdoors). An outside-pointing camera that's located inside can't use infrared for night vision of outdoor scenes due to reflection (see Night Mode). Plot out whether you have an outdoor power outlet located nearby, or whether you need to use a battery-powered unit (see Pick a Power Source).

In addition to maps for outdoor cameras, consider taking still photos from potential locations. Then print them out to consider the portion of the view you want to capture and how it will be framed (see A Lens Sets the View).

For indoor cameras, think about the best placement to capture the largest expanse, so you can use the fewest cameras. In some locations, a fixed camera with a broad field of view is best; in others, you might want a camera that captures less of a scene, but which can move around and zoom (see Fix a Lens or Move It Around.)

While surveying your need for indoor cameras, think about spaces you don't want to record and whether cameras have options to disable themselves while you or other family members or guests are present. Also mark where power outlets are relative to where you want to place a camera, and whether you have existing Ethernet wiring drops if you want to go the wired-network route (see Ethernet Connection).

Now make a list of cameras you think you want to get a full count and to enumerate characteristics. For instance, in this example spreadsheet, I named each location, noted if it were indoors or outdoors, whether it had power or Ethernet, and whether it needed to be mounted (**Figure 3**).

Camera	Location	AC outlet?	Ethernet?	Mount to wall/ etc?
Front porch	Outdoors	Yes	No	Yes
Living room	Indoors	Yes	Yes	No
Kitchen facing back door	Indoors	No	No	Yes
Back driveway	Outdoors	No	No	Yes

Figure 3: Enumerate your camera needs.

This sketch of needs will come in handy as you proceed through the chapters ahead. I suggest making notes in the spreadsheet or on a piece of paper about particular features you might want on individual cameras or on every camera, as well as noting models I mention as examples that meet your needs.

In the last chapter in the book, I dig into camera systems one at a time, and with this information in hand, you should be able to home in on the right model or models for your needs.

Choose Where Video Lives

It might seem odd to start the book by considering where you want to store video recorded by the cameras you install. And yet, it's a critical choice compared to all others, because different manufacturers and models offer widely varying sets of choices.

In this chapter, I lay out the options for storage and the tradeoffs for each from storage, cost, and accessibility viewpoints, including live streaming.

> **Note:** Privacy is a paramount consideration for many people. I have an entire chapter devoted to this: see Protect Privacy.

Where a Camera Stores Your Video

The currency of home security cameras is capturing video—either continuously or for short periods in response to triggers—that may be either available for view via live streaming or stored for later retrieval, and often both. This would seem to be such a trivial thing, but it's the pivot point around which all other decisions are made, and which affects your privacy and the privacy of others.

Let's look through all the alternatives and how they stand out in several regards:

- **Capacity:** How much video can you store before the chosen method fills up or starts deleting older video; or what is the duration of video (in hours, events, or days) it can store?
- **Capture kind:** Some cameras can be set to record continuously. Many have only an option to store clips, triggered by detected movement in a camera or certain other specific events.
- **Cost:** Is there an initial one-time cost, a setup charge, a lifetime fee, monthly or year subscription fees, or storage and access fees?
- **Bandwidth requirements:** What kind of internet connection is needed? (Also see the sidebar below.)
- **Protection:** Can the storage be stolen or destroyed?
- **Privacy:** Who has access? Who could gain access?
- **Quality:** Does the medium of storage limit video quality captured?

- **Access:** Are your options for remote access or later retrieval constrained by the storage method?

Proprietary Cloud

The most popular option among the most popular and well-known camera systems is what I call the "proprietary cloud." In this scenario, your cameras stream video in real time to internet-hosted storage entirely under the control of the camera maker.

> **What's the Cloud, Anyway?**
>
> The term "cloud" is rarely defined precisely. I like to think of the cloud as any online storage or system in which I don't have to manage physical hardware or connect to a specific server.
>
> For cloud storage, that means a pool of internet-reachable data that you have no idea where in the world it is or how it's configured. With camera-based proprietary clouds, it's just an amorphous blob of data storage that your cameras talk to and you can access via apps.

Here are the characteristics of proprietary cloud storage for cameras:

- **Capacity:** It's a big range, from 24 hours of free storage of motion-triggered clips up to weeks or months of continuous storage.
- **Capture kind:** Cameras typically only offer a particular type of storage with manufacturer-owned clouds, rather than the option to select between motion-based events and continuous video. You may decide between competing systems based on whether you need full video recordings or can rely on clips. Some systems offer a choice between the two types, too.
- **Cost:** These vary enormously. Some makers offer free 24-hour storage of motion-triggered clips. Others charge a flat rate per camera or set of cameras for full video storage for a set period of time. This can vary hugely. Here are a few example of the range:
    - **Motion-captured clips:** Wyze Cam Plus charges as little as $1.99 a month or $20.04 a year per camera for unlimited clip storage, and Arlo Secure will set you back $12.99 a month for unlimited cameras for a rolling history of 30 days of motion-triggered recordings.
    - **Continuously recorded video:** Google offers a rolling 10 days of 24/7 recording and 60 days of clips for an unlimited number of cameras for $12 per month or $120 year with Nest Aware (**Figure 4**). NETGEAR has a special continuous video recording plan for some Arlo models that's $9.99 a month for the first camera and $4.99 for each additional camera to capture 14 days per camera.



Figure 4: Google offers a plan for Nest cameras that includes a massive amount of stored video (Source: Google)

- **Bandwidth requirements:** All video is streamed, so you need as much bandwidth as is required to operate all cameras at your chosen resolution and quality simultaneously, in addition to any other network use (see Cameras Consume Bandwidth for Internet Uploads, below).

- **Protection:** Remote storage means video is secured as soon as it traverses the internet, even if a camera is stolen or is damaged in a fire or natural disaster. A criminal could sever an internet connection to block video capture, including from cameras they haven't spotted. That's why some cameras include memory cards to capture video offline—if they're not stolen or smashed.

- **Privacy:** While companies secure your video and protect your account, in almost all cases the keys to the castle are on their servers and in their control. Legitimate and illegitimate requests from governments, misuse by employees at firms with poor access control and monitoring, and hacking all remain problems.

Some Cameras Give You the Keys to Privacy

So far, there are two exceptions to the privacy issue for proprietary clouds: Apple's HomeKit Secure Video and some of Amazon's Ring cameras. In both cases, video is stored with end-to-end encryption (E2EE), meaning that it's always encrypted before transmission using keys stored in devices under your control.

Apple's HomeKit Secure Video requires a compatible camera from a handful of companies that include Logitech. You can mix and match cameras from different manufacturers on the same local network. Only people who gain access and can unlock a device you own or that you've invited to a Home group can access stored video or a live feed. Read Apple HomeKit for more details.

Amazon has enabled support for E2EE on several models of its cameras, mostly doorbell models. You just have to follow their steps to turn it on.

- **Quality:** It's entirely dependent on bandwidth. Most cameras you should consider let you choose 1080p through 4K resolution, and the number of frames per second or level of compression coupled with resolution determines bandwidth consumed. You can often compromise by using motion-triggered storage, which stores less overall video. Some cameras can send a higher-quality video clip that way because they can spool it out by not uploading in real time.

- **Access:** Cloud-based storage means it's easy to access video from anywhere. You're may even be using the cloud when you stream video from the camera live while you're on the same network, depending on the hardware.

Pick proprietary cloud storage if you have fairly substantial upstream bandwidth, especially for multiple cameras; want your storage primarily offsite or as an offsite backup; and aren't concerned about the risk of unauthorized access to your stored video.

If you never want anyone beside yourself or your family to have the slightest potential access to video, focus on the next option.

Cameras Consume Bandwidth for Internet Uploads

A camera might offer neither, either, or both of the first two upload options; all seem to offer the third:

- Continuous capture, 24 hours a day
- Event-based capture of clips
- Remote live, or streaming, access

It each case, the camera imposes the same upstream bandwidth requirement whenever it's streaming video: continuously or intermittently. In my research, I found no consumer-oriented cameras that cached clips and could spool them on lower-bandwidth networks.

Most resolutions require roughly the same amount of bandwidth among different camera makers. Google Nest cameras can use as little as 150 Kbps for 360p resolution on its Nest Cam Indoor, Nest Cam Outdoor, and Dropcam models, and up to 4 Mbps for Nest Cam IQ Indoor and Outdoor models for its higher-quality 1080p mode. For a 4K camera, higher-quality hardware compression may keep band-with requirements from bloating.

Each camera that offers internet-uploadable data or live streams requires its own share of bandwidth, so you need to add up the requirements for each camera you add to a system.

Memory Card

While it may seem old hat, some security cameras do offer storage to a memory card inserted into each unit as the only option or as one of multiple options (**Figure 5**). Cameras are set to either write until full or delete the oldest video automatically as storage capacity starts to reach its end.



Figure 5: A modern memory card can hold oodles of video. (Courtesy Kingston Technology)

Cameras from Oco, for instance, can accept a memory card and simultaneously stream to cloud storage, including a limited free tier. This is true with newer, third-generation Amazon Blink models, which use a coordinating hub—called a "sync module"—that can hold a memory card capturing video for several cameras.

Note: This is sometimes called "edge" recording, because that term is often used to refer to stuff networks that are end points: attached to the internet, but not a nexus that passes data between two points.

Note: A handful of cameras have a USB port for a thumb drive or powered USB drive. It seems rare.

Because a memory card can be removed, some models let you mount a removed card on a computer so you can copy files off to a storage drive or your encrypted online storage under your control. This allows deeper archives.

Record Locally, But Can't Disable the Cloud

Here's an irritating feature: NETGEAR Arlo has several camera models that can use either a microSD card or USB drive, but it's always as a simultaneous recording. There's no way to disable cloud recording on those models. Newer units from NETGEAR, like the VMB5000 or VMB4540, can opt to record only locally, however.

Here are the characteristics of memory cards used with cameras:

- **Capacity:** Varies. Typically from hours to days, depending on memory card storage, video quality, and whether full video or motion-triggered clips are stored.
- **Capture kind:** Usually an option for either motion-triggered clips or continuously stored video.
- **Cost:** Low and fixed. SD and microSD card storage prices have dropped enormously in the last few years. A 128 GB SD or microSD card from major brands is around $20. The cost is so low that you can purchase multiple cards and swap them if you want to copy the contents for archiving.

- **Bandwidth requirements:** None.
- **Protection:** Highly subject to natural disaster and theft, though memory cards are quite resistant to hardware failure over long periods of time. They can even sometimes survive damage, because they're enclosed in a slot within devices. A memory card is often best paired with a camera that's well secured out of easy reach of a burglar or other criminal.
- **Privacy:** If you use a device that only stores to a memory card or can be configured to use only that method, you reduce the potential for others to gain access, as they require physical access.
- **Security:** Only Eufy said they encrypted everything recorded to local storage, and allowed playback only on the device from which the recording was made when the owner is logged in. However, given events of late 2022, it's not clear how accurate their previous statements were, and they changed promises in their privacy policy and elsewhere.
- **Quality:** The option is available for top quality, because the cameras are dependent entirely on local storage limits instead of LAN or internet bandwidth for transfer.
- **Access:** Many camera makers that offer memory card slots also offer remote access through their apps to live and stored video. This can be configured in some cases, however, to limit access except to configuration over a LAN. Physically possessing the memory card would then be the only way to view captured video.

A memory card is a great choice in five scenarios:

- **Total privacy:** You want nobody else to have access to your video and don't want to store it anywhere on the internet. Someone would have to gain physical access.
- **Cost:** The one-time cost of a few SD Cards dramatically outweighs nearly every alternative except the network video option described below.
- **No good internet access:** For places in which there's no easy access to the internet or it's intermittent, slow, or expensive, a memory card provides an alternative.
- **Internet outages:** You want to be sure that even if a camera loses a connection, so long as you can gain access to the camera, you can retrieve captured video.
- **Quick access:** If you have an expensive, slow, or unavailable internet connection, you can still access your stored video.

Personal Cloud/Internet Storage

While the trend for consumer cameras is towards proprietary cloud storage, there is still a stratum of devices that offers an option for streaming video or backing it up to storage entirely under your control. This category of camera is often called an “IP camera,” or it’s a feature that requires configuration in a storage section of a product with multiple options.

The simplest of these devices can use SFTP (Secure FTP), https (secured web), or another secure protocol to interact with standard file-transfer server software at a hosting company or on a virtual server you might operate yourself.

However, some systems let you plug instead into a cloud-storage provider, which can provide effectively unlimited amounts of storage—though there are fees each month based on stored data and fees for downloading or scanning through video.

Here are the characteristics of your own online storage for cameras:

- **Capacity:** With a server you own or lease, you’re bound only by your device’s drive-based storage. With cloud storage, it’s effectively infinite. Some hosting services let you add storage on demand or tie your server into their in-house cloud service, too.
- **Capture kind:** You can typically choose continuously stored video or motion-triggered clips.
- **Cost:** For your own servers, the cost may be nothing above the price you already pay to run the equipment or virtual machine.
- **Bandwidth requirements:** Typically similar to proprietary cloud, but varies by equipment, compression, and resolution.
- **Protection:** Video is stored remotely, so it’s vulnerable only if not secured properly. Video can be captured up to the moment internet connectivity is disrupted or a camera is stolen, destroyed, or disconnected. Depending on your server configuration or cloud service options, your data may not be encrypted while it’s at rest and stored on a drive. However, that’s largely a risk only if someone obtains your login credentials, which is a similar risk for proprietary cloud video storage, too.

Use FTP Only When It’s SFTP or FTPS

Beware cameras that offer “FTP” service, but don’t provide encryption in transit. FTP is a truly ancient internet service, developed long before encryption was necessary or even widely available. It’s a straightforward network-based device-to-device copying protocol. FTP traffic can be directly intercepted on a local network or any point between a device and a server.

Decades ago, a version of the terminal-connection software SSH (Secure Shell) was adapted to file transfer as Secure FTP (SFTP), even though it really has little to do with the original FTP protocol

except its name. FTPS is much like HTTPS: regular FTP with encryption-in-transit added. Either is acceptable.

Unfortunately, even some very modern cameras aren't up to date. Netatmo's cameras are seemingly state of the art, but support only FTP, according to their support documents.

- **Privacy:** Controlling your own storage prevents outside access unless the camera maker has built vulnerable software that's exploited or the service you're using can be broken into.
- **Quality:** Can be extremely high, depending on your bandwidth choices, as you're not bound by a camera maker's service options.
- **Access:** You may face hurdles in accessing video stored this way, because company-made software may not provide easy access. You may have to look for files by modification date, download them, and scan through them to find what you want and be on a high-bandwidth connection to do so. However, you can typically use a range of standard file-retrieval or video-storage-playback tools, instead of a maker's proprietary tools.

Personal online storage of video provides a good balance of privacy, capacity, and access for the privacy-minded person who also feels confident in how well they can secure their video data. It pairs neatly with the use of a memory card as a local backup.

Local Network Video Recorders

Some security camera makers build their systems around multiple cameras that stream video from *dumb* cameras—ones that perform no onboard analysis—to central storage on a specialized appliance or a computer running special software, called a *network video recorder* (NVR) (**Figure 6**). These can be configured with multi-terabyte drives to store continuous video for days to months.



Figure 6: *A network video recorder centralizes storage on a local network. (Source: Reolink)*

In previous versions of this book, I covered centralized systems, because they were the only affordable way to deploy many cameras, store video locally, and retain continuous video. Now the *smart* cameras described throughout this book come in enough variety, at low enough cost, and with enough affordable and secure storage options, you can pick among devices in this book even if you want or need to install many individual cameras.

How To Retrieve Video

It’s one thing to store video; it’s another to retrieve it. It doesn’t matter how good your system is at recording video or capturing clips when it recognizes motion if you can’t easily gain access to it.

Depending on your needs, different priorities on accessing video will affect the choice you make about a system:

- **Streaming:** Can you access live video? All cameras I’ve looked at offer some form of live streaming, whether it’s over a local network or remotely, and almost always both unless you’ve disabled internet-based streaming or access. (Don’t buy a camera that doesn’t!) In some cases, however, the maker requires that you pay for a subscription to view a live feed, even if they let you view recently stored clips at a free tier. NETGEAR Arlo is one such ecosystem. Canary provides smartphone/tablet-based live access at no cost, but you can only view live video on the desktop if you have a paid subscription.

- **Motion-triggered clips:** One of the best features of modern security cameras is that they can figure out when motion occurs and upload clips only in those period or mark those periods even when continuously streaming for easier access via the viewing site or software (**Figure 7**). When retrieving video, you can flip through or select from time-stamped motion-based clips instead of scanning across hours of video.

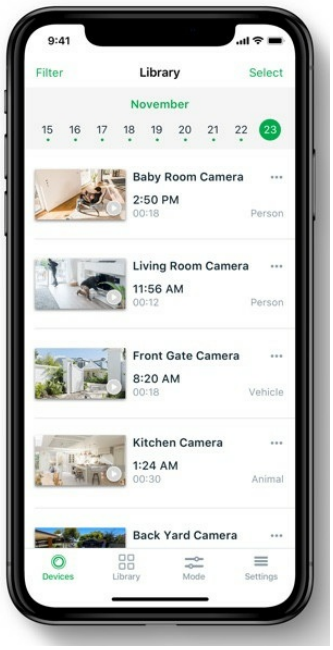


Figure 7: The app for NETGEAR Arlo organizes motion-triggered clips by time and identifies them by location. (Source: NETGEAR)

Note: Motion triggers can be set up in different ways, and may rely on infrared beams or computer analysis of video frames. For specifics on how that works, read Motion Triggers.

- **Mobile, desktop, and web apps:** Modern systems all provide a mobile app, but if you need a desktop app or access through a desktop browser for better viewing conditions, is that available, too?

- **Downloads:** It's often useful to store clips or a whole mess of video for future reference. Is that possible in a camera system's software? And how difficult is it? Some apps will let you download video directly to the photos repository on the device you're using; others may send you a link or require that you export the video. Desktop apps and web browsers more readily let you save directly to a folder somewhere in the desktop file structure.

Pick Your Storage Method

Now that you know about all the tradeoffs and options involved in storage, you should decide which method you want to rely on. This will shape every camera you consider purchasing, or may lead you to reconfigure an existing system or get rid of it favor of another.

In my view, there are three ways to consider which option will work best given your feelings about privacy and your interests in quantity and exhaustiveness of video stored:

- **Just the important clips in the cloud:** I expect the majority of readers, like the majority of camera buyers, just want motion-triggered (and sometimes audio-triggered and other events) to be captured and made readily available through cloud-based storage that you're not responsible for configuring or maintaining.

  If you're worried about privacy, but are an Apple user and feel you can trust the company, HomeKit Secure Video might be the right compromise for storage, even though it's available only from a limited number of camera makers (see Apple HomeKit).

- **Private recording, primarily events:** If you don't want any of your video to leave your local network, you're not alone. It's a common desire these days. You need to choose cameras that use local on-board storage. These options are quite affordable and readily available, and avoid recurring cloud-subscription fees, too. Your local storage is subject to theft, corruption, and disaster, so consider that as the main tradeoff.

- **Full-on recording:** If you want to have a complete record of everything that lasts for months on end, for whatever reason, you can only use an option I noted above in Local Network Video Recorders. Those systems include an NVR that you could equip with terabytes worth of drives. While this is vulnerable to theft, accident, and disaster, it's the only way to achieve that. I don't recommend this approach for most residential users.

Consider Physical Parameters

Home security cameras come in what feels like a nearly infinite combination of hardware features. As the cost for sensors, processors, cameras, and network interfaces has dropped, equipment makers can pick and choose broadly what they want to build in.

In this chapter, I help you navigate through the thickets of hardware. I start with an important issue of the value of a brand-name product (or lack thereof). You'll then learn about each category of hardware feature: network interfaces; stands, mounts, and power; motion-sensing types used with cameras; the variety of options you can get with a camera; and all the other hardware sensors, inputs, outputs, and so on that can be part of a security camera.

Pick a Brand Name?

Cameras and camera ecosystems that link them together span a broad spectrum of pricing. You can buy a no-name brand with a super-cheap price tag—and then worry if its security is up to snuff, and whether flaws will be fixed in software updates. Or you can spend a fortune and find that ongoing costs aren't worth what you get out of it. It would be nice if you could simply predict value by price.

I do not want to be the kind of technology person who tells you to trust brand names. Controversies and security issues erupted in late 2019 and early 2020 with the Amazon-owned Ring camera system, which should put the lie to big brand names being the solution to worries about products.

> **Note:** Amazon has since been squeaky clean and even upgraded its privacy options for some cameras to include end-to-end encryption for video recordings and live video.

But the converse is that what I might uncharitably call "no-name" products have their own set of problems. Because of the simplicity and low cost of creating new electronic products in China and some other Asian nations, the number of options for consumer products has exploded. Many are identical or nearly identical, relying on mass-produced hardware that is lightly customized for a particular buyer. I suspect if I wanted to, I could go to the Alibaba marketplace and create a GlennCam line of hardware to sell to you.

These products from small companies with no history or reputation by which to judge their performance often rarely update firmware for their cameras and apps used to access them after an

initial sales period that can be less than a year. Security problems or updates to mobile operating systems may render your cameras hobbled or unusable.

But to play devil's advocate with myself, a number of well-known electronics companies have also been challenged in recent years with not updating firmware on hardware they sold that's not very old and which has gaping security problems. For example, flaws a few years ago in implementations of Wi-Fi security that required updates in the firmware in Wi-Fi gateways revealed that several well-known firms weren't that interested in producing updates for recent or even current products very quickly.

With internet-connected devices, it's critical that security exploits in account management and firmware are dealt with right away. You need to trust the company to run a tight ship on security, to guard your privacy according to the promises they make (see Protect Privacy for more on that), and to release software and firmware updates quickly when exploits are uncovered.

I wish I had a magic formula to tell you which companies to trust, but I can offer this general advice:

- Check that the company has a history. If you've never heard of the company, can't find a trace of them on the internet, and they're not operating offices in a country you live in or outside of China, you should likely not purchase a product from them.

> **Note:** There's nothing wrong with China, but a lack of regulatory and business oversight in the country on international sales in particular sets a higher bar for companies that exclusively operate there. Many larger Chinese firms have offices in the United States, Europe, and other nations, however.

- Determine whether the company has a *bad* history. If they've faced similar problems in the past, no matter how large or long established they are, their response to those situations should be a guide.

- See how well they provide answers on Amazon.com and other online forums. While reviews may be faked, user questions about problems and a lack of answers (or a hostile answer!) are generally true. Consult Fakespot and ReviewMeta for an evaluation of the quality of reviews for a given product.

- While reviews on product and retail sites are unreliable, it's still worth looking through them and disregarding those that don't provide specific information. In particular, try to find mentions on independent sites that specialize in security or electronics.

Tip: For more insight into picking a company you want to buy hardware from, see my article in TidBITS, How To Buy Hardware That's Likely to Last.

Choose a Network Connection

You might think that Wi-Fi is the best option for video cameras, because it's the easiest way to connect them to a local network. This is true, especially for battery-powered and outdoor units!

But Wi-Fi can also be a problem. Your existing network may be unable to handle constant streams of bandwidth-hogging video. Let's look at the tradeoffs between Wi-Fi and Ethernet connections—without forgetting cellular, too!

Wi-Fi Connection

I would guess the Venn diagram of people who want a home security camera system and who have Wi-Fi installed is nearly a perfect single circle. And thus it might seem like your first and best choice would be to connect a camera via Wi-Fi.

However, despite having written about Wi-Fi for nearly 20 years and practically having Wi-Fi as my middle name, it's not always the best choice.

Wi-Fi is designed to be robust, so if an adapter inside a device and the nearest Wi-Fi gateway to which it can connect are unable to communicate at the highest possible speed, the two devices perform a variety of handshaking until they agree on a lower speed, one that can change dynamically as conditions change, too.

This means that your "3 Gbps" or other marketing-word Wi-Fi network might be communicating with a camera at one edge of your house with various physical obstacles between it and the Wi-Fi gateway at 11 Mbps or 54 Mbps instead of hundreds of megabits per second or faster.

Because cameras are streaming a continuous and often high level of data, a slower connection occupies a larger percentage of the network's available traffic slots than a faster connection.

That said, Wi-Fi may be your best or only choice in these circumstances:

- **No Ethernet**: If you don't have an Ethernet network in your home beyond a connection on your broadband modem, Ethernet is likely a nonstarter unless you also want to string wires through the walls (or behind furniture).
- **Ethernet doesn't reach:** It can be expensive and frustrating to add an Ethernet outlet even if home is wired for it. You have to trade off the issue of consistent throughput for the camera versus the cost and effort of installation. Me, I'd add an inexpensive additional Wi-Fi access point, as I note below.

- **Outdoors:** Most of us don't have external Ethernet jacks on our houses. If we did, we'd also have to deal with weatherizing the jacks. In cold weather, Ethernet cables can crack and fill with water or ice and fail, and you're supposed to rely on special, more expensive outdoor cables designed to weather heat, water, and ice.

If you're certain you want to use Wi-Fi or you have no good choice other than wireless networking, you can ensure that your cameras don't have video sputters or overwhelm the rest of your network:

- **Check your cameras' settings.** You may be able to reduce throughput requirements by picking a lower resolution or increasing compression (which adds artifacts and reduces quality) to achieve better video consistency.

- **Upgrade to Wi-Fi 5 (802.11ac).** If your camera supports the 5 GHz band (see Some Cameras Work over Only One Wi-Fi Band, below), you should use Wi-Fi 5, the fastest affordable flavor of Wi-Fi that's widely available and supported. Some cameras may only include Wi-Fi 4 (802.11n), but Wi-Fi 5 routers are backwards compatible, and you'll get overall better throughput on your network, which will leave more "room" for the cameras to stream video.

> **Note:** Wi-Fi 6 and 6E, derived from 802.11ax, are the latest Wi-Fi flavors. However, most security cameras remain on Wi-Fi 4 or 5, as those flavors are cheaper, don't require re-engineering, and can adequately support video streams. Some newer expensive cameras have upgraded; read specs carefully if you're concerned about cameras having an impact on overall network throughput.

- **Add Wi-Fi access points.** You can increase your network's capacity and by adding units closer to the cameras you want to deploy. Several Wi-Fi gateways with the same network name and security method look like a single entity to Wi-Fi clients, which connect to (ostensibly) the nearest, strongest signal. Even 802.11ac gateways designed to extend networks can offer great throughput and cost under $50.

- **Switch to mesh wireless.** This alternative to classic or traditional Wi-Fi lets each base station—called a node—communicate wirelessly with all the others and help provide optimum signal strength. It's also very easy to add another node if you need better throughput with almost no configuration at all.

> **Tip:** For more advice on purchasing, upgrading, and expanding a Wi-Fi network, consult my book *Take Control of Wi-Fi Networking and Security*.

Some Cameras Work over Only One Wi-Fi Band

Wi-Fi relies on unlicensed spectrum to communicate in much of the world (including the United States, Japan, and most of Europe), which lets you use it without having to obtain permission. That spectrum currently comes in three varieties: 2.4 gigahertz (GHz), 5 GHz, and 6 GHz. Some home security cameras use only 2.4 GHz networking to reduce cost and battery usage, reasoning that the streaming data speeds required will work fine within those limits.

Most routers are *simultaneous dual-band*, which currently means that they have separate radio systems that create unique networks to handle devices connecting over 2.4 GHz and 5 GHz; it's almost impossible you have a router made in the last several years that doesn't do this. Nearly all smartphones, tablets, and computers—not to mention many other devices—work over both bands, too, preferentially choosing the one that has the strongest signal.

You should rarely have trouble with a 2.4 GHz-only camera, because that band can carry signals farther (but more slowly) than 5 GHz or 6 GHz, as the higher-frequency band is more readily blocked by physical objects. If you can't seem to connect your camera to your Wi-Fi network, make sure the 2.4 GHz network is enabled—some routers let you disable it—and you have a strong signal for your camera.

Wi-Fi routers with Wi-Fi 6E, supporting the 6 GHz band, and routers with simultaneous *tri-band* support, appeared in 2022. However, most Wi-Fi clients in computers, mobile devices, and security cameras are far behind.

Ethernet Connection

Wires are cool. I mean, they're completely *not cool*, but they really do fit the bill in delivering high-speed data reliably. While I love Wi-Fi and write extensively about it, and have six Wi-Fi routers in my relatively small home, I connect all but one of those base stations via Ethernet. (The sixth uses powerline networking; see below.)

Why? Because gigabit (1 Gbps) Ethernet is inexpensive, reliable, and consistent. Ethernet switches for connecting devices and Ethernet cables are very cheap and typically reliable. (When something's wrong with Ethernet, it's almost always a bad cable, though!)

Not all cameras support Ethernet; many models are Wi-Fi only, because it's a popular option and cheaper for the manufacturer. However, some multi-camera systems require Ethernet to feed data to a NVR (network video recorder), which handles compression and storage, because they send high-resolution feeds.

Try Powerline Networking

If your home lacks Ethernet wiring and you don't want to string cables, but believe Wi-Fi won't meet all your needs, powerline networking provides a great intermediate option at an affordable price.

Powerline networking encodes data over home electrical wiring, and can perform at up to hundreds of megabits per second—as high as or higher than Wi-Fi rates but less than Ethernet.

To use powerline network, you need at least a pair of adapters which plug into electrical outlets. One goes near an Ethernet switch or a Wi-Fi base station or broadband modem with ports to connect devices to your local network; the other or others are placed near your cameras.

That's how we've spanned an area in our house that lacks Ethernet, would be hard to wire, and is a dead zone for existing routers. From a router nearby we use powerline networking to connect to another room, and then have a Wi-Fi network extender connected via the powerline's Ethernet plug.

Cellular Is an Option, Too

You're not limited to Wi-Fi and Ethernet—some camera models can use cellular data networks for video capture to cloud storage and remote access. This has a distinct advantage in a few ways:

- No other broadband connection is required.
- A criminal or accident severing a network connection doesn't affect video capture (up until the moment the camera is disabled, if someone tries to take it out!).
- Cameras can be put in locations where it would be difficult to reach via Wi-Fi or Ethernet.
- Cameras can easily be placed temporarily in a location.
- Solar-powered models can run indefinitely.

Such cameras are not designed to stream live video to a cloud service because data use would be excessive. The Reolink Go, for instance, which has 4G LTE cell-data support, and captures only motion-triggered events to a microSD card and to the associated cloud service. The same is true of the NETGEAR Arlo Go (**Figure 8**).



Figure 8: The compact Arlo Go is cell backed. (Source: NETGEAR)

You really burn up large amounts of data only while watching a live feed: 1 GB per hour for the higher-quality mode and about one-tenth that for the lower-quality mode.

Carriers vary in how they price service offerings. In some cases, you can add a camera for a flat rate, such as $10 per month, like a smartwatch or tablet. In other cases, you have to prepay for usage or purchase a special plan.

Mull Mounts and Pick Power

Cameras are manufactured to different tolerances based on whether the model might be placed indoors or outdoors. All the established security camera makers offer one of each variety, combined indoor/outdoor units suitable for both, or variations based on weather severity or outdoor placement.

Coupled closely with location is how a camera will be powered: an electrical outlet is nifty, but battery power is often necessary. If you're mounting a camera where it's hard for someone to spot or disable, how often do you have to climb a ladder or get on the roof to recharge it?

Indoors and Outdoors

Cameras have different manufacturing and operating requirements depending on whether they are intended to be used only indoors or could be used either indoors or outdoors or only outside.

Indoor-only models are typically designed for a more modest range of temperatures and humidity, like most non-mobile electronic devices, such as a TV set or AC-powered speaker. Often, makers assume power is readily available.

Outdoor-capable or outdoor-only models come with a variety of mounting brackets or add-on options, and are resilient to severe temperatures and resistant to water intrusion. They're almost always battery powered, though some have an AC option.

Let's look at how models are designed for each purpose—or both.

Indoor Cameras

An indoor-intended camera is likely to be AC-powered or have an option or model that's AC-powered, and come with a long cord if so. They usually have a simple stand. Mounting options tend to focus on an easy connection to a wall or, sometimes with an optional kit, attaching directly against a windowpane, facing outward (**Figure 9**).



Figure 9: Cameras used indoors sport an array of stands.

Inside, Looking Out

You might think at first glance the indoor/outdoor decision is as easy as, "I want to see things inside my house, so I need an indoor model for this location; for things outside my house, an outdoor model is the right choice."

However, because of power, network, safety, or theft issues, you may choose to mount an indoor camera pointing outwards, as we do in my home. That works fine during the day and when all the inside lights are off at night, but reflection can be an issue a night with the lights in the room on.

It also means that a camera with infrared night vision will only pick up its reflection—while most of the invisible light passes, enough reflects to make the video stream unusable. (Pick a model that lets you disable night vision if you make this choice.)

It's less likely you'd install an outdoor model looking in through a window; between reflection and field of view, it's not of great utility.

Some cameras come with a simple stand, so you can place them on top of a cabinet, counter, or entertainment console.

Indoor cameras typically are designed for a narrower range of operating temperatures, which is usually only an issue in extreme climates and unheated spaces, like garages, the inside of outbuildings, and unfinished basements.

Most cameras equipped with Ethernet (either alone or with Wi-Fi) are intended for indoor use.

Outdoor Cameras

Cameras intended to be used outdoors almost all have a common set of typical parameters:

- **Weather-resistant:** The camera needs to be sealed against moisture, and may even been water-resistant or waterproof. It can also operate in a large temperature range, often well below freezing and up to 140°F (60°C). (The ambient temperature will never be that hot, but the reflected or absorbed temperature can be.)

Water, Water Everywhere nor Any Drop Intrudes

Electronic gear that's weatherproofed has a two-digit standard Ingress Protection (IP) number. The first digit is about intrusion and the second about water. You almost certainly want that first digit to be a six, which means no dust or other particulates can penetrate.

As to the second digit, you will want at least 4 (resists rain and splashes) as in IP64, but it's more desirable to have one rated 5 (low-pressure water jets, as from a hose) or even 6 (high-pressure water jets, and invite me to your parties).

It's unlikely you'd find a camera with a higher rating, as those relate to immersion. All iPhone 11, 12, and 13 models, for instance, are rated IP68, which means they can be submerged. Apple further tested them for depth, and the 12 and 13 models can survive being up to 20 feet (6 meters) under water for 30 minutes!

- **Battery-powered:** Often, an outdoor camera is hard to reach—which is kind of the point to have a better vantage to record and to be theft and damage-resistant. This makes it unlikely you could supply AC power—and you probably don't want a cord that could be cut or pulled to grab the camera. Consider while determining placement how hard it will be to get to in order to unmount or remove a swappable battery, as you'll be carrying that task out every few weeks to months forever. A long-lived battery is also therefore highly desirable. A battery may also be paired with a solar panel, removing the need to recharge it at all. (See more detail below under Pick a Power Source.)

- **Wireless:** Per earlier discussions, running Ethernet to an outdoor camera may be tricky unless it's directly attached to a house or other building.

- **Several mounting options:** Because of the variety of outdoor locations, you often have your choice of mounts for a single model (typically sold for additional, but not outrageous cost), or models that each have a different mounting style (**Figure 10**). Third parties also offer universal mounts and some tailored to specific major brands.



Figure 10: As with indoor stands, outdoor mounts have a lot of variety, but typically focus on a solid attachment and a way to move it into a desired, fixed position.

You also may be inclined to want a tilt, pan, rotate, and zoom camera for outdoor use to provide more flexibility. See Movable Point of View for more details on those options.

Pick a Power Source

Cameras can be powered in two ways: by being plugged into an AC outlet or by an internal, rechargeable battery. But there are three related options to consider:

- Solar power for outdoor units to avoid swapping batteries or retrieving a camera to plug it in to recharge its battery

- Power over Ethernet (PoE), a way to deliver network and power in a single cable

- An uninterruptible power supply (UPS) to ensure an AC-powered unit keeps working if there's a power outage

AC Power

Outlet power is pretty straightforward: Plug 'er in. It's done!

However, it's worth checking specs on cameras, as the power-cord length can vary quite a lot from model to model. You may need a very long cord to reach from the camera's location to the nearest outlet. An extension cord might suffice, but it can be ungainly and aesthetically displeasing. This is where PoE could come in, too, as noted just below.

Many cameras rely entirely on USB. There is often a jack on the camera, which is commonly a standard squarish USB Type-B slot, such as is found on printers and older hard drives. The camera comes with a cable that has a standard USB Type-A plug on the other end, and a USB adapter with a Type-A jack.

Note: Cameras don't yet seem to have adopted USB-C, common now in computers, mobile devices, and headphones.

You may be able to plug into an existing USB power source, such as if you have a new outlet type or a power strip with USB jacks meant for charging. You may also be able to supply your own very long USB Type A-to-Type B cable instead of using the included one.

If you need an AC outlet, depending on your home construction (and whether you're renting), you may be able to have an outlet added affordably near the location you want to place a camera.

Doorbell Cameras May Require or Allow Special Wiring

Analog doorbells are wired through a transformer that provides continuous power that might be anywhere from 8 to 24 volts (V). Many doorbell camera models that replace an old-style press-button chime doorbell can work with some or all of that voltage range, though some models work with only one voltage (often 24V), and others have multiple models for different voltages (like one for 8V to 12V and one for 16V to 24V). (See an overview of doorbell models earlier in Ding, Dong! Who's There?.)

In many cases, you just need to turn off the circuit breaker that covers the doorbell, unscrew the old one and use a pair of needle-nosed pliers and a screwdriver to wire in the camera. In others, however, you might want to replace an existing transformer with a new one of the right voltage—Amazon offers a 16V drop-in replacement designed for several of its models. In some cases, you may need an electrician to repair a wiring issue.

Yet another option to power a doorbell camera if you don't have an AC outlet nearby, there's no active transformer, and you don't want to hire an electrician is a plug-in transformer of the right voltage. Sold for under $20, these transformer have low-power wiring you can run through a wall more easily installing new AC wiring.

Battery Power

A battery-powered camera typically costs a bit more than an AC-powered model, but it has so much more flexibility, it's typically worth it. Some manufacturers sell only cameras that include a battery, although they may also offer an option for AC power or sell an AC adapter as an add-on.

A battery is generally appropriate only for cameras that record just a few minutes of motion-triggered video per day, mostly in daylight, as infrared illumination takes more energy. Above that or with mostly night-time recording, and you might have to recharge or swap a battery every few days or weeks instead of monthly or less frequently.

You must rely on AC power if you need tens of minutes of video a day or continuously streamed video.

> **Some Cameras Switch Features Based on Power**
>
> I have found some camera models offer both passive infrared (PIR) and computer vision (CV) types of motion triggering, discussed in full in Motion Triggers later in this chapter. However, they rely on PIR when using a battery and switch on CV only when plugged in. This makes sense, because CV requires a camera to be in constant operation to determine motion.
>
> For cameras that offer 24-hour-a-day cloud recording options and cloud-based CV analysis, likewise they must be plugged in to continuous power.

Many makers let you remove the battery part of a camera, either as a battery pack that can be detached or extracted or as individual battery cells. These are almost always lithium-ion based, the same as used in smartphones and electric cars. Some cameras, such as the Amazon Blink camera line below, may require non-rechargeable, long-life lithium-metal battery cells. However, you will never wind up using alkaline and other rechargeables, as they can't provide power for long enough (**Figure 11**).

> **Lithium-Metal Battery Warning**
>
> Lithium-ion and lithium-metal battery cells are not interchangeable. Lithium-ion batteries produce more voltage. Read a camera's specs carefully before ordering additional batteries.



Figure 11: The batteries at left are lithium metal; at right, lithium ion. Yes, they look *very*

similar. The only way to ensure the difference is to read the labels carefully.

Get a Spare Battery for Outdoor Cameras

I advise that for outdoor cameras, you always purchase a spare battery that you can charge separately. Otherwise, you have to access the camera, remove the battery or the entire camera, plug it into power and wait for charging to complete, and then remount it.

With a removable spare battery and an external charger, you access the outdoor camera once to swap the battery and charge the depleted one for the next go-round.

There's no single way to measure how much life you get out of a single battery charge, because no two camera makers use precisely the same battery and circuitry to hook it up.

Several factors play into how frequently you have to recharge or swap a camera's batteries. I noted the duration of recording and infrared night-time capture above. Temperature is another issue: a camera operating far above or below about 68°F (20°C) will deplete a battery faster. As a rechargeable battery ages, it also decreases in capacity, requiring more frequent charging. If used in extreme temperatures, its capacity will decrease faster, too.

Manufacturers often provide guidance about the number of hours to weeks you can expect from a fully charged battery, although it's sometimes vague and highly footnoted. Two clear exceptions include Amazon's Blink and Lorex Technology.

Blink promises two years' service using replaceable, non-rechargeable lithium-metal batteries on their third-generation hardware (**Figure 12**). The company explains this further in a support document that the estimate for its first-generation equipment is 50 seconds per day of motion capture—it grabs five-second clips—and live viewing, or 11 hours across two years. For second-generation equipment, Blink estimates an average of 70 seconds of clips and live viewing, or about 14 hours over two years.



Figure 12: The Blink Indoor promises to last two years with a single set of batteries, or four years with an add-on battery pack.

Lorex Technology includes notes in the technical specifications for all their battery-equipped systems. For instance, for their L222A8 and U222AA "wire-free" series, the company estimates, based on 24 triggers per day, about 4 months with a two-cell battery and 6 months with a three-cell battery before recharging.

> **Note:** Some companies unrelated to the camera maker sell replacement, external, or high-capacity batteries for various models. This is highly useful, as many camera makers don't offer an external battery charger even if they offer swappable batteries!

Solar Power

For many outdoor installations, you may not be able to get to a camera easily to charge or swap its battery. Or you might prefer the convenience of never having to do so! A solar panel can dramatically reduce your need to interact with the camera.

Several security camera companies offer an integrated, bundled, or add-on solar panel designed to provide just the right voltage to charge the battery during the day. This trickle charge can let you record far more video per day and night, although you're still limited to motion-triggered events.

The cost is typically quite low: $25 to $80, depending on the features and thus battery draw of the camera. Reolink has a $24.99 panel for several of its camera models, and Ring has a $59.99 add-on. Third parties also offer solar power options for cameras that don't have a manufacturer-supplied product (**Figure 13**).



Figure 13: A third-party solar panel from Boao offers ongoing power to Amazon's Blink cameras.

Solar panels should match or exceed the water-resistance IP rating discussed in Water, Water Everywhere nor Any Drop Intrudes. And some maintenance is required: every few months, or whenever you notice the charge isn't topping up as fast, you need to wipe down the panel to remove dust and debris that reduce its charging capacity.

Power over Ethernet (PoE)

With Power over Ethernet, a camera draws its power and its connection to an Ethernet switch from a single special type of Ethernet cable. This lets you avoid using a battery-powered camera and its tradeoffs, while not having to have an AC outlet nearby your camera or have one installed. It's a form of low-power wiring similar to that used for outdoor lightning.

Most PoE works within the power limits of standard modern Ethernet cable varieties, known as Cat 5E or Cat 6, the same kinds required for reliable gigabit Ethernet. You can upgrade an existing Ethernet switch in your home cheaply to get one that supports PoE; the TP-Link TL-SG1005P is a five-port model with a $50 street price.

Some camera makers build PoE into the Ethernet side of their cameras, but if they don't they may sell a PoE splitter. You plug in an Ethernet cable to the switch, run it to the camera, and plug the splitter in on the other end. The splitter has a DC plug to power the camera and an Ethernet data plug if the camera or another device needs connectivity.

> **Warning!** Because each camera has its own particular DC voltage requirements, you need to either buy a PoE adapter or splitter from the camera maker or acquire a third-party one that meets the camera's specifications. Read reviews carefully, as buyers of many third-party PoE splitters have had negative experiences.

Definitely consider PoE if getting power or networking throughput to each camera is an issue and if you already were interested in centralized local network recording. If you don't already have Cat 5E or Cat6 capable Ethernet, it means pulling wire—or hiring someone to pull it for you and put in the appropriate jacks—but can still be cheaper and easier compared to AC power or batteries.



Figure 14: A PoE splitter lets you power a home camera over Ethernet and no AC outlet nearby. (Source: Revotech)

Uninterruptible Power Supply (UPS)

If you live in an area with regular power fluctuations or outages, you may already have a home generator that can kick in or that you power up. Your first concern with a power loss might not be your cameras, in any case.

However, some people may have the concern that a burglar would try to cut power to the house in order to disable an alarm system or cameras. Most conventional alarm systems include a multi-hour battery backup to keep working across brief power outages and a power cut. This can also allow an older system to call out over a wired phone line, as the traditional phone system doesn't require power from a home to operate.

> **Note:** As many households have given up a wired phone line or never install one, alarm systems now typically offer a broadband/cellular option. If the internet is active via a local network using Wi-Fi or Ethernet, the system relies on that; if it's not, it sends data over a cell modem built in for this purpose.

But smart-home alarms and sensors may be a mix of line power only, battery backup, and battery powered. Having a UPS that's connected to a camera (or multiple small UPSes, scattered around) and your Wi-Fi gateway or Ethernet switch and broadband modem can make it possible to keep video streaming and remotely available even when power is out. You can spend about $100 for a small unit designed to keep those relatively low-power devices in action for one to two hours.

> **Tip:** Consult my ongoing round-up of UPS models at TechHive.

> **Note:** Cable plants (the infrastructure for cable TV/internet systems), fiber-optic, and phone-line DSL networks typically continue to operate to the house even when there's a widespread outage, so long as the outage doesn't last more a few hours to a few days, and the actual cable or telephone wire to your home or area hasn't been severed.

How Cameras Capture a Scene

Security cameras are just like any other digital camera: a lens captures light and then focuses it on a sensor. The sensor is divided into light-sensing elements that produce an image in the form of a grid of pixels. So far, so good.

But there are many aspects of cameras and options to consider in figuring out the particulars of what is captured in a scene.

I break this down into two major characteristics: the part of the view that a camera's lens is pointed at that it captures (and which can be cropped), and the way in which the camera remains fixed on a view or may move to alter what it sees.

Note: I dig into resolution and video-capture quality in the next section, under Resolution and Quality, as it's somewhat distinct from what a camera sees.

A Lens Sets the View

A camera sees the world through its lens, and that lens is really a slice of the direction at which it points—its angle of view (**Figure 15**).

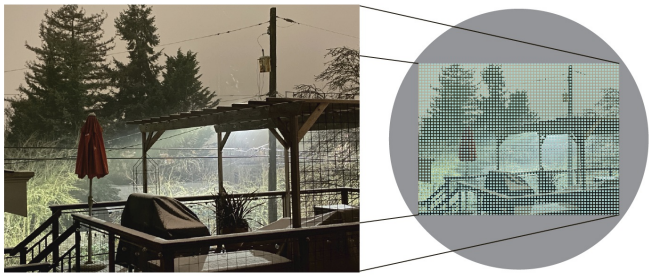


Figure 15: A lens projects a view (left) onto a sensor.

Angle of View

What's called the field of view for a camera is more precisely defined as its *angle of view*, expressed as a single number in degrees (**Figure 16**). This number almost always represents just the horizontal arc from left to right. There's also a vertical measure (from top to bottom), which is proportionate to the capture ratio.

Cameras capture effectively a two-dimensional plane, which is flat, but the measurement is in degrees, because it describes how big a hunk of the sphere around a camera that it captures.

A lens is round, so why does it capture a rectangle? Because camera sensors—whether for a DSLR, smartphone, or security camera—are rectangles, too.

For a standard HD-style 16:9 ratio (or crop, see below), for instance, a 180° field of view (edge to edge on a flat fronted camera) would mean about 100° from top to bottom (**Figure 17**).

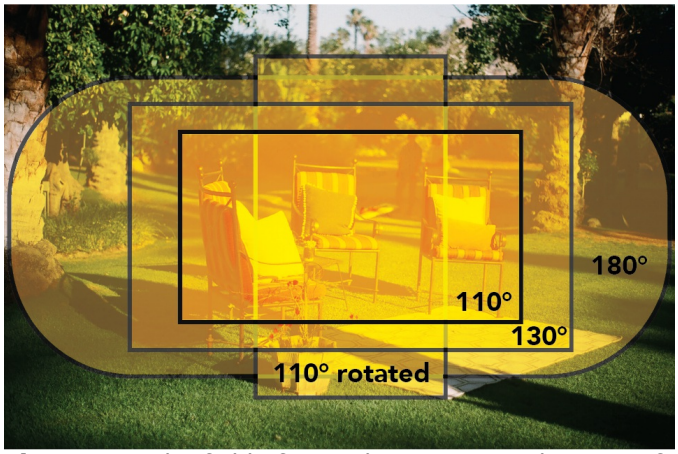


Figure 16: The field of view demonstrates the area of the view that a camera captures. (Lawn scene by Brandon Hoogenboom via Unsplash.)



Figure 17: The Logitech Circle View has a 180° field of view.

The vertical angle is typically less important, because people and other animals walk on the surface of the Earth, and most of what we're trying to see are the movement of non-flying living things from a street level to the top of a flight of stairs, say. In limited cases, you may want to rotate a camera with an appropriate stand or bracket so the default wider horizontal plane is at a different angle or even 90° rotated to capture a bigger top to bottom view.

> **Note:** Because of the fixed ratio, you almost never have a choice about vertical measure, either—but a wider horizontal angle in 16:9 ratio gives you a bigger vertical one, too.

However, some cameras can be mounted in a variety of orientations or manually rotated through 360° around a mount to fit your needs. (That's separate from the tilt/pivot/rotate described in Movable Point of View.)

For a fixed-view camera, I highly recommend a horizontal angle of view of around 130° or more, which is commonly available (**Figure 18**). Many cheaper cameras must rely on a less-expensive

set of optics, and have instead about a 110° angle of view. That captures too small a slice of a room and outdoors, except for some particular installations—like a room's corner.

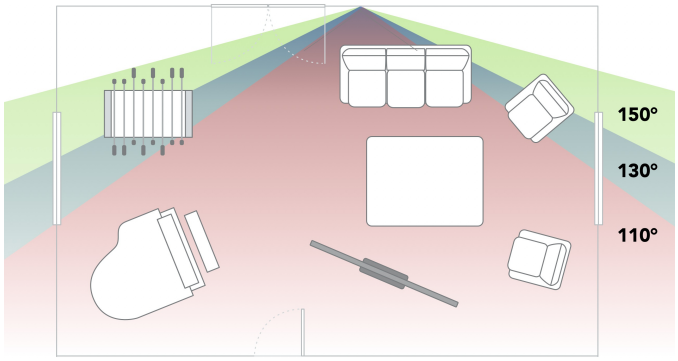


Figure 18: Take a look at a room and consider how the angles of view of different cameras will capture parts of it.

The tradeoff? A bigger angle of view means less detail captured when using the same sensor—such as 1080p. You may need to decide to go from 1080p to 2K or 4K to get the detail you need at the angle you're planning for.

Tip: Get a protractor or even print out a piece of paper showing a semi-circle of 180° of angles. Then have someone hold pieces of string from where you're standing parallel to the angles on what you're holding to "preview" the view of different cameras.

Focus on the Distance

Camera lenses have to focus on a view to provide a clear picture. Many security cameras have a fixed focus with a fixed *depth of field* (the range of distance from the camera that is in focus). That means that only items from several inches away to tens (or even hundreds) of feet away are sharp.

Focus is a mechanical property, like optical zoom, so cameras that can move about or zoom in and out typically also have a variable focus, which can affect the minimum distance at which objects start to be in focus and restrict the depth of field to a narrower range.

Crop the View

Some cameras may let you choose how to crop or frame the field of view, too, by selecting among two or more options. This can be handy if there are fewer or more salient things you want to observe depending on that cropping. With a lens that can go up to 180°, the wider the view, the more distortion, as more of the most bulbous and distorted part of the fish-eye lens gets used.

Note: All fixed-view cameras lack digital zoom, discussed next in Fixed View.

The cropping doesn't change how much of the lens's captured light projects onto the image sensor, and the output resolution remains fixed at 480p, 720p, 1080p, 2K, or 4K, typically.

Fix a Lens or Move It Around

Early webcams and security cams had relatively low resolution, standard lenses, and low frame rates, and made up for it with motors and lenses, so a camera could be moved and zoomed to the right position—sometimes automatically tracking detected motion.

Over time, that changed as the quality of lens and size of image sensor improved dramatically while remaining within the budget of many people. Both fixed and movable options abound for home security cameras.

Fixed View

The majority of cameras aimed at home users have a fixed field of view: their lens has a set focal length, which determines the set of distances at which objects and people remain in focus. That's usually from a few inches to tens of feet.

You put the camera on an indoor or outdoor mount attached to something or a stand that holds the camera in place. If you want to change the view, you have to move the camera.

Some fixed-view systems offer a digital zoom, which is just an enlargement of a subset of pixels captured in the image sensor. Blowing up pixels doesn't add information, though it can better fit into video-playback formats or some *upsampling* algorithms make video appear smoother instead of pixelated, so it's easier to pick out details in it.

A fixed-view camera is the easiest and most likely option to choose.

Movable Point of View

If you have a particular reason—from recurrent theft to bird watching—you may want a camera that can do typically two to four kinds of movement or change of view:

- **Pan:** Horizontal movement left and right relative to a base, typically rotating around the base
- **Tilt:** Vertical movement relative to the base, seen as up and down
- **Zoom:** The ability to change magnification of the view through a motor that changes the relationship between lens elements, allowing a closer view

Note: I don't call out digital zoom in this book, which simply makes pixels bigger and blurrier, as it's generally not useful. Some cameras do offer digital zoom to highlight and follow action, but it's no crisper than the full frame.

Each of those elements has a measurement associated. Pan and tilt are typically in degrees of motion; some cameras can pan nearly 360°, while others have much smaller axes (**Figure 19**).



Figure 19: The Wyze Pan (left) can rotate 360° around its base; the D-Link Full HD Pan & Tilt Wi-Fi Camera rotates 340° and has a 110° range of tilt motion.

Zoom may be measured as a multiple (like 2x or 10x) or by 35 mm lens equivalent—that's like saying "the size of an average book" to help make a mental comparison if you're used to 35 mm (and equivalent) cameras.

Cameras with mechanisms that let them move can always be controlled remotely by an operator with access to the device's software interface. Some can be programmed to sweep in a pattern or even identify motion and track it.

And you can find models that can create a comprehensive snapshot panorama by methodically panning and tilting, something useful for navigating around a space, or to get a picture of the current state of things after a burglary or disaster.

A camera that can move around is typically of specialty interest. These cameras typically have much smaller fields of view, but may also capture more detail, because they're projecting that smaller area onto sensors that have as many pixels as large field-of-view cameras.

Pick Camera-Based Features

Once you have the big parameters figured out, you should also think about which features related to physical video capture you want in one or more cameras in your system. Not every camera needs to have the same features, and some manufacturers offer a large range of models with different options and price points that all work together.

Resolution and Quality

How much detail do you want in the video you capture? It's a key question. When security cameras intended for the home were first introduced, they offered fairly coarse resolution, in the 320p to 480p range (to use modern terms). The frame rate could be quite low, the sensors were noisy, and infrared night recording was poor.

We are so far away from that you face the opposite problem: if you want, you can capture 4K video at 30 frames per second (fps) with the crispness of near-television production quality. It's unsettling.

Super-high resolution requires super-high local network throughput coupled with either terabytes of storage or gigabit internet or both. It's rarely necessary or useful for home installations. If that's what you need, it's possible and affordable.

Many camera offer not just a selection of resolutions at which to record, but also controls over compression. With modern video compression, quite high levels can still allow for a lot of detail. But the more compression you employ, the less detail remains distinct, no matter how high a resolution you choose. It's always good to experiment if you're not sure what setting will work best from the location at which you deploy a camera. Because distance, detail, and clarity will all interact, that's the only way to be sure of the right options.

More likely, you will want to pick 1080p with some degree of compression. This can provide quite a lot of detail, such as resolving faces, license plate numbers, or other elements at a distance as well as up close, but keeps local network transfer, storage, and broadband upload speeds moderate (**Figure 20**).



Figure 20: Resolution affects clarity and detail, as you can see in this simulation of 4K, 1080p, and 720p versions of the same person's face (left to right). (Photo by Craig McKay on Unsplash.)

The difference in quality can be huge. Nest's Cam IQ models consume 2 Mbps for "medium-high" quality capture and 4 Mbps for "high" quality.

The flip side of these options for resolution and quality is that if the bandwidth available isn't high enough to pass through your selected options, the camera will typically dynamically adapt and increase compression or drop to a lower data rate to keep streaming video—just like Netflix does for watching programming.

Tip: For future-proofing a purchase, you may choose a camera with a higher resolution than you currently want to employ, knowing that bandwidth and storage costs drop over time, and you may opt to switch it from 720p to 1080p or 1080p to 4K at a later point.

Frame Rate

Every digital video camera is actually capturing a series of still images at some frequency and packing them in a compressed format for storage and playback. Resolution measures the area of an image, while the frame rate in fps measures how many are captured.

Most of the cameras that list a frame rate say they record at 30 fps—or sometimes, *up to* 30 fps without elaboration. A few cameras are notably slower, like the NETGEAR Arlo, all models of which seem to tap out at 24 fps, and the Wyze cameras, which capture 10, 15, or 20 fps, depending on the model and whether it's using night mode.

The "up to" portion probably has to do with night vision, because the few manufacturers that make it explicit list a separate rate for day and night shooting. Most cameras need a longer exposure to capture an image at night, not just the illumination of infrared LEDs. That means the frame rate slows down. The Arlo models run 15 fps in night mode, while Wyze drops to 10 fps.

The difference between 24 and 30 fps is not much in daylight, as long as the exposure is roughly the same, because you want crisp quick snapshots that don't blur faces or other objects in motion. At night, longer exposures and a lower fps mean blurriness combined with a jerky motion that may not provide enough detail for your purposes.

Some cameras specifically advertise features to improve low-light capture, like high-sensitivity camera sensors and high dynamic range (HDR) capture that combines multiple exposures for each frame.

For daytime use, most cameras have high-enough frame rates to ensure fast-enough exposures. At night, however, you should consider your purpose: Are you're trying to capture crimes and need crisp faces, or spot whether your own cats and dogs are roaming around or if it's other pets (or other animals)? Or do you want just a more general sense?

If night-time crisp captures are a must, focus your research on cameras that offer actual (not simulated) night-time footage on their sites and provide detail about how it works.

Night Mode

When our older kid was a baby, we purchased what was likely the last generation of CRT-based baby monitors that used a very noisy proprietary wireless signal. Its key feature? Night vision!

Using infrared LEDs, invisible and harmless to the naked eye, we could keep our eyes on our little pumpkin.

Nowadays, the picture quality would be 50 times crisper and we'd be able to stream it not to a tiny weird black-and-white CRT but to our mobile phones. Home security cameras typically come with infrared LEDs as a basic option, although some makers offer it as a feature only in certain models to differentiate among tiers or offer a less-expensive alternative.

> **Note:** Back in the CRT days, baby cams used terrible proprietary wireless. One night, we thought our baby was missing. Instead, our device had tuned into another neighbor's crib camera! That's not a problem with modern equipment, thank goodness.

The LEDs are limited in how far they can cast light, and different cameras can have hugely varying ranges. Among models made by Reolink alone, the distance can be 33 feet (10 meters), 100 feet (30 meters), or 190 feet (60 meters).

Some companies go into very granular differences—one model offers 15 feet of illumination, another 20, and another 25. But those are all measured in particular conditions, and you'll always need to test your own views.

The illumination distance can depend on whether the camera is battery-powered (and focused on conserving energy where possible), or optimized for both day and night recording and featuring high-intensity LEDs. Think about a penlight flashlight with one AAA cell battery versus a multi-LED flashlight with several AAs, and the difference in illumination between the two.

Generally, there's no drawback to night-mode recording unless you're preserving battery usage. The infrared LEDs kick on typically automatically when the light is too dim for normal capture, but they do pull some additional power on top of the camera's normal function.

The night mode view is often in sharply contrasting and hard to distinguish black and white, but newer cameras offer color night vision, which relies on some combination of camera sensors with higher sensitivity, higher-illumination infrared LEDs, and image processing.

In some cases, you may want to disable infrared LEDs. In particular, if you use an inside window-mounted camera pointing outward, most models are built such that the infrared LEDs reflect within the window pane, making the image impossible to make out. Such models should offer a configuration option that allows disabling night mode.

Motion Triggers

Most people don't need a continuously recorded feed stored for days or weeks or indefinitely of everything their cameras see. For particular purposes, like needing to monitor cameras and have

footage later for security or law-enforcement purposes, sure.

But that's not the case for the overwhelming majority of home security camera users, who mostly want to know when and if something happens. (For a little extra security, some systems can store full streaming video for a day or longer before dumping it, but might keep motion events longer or indefinitely.)

> **Activity Zones**
>
> Many cameras let you refine motion triggers by drawing activity zones, to specify areas to either monitor or exclude. These activity zones are typically loaded into the camera, and can dramatically reduce notifications, clip recording, and battery usage on wire-free cameras by ignoring motion in places that you don't want to track. See also Configure Triggers.

Most systems are designed around capturing or marking video only when a camera detects motion. Cameras rely on one of two sorts of detection:

- **Passive infrared (PIR):** Passive infrared detects changes in heat signatures. It's a low-power method and generally effective (**Figure 21**). However, it works only over relatively short distances, from a few to tens of feet (roughly 1–10 meters). No visible light is required, but they don't work through glass. And motion typically has to be perpendicular to the beam's direction, which can affect where you mount and accuracy. PIR-equipped cameras may let you adjust the level of sensitivity, which corresponds to the size of object passing through the beam.

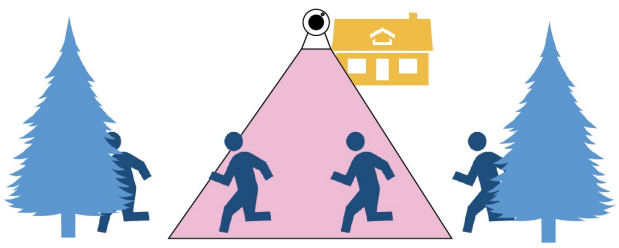


Figure 21: Someone has to pass across an infrared beam to trigger recording with PIR.

- **Computer vision (CV):** Computer vision uses frame analysis and machine learning to detect whether motion has occurred across successive frames (**Figure 22**). CV-based detection allows a user to define zones in the field of vision to watch or ignore. Some cameras let you mark zones to trigger only if the camera system detects a person (by shape or face), or motion by vehicles, animals, or packages (**Figure 23**). CV can also be used for facial recognition to identify particular people enrolled in a system; see Facial Recognition just below. Some CV happens in a camera; other systems may analyze the video in a hub or in the cloud.

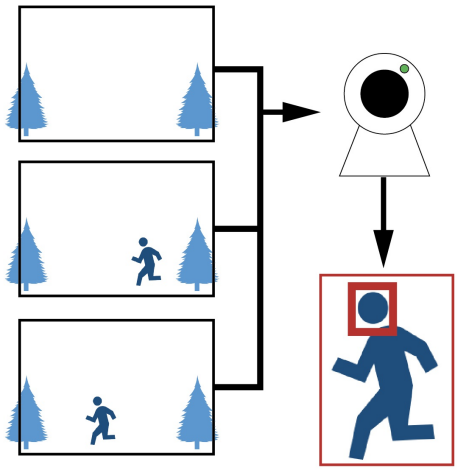


Figure 22: With computer vision, the camera (or, sometimes, the cloud) analyzes successive frames of video to detect motion. It may even identify whether it's a person and attempt to recognize the face against stored profiles.

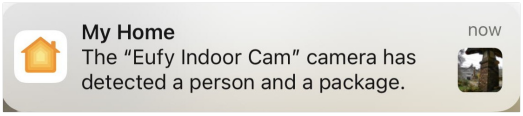


Figure 23: Apple's HomeKit Secure Video alerted me to a person dropping off a package.

- **Both PIR and CV:** Some cameras may combine both PIR and CV, as CV works particularly poorly in low illumination where PIR works as well as in daylight. In other cases, PIR is used when a camera is battery powered and CV when it's plugged in. For a few camera models, CV is only available when a camera is powered and a subscription is active.

The different method of detection can also effect precisely when a recording starts. With PIR, the focus is on preserving battery life. Unless the PIR sensor is tripped, the camera is entirely off. (PIR cameras with AC power may let you choose a different setting.)

That means if an event happens "off camera," but audio, more-distant, or less-infrared-triggering behavior happened before the PIR tripwire, it's not recorded at all.

Tip: Reolink advises pointing PIR-based cameras towards a path that people are likely to cross rather than to walk towards or away from the camera. This cross-path position will more readily trigger motion detection.

With CV, the camera has to be on all time to perform the analysis, and buffers a small amount of video, sometimes as much as 30 seconds. If there's a trigger, a video (and audio) clip including that preceding part will be streamed to the servers or marked as an event and retained if it's automatically streaming everything to an NVR, memory card, or internet-based storage.

This PIR/CV “precognition” difference, where the camera appears to start recording before it “knows” something has happened, can be a make-or-break feature for many people—it is for me. I want a recording to include anything that happens before a major trigger’s threshold has passed; otherwise, I may miss the lead-in to an accident, disaster, vandalism, or theft.

Storage capacity, bandwidth, and motion-trigger capture are all interrelated, and I explain capacity issues for each kind of storage in Choose Where Video Lives. You then need to know not just which kind or kinds of storage a system you’re considering offers and you want to use, but how it manages motion-triggered clips versus full video storage.

Find Out What’s Going on While You’re Not There

Motion-triggered clips can provide some great insight into what is happening around your property while you’re not looking—particularly in the wee hours, at night, and at odd moments of the day.

The single funniest thing I’ve ever seen on my cameras is while my family and I were in London. While there, I would check to see if packages were delivered (so I could ask a neighbor kid we were paying to pick them up) or if anything else was awry.

One morning, I open the app and discover that the largest raccoon I have ever seen in my life—far larger than any I even knew were in my neighborhood—waddled up our front stairs at about 5 P.M. on a summer day, walked down the front walk and around the side of our house. About an hour later, it returned the same way. Haven’t seen him or her since.

Facial Recognition

Some camera systems go beyond recognizing people and actually identify faces. They automatically identify a facial area, and then can match against some kind of stored profile.

There are three ways this can work:

- **Match in camera software, only locally:** Faces are identified generically—not matched against other data you have stored—but you can label faces and the software gradually associates all faces it captures of the same person with that person. However, it happens entirely in locally stored software. The Tend Insights cameras offer local-only facial ID in 47 U.S. states. This option has the fewest privacy red flags, if you trust that the maker is doing exactly what they say they are.

- **Match via HomeKit Secure Video:** Apple uniquely matches faces locally information stored in the device owner’s Photos library, software available across Apple’s operating system that lets people identify faces and add matches over time. The owner can determine whether other people in the household see the matches from their Photos library, too. These facial matches and security camera video are always encrypted before it leaves devices, and Apple doesn’t send facial-recognition data to its servers without user device-based encryption. Apple has been a benchmark for privacy for the most part, and this facial-

recognition approach matches its general approach. See Use HomeKit to Store Video and Trigger Alerts.

- **Match in cloud software:** Facial information is sent securely to a vendor or other cloud, where it's matched against other information you've identified there. This potentially puts this data into the hands of other parties, which can include the company itself, rogue employees, government agencies, and crackers. Google's Nest cams seem to process data this way, although Google goes way out of its way to avoid stating explicitly that it uploads data to the cloud. The feature can't be used in the EU or Illinois. I'd prefer to not have facial-recognition data processed or living the cloud, because even if it's promised that it's only used for my account, the data is outside of my control.

> **Note:** In addition to specific faces, some devices can recognize that a person, animal, or vehicle is in frame, and identify it generally and notify you appropriately.

Consider Extras Beyond Video

I've focused almost entirely on video so far in this book, because it represents the majority of the issues around decisions you make about storage, access, and features. But home security cameras often have additional features, and some have some bonuses on top of those.

Mic and Speaker

Many cameras including audio recording and speaker capability. This lets you record sound alongside video, a natural combination.

Depending on the camera, it might also function as a two-way intercom, which can be awfully handy at your front door with a doorbell camera or if you need to interact with a tradesperson, babysitter, or nanny in your house when you're not there.

You can even yell at a thief! It's been known to happen.

Sound picked up from a mic is almost always recorded alongside video and available with any video motion-triggered clips or stored full-length video. Some cameras may let you disable the mic (and speaker).

Doorbell and Chime

A popular category of multi-purpose camera is the doorbell cam, as discussed back in Ding, Dong! Who's There?. It makes sense: where do you want to see the most what's happening and where do people mostly try to get your attention legitimately?

These combination devices often have a fish-eye style lens to bulge out from its spot on or near your door to capture the broadest (if distorted) view. The focus is very short to allow close-up views that could range from several inches to a dozen feet away. That makes a doorbell camera less useful for general-purpose video views.

These are typically mounted outside, which gives them good visibility, but also makes them susceptible to damage or theft. Some models can be installed through an existing peephole in a door or via hole you drive, like Ring's Peephole Cam. (That sounds much dirtier than it is.)

Because these double as doorbells, someone approaching the camera will send you an alert, and the device has a button someone can press to send a more direct alert, too. Many models may be paired with an optional or included chime to sound off inside the home; some can work with a previously installed analog chime using a kit that is part of the camera system or sold separately.

A doorbell cam *also* lets you pretend to be home. The person at the door might be able to peer through windows, but they know they're being recorded when you say, "Hey, what's up?", even if they don't think you're really nearby.

Alarms, Lights, and Smart Stuff

A few security cameras integrate with or are part of smart-home and alarm systems. That means you can have one interface that lets you incorporate a siren, floodlights, non-camera-based motion detectors, glass-break sensors, smart switches and bulbs, and smoke detection, as well as calling a monitoring service (**Figure 24**).



Figure 24: Ring's Floodlight Cam combines security lights and a camera for a startling effect.

This is still an emerging category, which makes me wary about recommending it. Most are also associated with extremely large companies that you might not want to provide additional information to or access to your home, like Amazon (Ring), Google (Nest Secure), and ADT (the home security monitoring company).

For now, I suggest picking the right set of products for the right job, even if it means having two separate systems. This is absolutely required if you're fine with certain aspects of your home being remotely accessible and monitored while you want all video to be stored locally only. The smart-home/home-security ecosystems all rely on cloud-based storage of video.

Be Alert!

Video is obviously the key aspect of a home security camera. But alerts are a close second! Without a system of alerts that you specify and moderate to get just what you need, when you need it, your camera has little value as a security tool.

Now, you may be recording for later review and relying on scanning through motion-triggered events or watching a system-generated summary—some systems are limited to just that kind of recording, too. But even then, I can't imagine that you wouldn't have certain kinds of events that would rise to a level of immediate texting, push notification, or email.

Every system offers different kinds, quantities, and intensities of triggers, as well as varying delivery methods of sending you alerts.

I separate the series of events that happens into this sequence:

- A trigger, called on some cameras an "activity"
- An action of some kind, typically recording a video snippet or marking that a trigger happened at a particular point or during a particular period
- An alert, optional, which might be a sound or light on a camera or a message or notification sent by the camera or a local hub to the camera's owner or people with shared access

Let's look at triggers, actions, and alerts, next.

Configure Triggers

Depending on the system, you should have some of the following choices for setting up event triggers:

- **Motion:** Whenever motion is detected, an event is triggered. This is found on nearly every camera. You usually can set a degree of sensitivity so that every flutter of a leaf doesn't set off a recording or alert.
- **Person:** For cameras that have computer-vision (CV) support, as described in Motion Triggers, you can set up triggers that only go off if the device detects a person in frame.
- **Identified person:** In a system that has both CV and facial detection, you may be able to set a trigger whenever someone programmed into the system appears, as well as when an

unknown face comes into view (**Figure 25**). See also Facial Recognition.

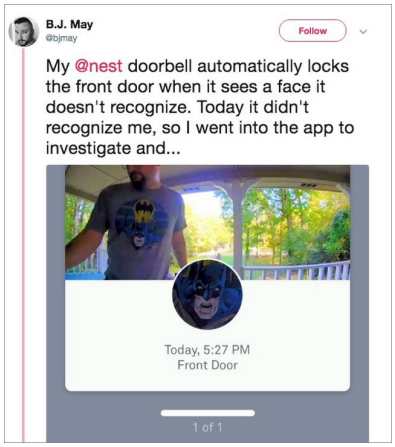


Figure 25: Dun-nuh dun-nuh dun-nuh dun-nuh, Batman!

- **Activity zone:** If you can set up zones of motion, for either passive infrared (PIR) or CV, you can typically have custom triggers based on behavior in a defined area. Zones also may have degrees of sensitivity that each are set with different thresholds. On most cameras, I highly recommend defining zones if the feature is available, and paying extra for a service level that includes zones.

> **Reducing Notifications through Zones**
>
> Our front-facing camera sweeps in 180°, which includes the heads of people on a sidewalk two levels down from our porch and part of a nearby busy street. If I hadn't marked activity zones, I'd receive notifications every few minutes—or continuously.

- **Doorbell:** Standalone doorbell cams or ones that are available as part of a set of compatible devices have a button that someone can press in addition to any motion or person triggers.
- **Audio:** Some cameras can monitor for odd or loud sounds—or any sound above a threshold, such as the Wyze Cam V2.
- **Alarm:** A few cameras, including several Arlo models, can recognize smoke and carbon monoxide detector alarms. That's a fascinating analog bridge if you're using traditional standalone detectors or even a separate smart system.

> **How Detector Alarms Get Detected**
>
> I never knew before researching this book that detectors that produce alarms often rely on standardized signals to allow them to be both easily recognized and differentiated by human beings—but it helps algorithms, too.
>
> The Temporal-Three (T3) signal is three long beeps and a pause, and is used by smoke detectors. The T4, four beeps and a pause, is what carbon-monoxide detectors use as their fingerprint.

Arlo and Wyze offer models that support recognition. Arlo advises reading detector manuals to see if they conform to T3 and T4 standards, and also running a test of the alarm sound to see if the camera can pick it up from the location at which it's placed.

Apple Offers a Glimpse of Recognition Future

It only serves to reason that common, recognizable, and repetitive sounds are susceptible to machine-learning training. Starting in iOS 14 and iPadOS, you can allow an iPhone or iPad to identify environmental sounds. In version 14, the included alarms, a knock at the door, a dog or cat, a baby crying, shouting, and much more. Version 15 added a boiling kettle and breaking glass.

It's easy to see how such recognition could enhance a home-security camera, even without a full-blown home alarm system. Apple hasn't rolled this recognition out to HomeKit Secure Video, likely because it requires onboard neural processing, something found in its custom phone, tablet, and computer chips. But it's only a matter of time!

That's already a lot of triggers, but there are a few others that are more like *meta* triggers: they have to do with the state of the camera, rather than something the camera sees or hears. This includes:

- **Camera offline:** Cloud-based systems know when your systems are online or off, and can send a push notification or other message when they detect a camera or cameras can't be reached. Because these messages are sent from a central system and use an app or SMS, they can work even if your home broadband is offline.
- **Signal from another device:** In some ecosystems, like Nest, the system can trigger a camera to start recording because something bad or important has happened elsewhere among linked sensors. For instance, if a Nest Secure alarm goes off—a door is opened with the alarm set—it will start recording as long as the "emergency clip" setting is turned on.
- **Device removed:** If a camera is deleted from an account, some systems alert you about that as an extra level of protection.

Actions Respond to Triggers

Triggers may be set to carry out a variety of actions. A trigger might cause a camera or system to log an event in a text file, capture a still image, record audio, capture a 12-to-90–second video sequence with sound (depending on the device, free or paid service plan, and settings), or cause a notification to be sent.

Some systems may allow just two of the above—recording audio and video and sending a notification are *de rigueur*—but others allow all of the above.

This can all sound overwhelming! If you have cameras that support all the triggers and responses, won't you be overwhelmed with alerts? That's where tuning responses comes in. You may typically want to have a camera record many video clips for review, but the threshold at which you want to be notified is far higher.

Receive Alerts

An alert is some form of communication that lets you know a thing happened. Alerts can range by system and configuration from a single bit of text that offers a limited amount of information about what happened to a snapshot attached to a message that lets you preview what triggered the system (**Figure 26**).

Cameras and camera systems have all sorts of ways to let you know you should pay attention to something that happened:

- **Push notifications (mobile):** Because cameras are nearly always paired with apps—I don't know of any that aren't—the easiest way for a camera to alert you is by using a push notification. When setting up the app, you must opt in to notifications and can configure how and where they appear, including when your phone is locked and often even when you're in a do-not-disturb mode.

- **Email:** After mobile push notifications, email is the second-most-common way to send alerts. Some cameras can directly connect with any mail system, but require your email credentials to work. I'm not a big fan of this. More sophisticated cameras and manufacturers have you authorize access through existing systems, such as with Google to send messages via Gmail.

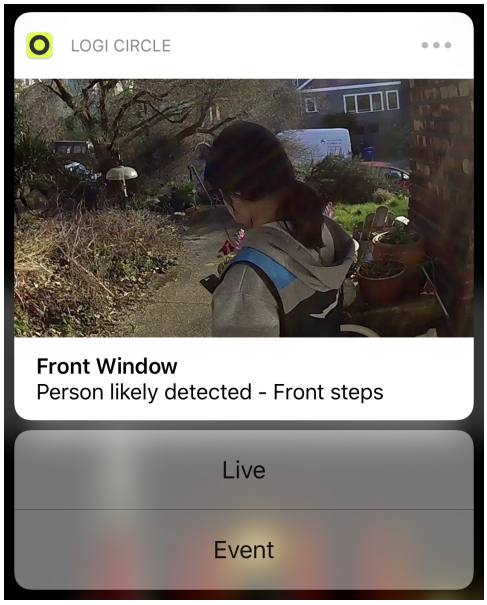


Figure 26: The Logitech Circle alert shows a still image in an alert if the appropriate trigger goes off.

> **Note:** If you use two-factor authentication, such as with Apple ID/iCloud or Google accounts, you will have to create an app-specific password to provide login information for a system that connects directly. Read more about app-specific passwords in Joe Kissell's *Take Control of Your Passwords*.

- **Text messages (SMS):** Strangely, SMS is an uncommon option among home security cameras and systems. For standalone cameras, it would be a hassle for manufacture to set up a system. But with centralized networks, it wouldn't be that big a deal or that expensive (or they could charge an extra fee for it). But because of the abundant ability of push notifications, text messaging is rarely available.

> **An Alert Usually Requires an Internet Connection**
>
> Alerts typically require an active internet connection, even if the alert is being sent to a device in the same house on the same Wi-Fi network. Some cameras may be able to trigger a local network message, but most talk to a cloud-based server.
>
> Some alarm systems that include or allow cameras may offer a cellular-network backup option in case your broadband connection drops. That includes systems like Google Nest, which offers a cell backup where alarm messages can still get out—but not video. There are cameras that include cellular modems as their only method of connection, not for backup. See Cellular Is an Option, Too.
>
> However, I'm not aware of camera-only systems that include a cellular backup option.
>
> The growth of 4G and introduction of 5G networks may make it feasible to have an affordable *failover* link, like a mobile hotspot, which would automatically shift from your internet connection to a cellular data one without being horribly unaffordable and be high speed enough to provide motion-triggered video clips.

Alerts can be modified by other parameters, too:

- **Status:** Some systems monitor your *presence*, or where you are and on what devices. They can figure out if you or any family member is home and disable certain alerts, sometimes by determining that an associated smartphone is in the home. Others let you set a home and away status, like arming an alarm system.

- **Facial recognition:** On systems that can recognize people by their face, you can often enable or disable notifications based on whether the person is recognized. You might want to know when a kid arrives home if you're not there, or if an unknown person is at the stoop, probably delivering a package or the mail. See also Facial Recognition.

- **Geofencing:** Arlo offers a more specific presence option for several of its camera models, called *geofencing*. Geofencing refers to using global coordinates to identify when a device

has entered or left an area. Arlo lets you enroll your own and family smartphones, as well as those of friends, to switch the system between a more active “away” mode and a less-responsive “home” mode.

- **Schedule:** You may want to set a time of day and day of week schedule that turns only some triggers in a certain range into alerts. On systems that this support this, it may be an active setting (send only during these hours or on this schedule) or an inactive one (don’t send alerts during these periods).

Secure Your System

It does you little good to install a system that tries to protect yourself, your home, and your family if an outsider can easily break in—whether while parked outside or from 10,000 miles away.

The default security of a system out of the box varies incredibly among manufacturers, making it critical that you follow your own security protocol in setting up new accounts and devices.

In this chapter, I explain the risks you face, how to secure your device with good general account and password hygiene, and how to keep your devices safe on the internet and up to date. I conclude with what is necessary to share access to your cameras and stored video safely.

You Face Real Risk

One reason to take this so seriously is that criminals and trolls are constantly scanning the entire internet—yes, really, the entire internet—to find devices that are improperly secured or that let them test endless combinations of things to break in. If you have an improperly secured directly connected internet device or a poorly secured online account, you almost certainly *will* be compromised.

This is no academic exercise. Back in early 2020, several news outlets reported on crackers gaining access to Ring accounts, going so far as to create podcasts in which they pranked Ring owners. In one case, someone started yelling at an 8-year-old girl from the camera.

Even though Ring cameras are new and frequently updated, the biggest problem is from outdated gear.

Avoid Earlier Generations of Cameras

Not very long ago, most affordable home security cameras had very few of the features we now look for in such a device. They were really webcams, designed for videoconferencing and recording at one's desk, and some were repurposed with features that made them more generally useful.

They lacked robust triggering, had low resolution, had a small field of view, and didn't have options to stream to cloud storage or come with storage plans.

Most importantly, they weren't well secured against internet-based attacks. Manufacturers used inexpensive embedded operating systems that were quite similar to that used for home network routers, and lightly customized them, but didn't harden them against attack.

Those are the cameras you typically see on the kind of site I just mentioned above. I would not purchase nor can I recommend any of these older models, which are still readily available—often very cheaply. Generally avoid camera models released in 2018 or earlier; specifically, search on any model and "hacked" if you're looking at any older system or one that isn't optimized with high-quality versions of features described in this book.

> **Tip:** I noted earlier in the section Pick a Brand Name? that you should lean towards equipment make by major manufacturers. However, that's not good advice in bypassing the risk of older gear, because some of the biggest electronics makers, like Linksys and Foscom, had vulnerable products.

Can You Trust Any Camera Maker?

I'd be remiss if I moved on without noting the frequent coverage in technical and mainstream media of hacking of various kinds that allows access to stored data, account information, or live feeds. Back on December 30, 2019, a story appeared about Wyze, a well-liked inexpensive maker of cameras.

Due to an absurdly amateur error by one of its new programmers that wasn't overseen or caught by anyone else at the company, information about 2.4 million of its customers was exposed. While passwords were encrypted, as you read above about password reuse, merely the knowledge of someone's email address can sometimes give crackers access to their accounts unless passwords are immediately reset by the site operator and those old passwords aren't allowed to be used again.

Even worse was the set of design and security failures at Eufy that showed Eufy was making misleading statements about encryption and privacy (that the company then removed from their site without fully addressing), and that they had the potential to expose unencrypted video streams accessible just by knowing a URL. (I removed Eufy from this update of the book as a consequence.)

There is no way to know or predict which camera maker won't manage your data well. And companies may have taken every proper precaution, but a flaw in widely used software lets crackers in without any fault by the manufacturer whatsoever. It's always a risk we take when we store data outside devices under our control or allow companies to maintain account information about us.

Set Up an Account or Device Password

Any camera or camera system you acquire will have at least one layer of account or password to access the equipment. For remote-based systems, you likely create an account at a website, and then access it via some combination of web app, desktop app, and mobile app—web and mobile are most common.

Pick a Strong Password

Never leave any default passwords in place for your devices, and no password you set should be very simple, even if the system allows it. User `admin` and password `admin` can be easily cracked automatically on an internet-connected camera, while `glenn@foo.com` with a password of `glenn` is also potentially subject to automated cracking.

In addition to any online accounts, individual cameras or locally configured video systems may also allow or require device passwords. As with the administrative accounts, set those up uniquely and strongly, changing all defaults.

In every case, choose a strong password that's easy to enter and that you can keep a simple record of. Preferably, use password-management software discussed in the next section to avoid having to wrangle that yourself.

If you must come up with a password manually, keep in mind that a strong password doesn't have to be a set of mixed numbers and punctuation, no matter what the sites say. Those are fine, and may be required by hardware, sites, or services that only give you 8 to 12 characters, say.

But a long password that contains randomly selected words, not phrases from poems or books, works just as well. These can be memorable and are always far easier to type on a keyboard or tap on glass. They are no less strong than a short burst of gobbledygook.

The password `hiccup-flubber-muskrat` is even stronger than `2J99!$kjOp5`, for instance.

> **Note:** It's unlikely you need to memorize a password, but if you think there's a case in which you wouldn't have a mobile device or laptop and need to reach your account to retrieve video, memorization of a password should be one of your considerations.

Don't Reuse Passwords

Unwanted account access most often arises not from crackers gaining access to an underlying system, which lets them sniff everyone's cameras, network traffic, transactions, or whatever the currency of a site is.

Rather, in most cases crackers rely on one of two approaches:

- Stealing an account database from a service that hasn't engaged in best encryption practices and isn't aware their users' passwords were exfiltrated. Shorter and easy-to-guess passwords—huge lists of such things exist—encrypted using technology still common just a few years ago, and still widely in use, can be rapidly decrypted.

- Trying combinations at other sites of emails and passwords already stolen and cracked from earlier break-ins and posted or sold online.

The latter is increasingly common as sites improve security, including the techniques to prevent easy or mass cracking of passwords even if an entire database is stolen. The site Have I Been Pwned? lists 9.3 billion accounts whose entries have been posted publicly or otherwise extracted, even if the passwords remain encrypted.

The way to avoid this sort of cracking of your account is to use a unique password at every site, and change all existing duplicate passwords at site you now use. I recommend 1Password for this task, as it works across several platforms, is quite affordable, and lets you create, manage, and fill in passwords in apps and at web site.

Tip: Joe Kissell wrote a whole book about the 1Password ecosystem—*Take Control of 1Password*—as well as a more general book about password management, *Take Control of Your Passwords*.

Enable Two-Factor Authentication

The rise of passwords theft has been paced by availability of a tool once cumbersome and used largely in corporations: multi-factor authentication. Each factor is a separate element and two (and sometimes more) are required to log in to an account or gain access to hardware.

The rubric is something you know, something you have, and something you are—that is usually a password, a device, and a fingerprint or facial scan (biometric).

Many internet-based accounts and some device-based ones rely on a password that you enter, followed by a six-digit numeric code sent to a device or retrieved from an app. The login requires both. Possession of the code "proves" possession of the device. This is known generically as *two-factor authentication* and often abbreviated 2FA.

Phone Numbers Can Be Hijacked

While it seems like phone numbers are an intrinsic part of a phone, they are not. Rather, a phone number is associated by a cell carrier to a unique identifier in the module—usually a Subscriber Identity Module or SIM.

Change the association, and the phone number rings elsewhere. It's not trivial, but it's not very difficult to use social engineering (i.e., lying in a convincing manner) or even bribery to get a cell company support person to make a change to someone else's account.

The industry is slowly moving away from phone number-based factors such as codes sent via SMS as a result, partly because some sites send a password reset link to the same phone number as is used for 2FA. Obtain the number, and no password is needed: force a reset, get the link, reset the password, use the phone to validate.

The notion is that 2FA prevents a wholesale attack: a mass theft of passwords for accounts protected by 2FA can't lead to a mass break-in those accounts. Instead, it forces attacks to be "retail," or one at a time: each password theft has to be paired with a second-factor theft.

Only some camera makers offer or require 2FA; turn it on wherever possible:

- **Apple:** Apple ID accounts used with Apple devices almost all have 2FA enabled, though it's not strictly required for HomeKit Secure Video—it should be.
- **Arlo:** Arlo has offered it as an option since September 2019.
- **Blink:** Blink began requiring all users to use 2FA in mid-2020.
- **Ring:** Ring made 2FA mandatory since January 2020 for new account setups, and offers it for previous account holders.

The easiest way to use it when an option is available other than a texted code (or sometimes an automated voice call speaking the code) is with an authentication app. Several exist, but I recommend the free tier of Authy, which is a secure way to manage second factors and sync them securely across your devices. If you largely use Apple products, you can also opt for Apple's built-in verification code system in iOS, iPadOS, and macOS.

Risk Always Remains

It's impossible without having access to a site's inner workings or without them publishing an independent audit to know how well the company controls account-cracking attempts. Well-designed sites block IP addresses and lock out accounts when too many bad logins are tried or they're tried too quickly.

Unfortunately, all too many sites and a lot of standalone firmware on devices directly connected to the internet have no throttles at all to guard against attacks, making a good password the best defense.

This can make it an advantage to manage your own storage on equipment you control (virtual or real) or using a well-known online storage system, like Amazon S3, which has robust account

security so long as you ensure you don't set up storage to allow public access. (Amazon now has safeguards and alerts against setting this up unintentionally.)

Secure Hardware and Data

The next smartest thing you can do after ensuring that your camera can't be administered by anyone but you, with a strong password you've set, is to make sure that its internal operating system and other software—its *firmware*—is as fresh as possible. You can also work through settings to make sure there are no unlocked doors or partially open windows that someone can force their way through. Finally, you may need to enable encryption or turn it up to the highest level.

Keep Firmware Up To Date

One the greatest risks you face with security cameras is partly outside your control. Those are exploits that can be managed via a company's website or via direct access to internet-connected hardware due to flaws in the camera or account software.

What you can do is make sure that you always have the latest version of the firmware installed. I note this as one of the reasons to pick a brand name over generic, cheaper gear in Pick a Brand Name?.

> **Warning!** If you can't find either a downloadable firmware update within the last six months or a change log that lists all the firmware updates released and pushed automatically to a camera you're considering in recent months, don't buy it.

Here's some steps that are within your control:

- **Register the camera.** While this may unfortunately give the company some permission to market other stuff to you (based on the country you're in and the options on the registration form about receiving marketing materials), it can also make sure that if there's a recall or critical update you'll receive an email.
- **Sign up for security mailings by the maker.** Some companies maintain separate mailing lists in which they post information about security updates for specific gear or all their products. It may mean some unwanted email, but it keeps you up to date.
- **Set a Google Alert for your camera model.** Google offers a free service that monitors news for mentions of keywords. If your camera model (or even camera maker or product line) winds up in the news, that's rarely for good reason—and it may give you a leg up on either taking your camera offline until there's a patch to a flaw or downloading and installing the pass.

- **Install firmware updates as soon as they're available.** Firmware updates can sometimes cause trouble for a small number of customers. But the benefits of patching security outweigh the low possibility of a problem requiring technical support.

Lock Down Settings

It's worth going through literally every setting in your camera and reading the freaking manual, too. Sometimes there are switches that, by default, allow way too much easy access into your devices, whether over the internet or your local network.

Cameras oriented towards simplicity, proprietary cloud storage, and the least possible configuration tend to have the fewest or zero ways to set them up for poor security. They either lack options that could cause problems or, if they have them, the defaults are set sensibly, and require some effort to override.

Cameras that have more options you dig down through, sometimes hundreds of configuration settings, tend towards the potential of less secure defaults out of the box and the potential to more easily make a change that opens up a camera for remote hacking attempts.

For instance, cameras from Google Nest and Ring offer no real method to break security other than to let the wrong people share access to an account (see Share Access below). But Reolink offers a simple page for its highly configurable cameras and NVRs in which you can enter an address and port that your network router or broadband modem can forward to the internet, exposing it (**Figure 27**).

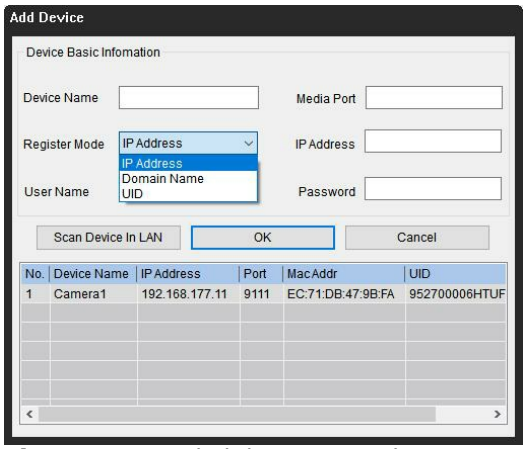


Figure 27: Reolink lets you push your camera through a router for remote access, which is useful but also adds risks.

A Quick Primer on IP Addresses and Ports

Internet protocol (IP) addresses are the way devices are reached via the internet and across local networks. Public addresses are exposed on the public internet and each is equally accessible to attempts to attack services attached to them.

Private addresses work in local networks; most home network rely on private addresses, sharing a single public address, and providing a bit or a full firewall between the internet and a local network. A router bridges private and public addresses, more or less.

IP addresses have the equivalent of numbered cubbyholes, called ports. Low-numbered ports are wired to a fixed set of services, like receiving email, converting domain names to IP addresses, and handling incoming file-transfer commands. Ports from 1024 into the 60,000s can be used for any purpose.

With port forwarding, a router takes a port that offers access on a given private IP address on a local network and maps it to a different port on its public IP address. This limits access from the public internet to just that port but it also makes it accessible for cracking attempts.

Devices get hacked when ports are exposed to the internet and the device's firmware doesn't properly handle unwanted or malicious input.

I recommend disabling all unneeded remote features and reducing the kinds of access to your device. Then you can add access as needed.

Some people may want to add a hardware firewall to their network, or enable one already available in their network router or broadband modem, when they add remotely accessible devices. Even inexpensive and built-in firewalls can be sophisticated enough to block remote addresses temporarily or permanently that attempt to gain access repeatedly using known patterns of abuse.

You can also configure a firewall to disable access to most of the public internet, and only allow incoming connections from, say, a VPN service's range of addresses that you use all the time, your office IP addresses, or other limitations that reduce attack surface by random people.

Encrypt Video Transfers, Storage

It used to be that encryption of data passing over a network, whether your own network or the wider internet, was often lacking from networked hardware and services, and when available, was considered optional. The reality of those days is many years past.

Now, encryption is fast and cheap. Standalone hardware often includes either fast-enough processors or specialized circuitry to speed encryption. (That's true of all modern mobile and desktop computers.)

There are two states of data you need to consider: the kind moving around and the kind sitting on a hard drive, flash card, or SSD. Then there's the degree of access to the encryption keys that affects data both in storage and at rest.

Encrypt Data in Transit

Data in transit encompasses all bits that pass within a home network's Wi-Fi or Ethernet routers and switches, and from a home network to cloud storage. Data in transit should *always* use at least basic encryption to protect video and other data from being snooped on. Home security cameras typically employ layers of encryption.

Require a Base layer of Transport Encryption

Cameras almost always rely at least on TLS (Transport Layer Security), a standard for web-based encryption used with HTTPS connections in browsers. It's used more broadly for many services, including email and streaming video.

Some cameras, like those from Ring, stream video using SRTP (Secure Real-time Tunneling Protocol), an encrypted form of the RTP video-streaming protocol. It uses a quite similar method to TLS to wrap the video in encryption. Such cameras use HTTPS for other kinds of server interaction.

With a camera with well-designed security, any connection you make over the local network directly to the camera uses HTTPS and any connection between the camera and cloud storage also uses HTTPS or a combination of SRTP and HTTPS.

> **Tip:** Some cameras store only clips or footage in the cloud, so you connect to the camera only for live video; all video you play back is retrieved over the internet.

I did think that any camera released in the last several years would always enable HTTPS, SRTP, or other secure data transit by default. But in my research, I'm no longer certain that's true, nor is it necessarily straightforward to find that out.

To determine whether a camera sends only encrypted data or can be configured to do so:

- Check online support files or product sheets for details. You can typically use a search engine to find *camera name* plus *encryption* and see deep results from the maker's site.
- Find the manual or download it and read through whether data-transit security is mentioned.
- If you already have a camera, open its configuration settings and see if there are options to make transmission more secure.

Nest, for instance, makes it hard to find out what standards and practices the company uses for data in transit. With some searching (ironically via Google), I finally found a page that described the policy succinctly and with good detail: "…when you stream your camera video feed to your mobile phone, we protect this data with multiple layers of security, such as HTTPS and

Transport Layer Security, while the data moves between your mobile phone, your products (like your Nest Cam), and our cloud services."

Rely on Higher Security in Transit with a Digital Certificate

The only trouble with HTTPS and SRTP is that it relies on global internet architecture to ensure a secure server at a given domain is the one a camera expects. That makes sense when you're using a web browser to visit arbitrary websites you may visit only once in your life. Creating a more complicated security relationship makes no sense.

But with cameras that store data in the cloud, they typically connect only to a limited set of servers operated by the camera maker or, with Apple's HomeKit Secure Video, a trusted partner. (Cameras or systems that let you set your own server destination have other security issues I discuss in Personal Cloud/Internet Storage.)

When a web browser connects with a web server using HTTPS, a negotiation between the two takes place. The server sends a digital certificate, a standardized format for passing an encryption key and other details. The browser validates that the certificate was properly issued for a server at the domain responding using information built into the browser or the operating system on which it's running.

With a security camera using standard HTTPS or SRTP, the same process happens every time, even though the camera is almost always connecting to a single server or a set of predefined servers. This introduces a slight risk of impersonation of the server if a malicious party were to be able to issue a fraudulent but verifiable certificate and hijack a domain.

While this seems improbable, it's been used for targeted attacks in the past, including against Google users. The good news? None have been disclosed for several years, while the infrastructure around digital-certificate issuance and detection of impersonation has stepped up enormously to deter it.

Nonetheless, some camera makers go a step further than standard HTTPS/SRTP and build in a unique digital certificate using an in-house certificate-issuing system. Each camera connects only to a server that it can verify against information built into it, and servers only accept connections from devices that can prove their identity.

This includes Wyze, which notes in FAQ, "Each camera has its own secret key and certificate so that we can validate its identity during handshake."

Encrypt Data End-to-End in Transit

Yet another layer involves device-based encryption that only encrypts and decrypts video on devices under your control, storing it in the cloud only in encrypted form. This sort of encryption

is both another layer of protection in transit and a significant boost at rest. See Encrypting with End-to-End Protection just below.

Encrypt Data at Rest

Depending on the kind of storage you use, there more or should be additional encryption:

- **Proprietary cloud:** Data at rest on company servers should be encrypted. The company that runs the cloud retains the key, and should have policies in place preventing easy access by all but a limited set of employees to decrypt customer video. You may be able to find this information on a website or in a manual. For instance, Arlo says, "Recordings are encrypted with the user name and password you that create."

- **Personal cloud/internet storage:** Some cloud-storage providers automatically encrypt data that at rest, just as in a proprietary cloud, and maintain their own encryption keys for it. Others provide no basic encryption, but some let you layer encryption on top by providing your own encryption key. Amazon, for instance, offers default encryption for its Secure Storage Service (S3) private storage (called buckets), but you need a camera that works with Amazon S3 and can provide the key. You should be able to find this information on the website or in a product manual. (This is effectively end-to-end encryption, described next.)

- **NVR or other local storage:** Network video recorders continuously accept video, and typically offer no at-rest security. However, depending on the system, it may support a storage drive (internal or external) that, when powered down, is fully encrypted. When powered up, a password must be entered and all data is accessible while it's in use. This is typical of how full-disk encryption (FDE) is offered in modern desktop operating systems.

- **Memory card:** These suffer from the same issue as NVRs, even with much less storage. I can't find any camera system that offers an option to set an encryption key to write video for locally encrypted at-rest storage.

Encrypting with End-to-End Protection

A rapidly increasing trend towards data privacy across all messaging systems, and data transfer and storage, is end-to-end encryption (E2EE). It has been part of Apple's iMessage from the start and the company uses it for ever more parts of what can be synced via iCloud, like HomeKit Secure Video. E2EE is also the defining characteristic of the Signal messaging system, and was added as a free option to the Zoom videoconferencing service.

With E2EE, only endpoint devices generate and store the encryption keys and other cryptographic elements necessary to encrypt and decrypt data. This happens *before* it's sent over

a local network or over the internet to cloud storage. All decryption happens on individual devices after the data is received via a local or remote connection. The data stored on cloud devices is fully encrypted in a way that no one associated with the camera maker or the cloud-storage operator can access, because they lack the keys—only you possess them.

The setup process typically involves these steps:

- **Account change:** You typically start with your account, accessed through a website or proprietary app, and enable E2EE as an option. That doesn't lessen the security, as it simply engages a mode.
- **Initial phone, tablet, or computer enrollment:** On one of your devices, like a smartphone, you prove your account access, and an app or website generates encryption keys locally, which are only stored locally. This process also creates a sort of package of information that allows subsequent devices to enroll.
- **Camera enrollment:** Each camera has to be added to the E2EE set. This may involve physical access, entering a passphrase, or connecting via Bluetooth or Wi-Fi to prove physical proximity.
- **Subsequent device enrollment:** Further phones, tablets, and computers are added to the existing set by proving possession of a passphrase or password that unlocks the package of encryption information described above. With Apple's system, you're prompted to enter the password for an enrolled iPhone, iPad, or Mac; with Amazon's, you need to know a passphrase you created.

Apple set the standard with its introduction a few years ago of HomeKit Secure Video, an option for manufacturers to build in E2EE into their cameras as the only option or as a mode that can be enabled. I discuss that fully in Use HomeKit to Store Video and Trigger Alerts.

It was relatively easy for Apple to build out this robust system, because it's limited to Apple hardware and requires a HomeKit hub, which is a relay feature available only in Apple hardware. Apple had also already built multiple syncing systems that rely on E2EE, such as iCloud Keychain, which rely on user-controlled devices that hold keys.

Apple Also Offers E2EE for Other HomeKit Cameras

Dozens of cameras support Apple's general HomeKit IP camera framework without including HomeKit Secure Video. All these cameras use a distinct but equally secure E2EE method for streaming live video to iPhones, iPads, Macs, and Apple TVs associated with the main user's iCloud account, plus any household members also authorized. When devices access a camera over the local network, it's a direct connection; when accessed remotely, a HomeKit hub is required to relay the data.

Amazon joined this E2EE trend in January 2021, by upgrading several of their Ring camera models to support it as a configurable option. Ring's E2EE requires mobile enrollment for now, so you have to have an iPhone, iPad, or Android device to use it.

Share Access

Many camera systems let you create a system of users and access, which allows family members, colleagues, or others to view live or recorded video. Managing permissions and accounts is important so that you don't inadvertently provide access to anyone jiggling your internet doorknob or allow too much access for people you want to provide limited insight to.

Every camera and system is different! This goes without saying, but it's particularly the case when it comes to how you can let other people have full or limited access, often up to administrator style access, while you still retain (or sometimes share) control.

> **Sharing Constrained by Bandwidth and CPU**
>
> Bandwidth and device computational power will limit sharing. Depending on whether you're connecting directly to a device or through a cloud-based hub, you may find that anywhere from two to 12 people can stream at the same time.
>
> You may be able to connect directly to a camera or to a hub or NVR that controls the cameras. In those cases, the numbers of simultaneous live or recorded-playback users could be quite limited. It's more likely if you're accessing cloud-based storage and a cloud-connected camera that limits are imposed by the maker but aren't constrained by the device.
>
> Even if the capability for lots of live viewers is available, bandwidth may prevent you from getting the right level of video quality of performance on the device you're using, the network you're on, or the network that the camera is on.

Here's the general sequence of what to do and how it varies:

- **Invite someone:** In nearly every system, you use an in-app or web app invitation system. The other person may have to register an account with the same maker's site first, but that's rarely the case. Most of the time, they receive an email invitation that explains how to create an account or download an app. (This invitation step may come early or late in the sharing process.)

- **Choose which cameras:** For multi-camera systems, you either share each individually, mark which cameras to share, or created a shared set. In others, you may be able to let some people or everyone in a group view live video but not recorded clips.

- **Set permissions:** Many systems let you anoint other people with various abilities. That can vary from "can only view during these hours" or "can view for 24 hours" to "may move a

tilt/pan/zoom camera around" to "can administer the device and change setting, including inviting other people."

Show Me the Matrix

At least one camera maker, YI, lets you bring up a sharing screen in their camera app that shows a QR Code. Someone you want to share with installs the app first, then scans the code from a similar section in their copy of the app.

For me, every sharing system has to come with methods to *revoke* access. Otherwise, you're giving away the store forever. Most systems let you edit active users and remove their access or disable it while leaving their account intact, or modify their permissions.

Protect Privacy

Privacy isn't so much a double-edged sword as a pointy mace without a handle that's very hard to pick up. In the modern era, you have to consider your own privacy and whether you're invading other people's. You also need to think about whether police or government agents will have an interest in what you're recording—live or archived.

In this chapter, I look at these three issues: your privacy, that of others, and the surveillance state and your role in it.

Keep Your Cameras and Video Private

Video is intimate, even when you're fully clothed and reading *Bleak House* on a couch in your living room. It's worse if you have children or other people who live with you who are vulnerable or naïve.

The basis of installing any home security camera system, whether it points outward or inward or both, is that you must be able to control who has access to it and prevent everyone else from viewing it.

> **Note:** At least some camera systems can be set up to stop recording video when they detect you're at home, have a setting that lets you easily turn recording on and off, or have a privacy cover for the lens you can manually engage.

You will have noticed that throughout this book so far, I have emphasized features that let you understand how, where, and how securely your video is accessible, transmitted, and stored. Before we move on, let me summarize what you should demand and configure to ensure the privacy of your cameras and video captured from them:

- **Limit access to the device and account.** This includes:
    - A strong password is required (or at least allowed) for all accounts and direct device access.
    - There is no configuration access to the device or account without knowing the password (and account name, if required).
    - Cameras should reject all unnecessary connections over the internet by default (preferred) or let you enable blocking inbound internet attempts. If you want remote

access, it should be tunneled back to your network or require a specific, limited, secure configuration.

    - Devices that can only send video continuously or as clips to a proprietary service shouldn't allow any inbound access, and they should include a mechanism (typically cryptographically based) to ensure they can't be fooled into streaming video elsewhere.

- **Limit access to the video.** Only authorized parties can view live video or stored video, whether through a direct connection to the camera, a locally based NVR, or cloud storage of any kind.

- **Encryption must always be used.** The surest way for your video to be accessible is by it passing over a local network (even one with a Wi-Fi password) or over the broader internet. Encryption aids privacy by an extraordinarily large degree.

- **All changes to access must be approved.** Some camera makers have changed their privacy rules since their introduction. Each of these changes should be opt-in, and allow you to maintain your previous personal privacy stance.

- **Deleting video.** You should have the ability to know when your stored video is deleted and the right to insist all video is deleted if you cancel an account. Optionally, you may want or be able to purge video manually from a cloud-based or local storage system.

Consider these points in what system you buy, how a company changes its software and options over time, and how you configure hardware you already own.

There's one more subject that I want to call out separately, which is the right for your stored video and remote access to your cameras to be protected by the legal policies and legal counsel of the company that makes your cameras, depending on the features of the camera or a broader system that you use.

Companies can take a variety of stances about how readily they cooperate with law enforcement and government agencies who make a request or demand, or who follow procedures (which vary by country) for a compulsory demand, such as a subpoena in the United States and many other nations.

Respect Other People's Privacy

We can't talk privacy by just focusing on our own. If we install cameras, we're also always potentially infringing on the privacy of others. You should consider how you inform others about your cameras, the placement of them, and how you share video.

Is It Legal to Record Video?

I'm not a lawyer and this book decidedly is *not* legal advice. But I can tell you that the legality of audio and video recording in the United States almost entirely depends on regulations in the state in which you're located.

Generally, states consider it legal to record on private property, both inside and outside, as well as views that include places in which people don't have a general expectation of privacy, such as walking down a city street or standing in their front lawn where anyone can see them from a public street.

And recording for security reasons may be specifically allowed in some states. That means it has to be for personal use, not for broadcast or dissemination. You can grab video from your house pointing at the street, but potentially not post it on YouTube.

> **Posting a Sign May Not Be Enough**
>
> You might consider post a sign that you're recording video. In some jurisdictions and situations, you may be legally or contractually obliged to post a sign. These signs are readily available from home stores and online, and sometimes have a, er, humorous message like: "Smile! You're on camera!"
>
> However, even when a sign fulfills a regulation, it doesn't necessarily get you off the hook for all purposes for which a video (or audio, see below) is intended. You may also require the explicit consent of the other party to be recorded.

However, aiming a camera so that you're recording private areas in someone's house or yard you can see from your vantage point and which are reasonably considered private could be illegal or actionable: you might be subject to criminal charges or a lawsuit.

In those cases, too, even if the recording by itself were somehow legal, it's possible making live streaming access available or posting video could put in jeopardy.

If you're concerned about the particulars of your setup, consult the laws of your municipality, a privacy-rights group, or even a lawyer.

> **Is It Legal To Record Audio?**
>
> U.S. Federal law requires that at least one party in a conversation give consent to recording, including if another party who isn't speaking or part of it is managing the recording. This is true whether audio is recorded by itself or as part of a video recording. This law makes it a federal crime to eavesdrop by recording someone else's conversation in physical or digital spaces.
>
> However, states can layer additional requirements. Some require every party on an audio call consent. In states with single-party consent, creating the recording is enough. With all-party consent, you need to get affirmative consent—a sign likely isn't enough—before proceeding to be fully in compliance. Again, ask a lawyer if you have substantive questions or concerns.

Omit the Private Bits

Amazon seems unique in offering privacy zones that exclude recording in defined areas in many models of Ring and Blink cameras (**Figure 28**).

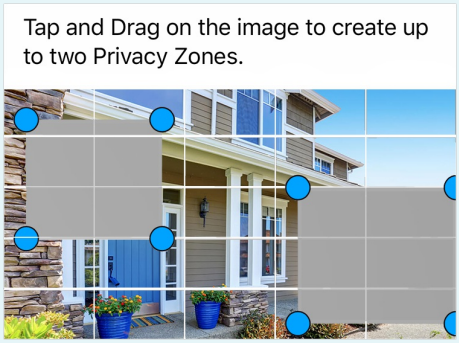


Figure 28: *In Blink's camera setup, you can define areas that are never recorded or transmitted.*

Areas marked as private are blocked in software and not viewable through live access nor uploaded to cloud storage. This seems like a highly desirable feature for other camera makers to add.

Protect Visitors and Hired Help's Privacy

There's typically a dual purpose for interior cameras: to produce an alarm or capture video of someone unwanted in your home, and to monitor contractors, tradespeople, nannies, and babysitters—and sometimes to keep an eye on teens and parents or grandparents.

A trespasser has no per se rights over being recorded on your private property. (See Is Video Admissible in Criminal Cases? for more on how that kind of video can be used.) But other people do have rights.

The main guidelines appear to be whether you are recording video for a reasonable purpose while also protecting reasonable expectations of *indoor* privacy. This includes recording to capture theft or mistreatment of your children, for instance.

For children, they may have no such expectation from parents, even if—by the time they're teens, say—they may find it distasteful.

But for people you invite into your home for social or professional purposes, or whom you hire, like a nanny or contractor, you typically have a legal obligation to honor their privacy. That means no cameras in bathrooms, or in other spaces in which someone is allowed and may close the door for private functions, which could include a bedroom or other space in which they are changing clothes or having a private conversation. If you have live-in help, their private areas would be off limits, too.

This would also be true for parents or others that may have a cognitive decline or impairment. But a camera might be recorded in a bedroom for safety or health purposes, if deemed reasonable, such as ensuring someone didn't fall out of bed.

Protect Renters and Tenants' Privacy

Stories now abound of people checking into an Airbnb room stay, and discovering cameras within the residence. Sometimes, they're obvious and in appropriate places, such as general gathering areas or an entryway. Other times, they are very creepily hidden and in private locations, like a bedroom, bathroom, or WC.

> **No, Really: Creepy**
>
> These hidden cameras aren't hidden in the sense of located discretely out of the way. No, these are intentionally disguised: embedded into USB chargers, tucked into alarm clocks, and even located behind one-way or matte opaque surfaces so they can't be spotted.
>
> A New Zealander described one her family found in April 2019 in a rental house in Ireland: "We just found a camera hidden in a smoke alarm case in the private living room of a listing. The host admitted to the concealed camera over the phone, only after presented with our irrefutable proof."

If you're renting out your space or house, you might already have cameras deployed. Or, you might decide it makes sense to monitor activities—particularly comings and goings—to protect yourself and have evidence if you have a dispute with a renter or tenant.

Some Airbnb and VRBO listings, for instance, state that absolutely no one but the parties listed in the rental may enter the premises.

But the flip side is that people like to expect privacy when they are in a private place, whether it's their home, a tent, a hotel room, or a room for the night.

As noted earlier, this is not legal advice, but I can offer some general insight and ways to find more information.

> **Note:** These guidelines are based on regulations in the United States; some countries have even more stringent rules.

Here's what you should keep in mind as someone who is bringing people into a room in your home or an entire property (like a house or apartment) for anything from a one-night rental to a multi-year lease:

- It's generally legal for you to place cameras facing entrances and exterior spaces and in interior public and common spaces. As a tenant rights lawyer noted on his blog, "The law

favors a property owner's right to record because they have a duty to provide tenants with security. Common areas include laundry or trash rooms, hallways, and shared entryways."

- You generally need to inform a tenant, even an overnight renter, that cameras are in place in public locations. This might be a posted notice or a disclosure along with a rental agreement.
- It's generally illegal to have hidden or undisclosed cameras in places were people expect privacy, such as in a home, apartment, or single room in a boarding house or home-rental property.
- It may be legal to have cameras in some areas of a private home with full disclosure to the tenant or renter, especially if you're renting out a room or floor and not the entire home.
- It's generally illegal to place cameras in bathrooms and bedrooms in private residences, regardless of what portion you're making available to someone else.

To avoid violating someone's privacy and violating the law, check guidelines issued by your municipality (cities usually have tighter rules than states), talk to other landlords or hosts or join a group of them, and—as always—consider consulting an attorney.

Airbnb upgraded its existing rules in 2018 to make disclosures very specific; these currently read:

> …*security measures like security cameras and noise monitoring devices are allowed, as long as they are clearly disclosed in the listing description and don't infringe on another person's privacy.*

When you create a listing on Airbnb, you have to provide information about where each camera is what space it's recording.

Note: Airbnb used to make it clear that guests couldn't record a host or other third-party present, but they have removed that language. Now, I can't find a single mention on the site about that. Airbnb's current rules state more generally "You should not spy on other people," covering both guests and hosts.

Are You Part of the Surveillance State?

In 2020, Gizmodo and other news sources revealed that police routinely gain access, with permission, to Amazon's Ring cameras. That prompted more disclosures from Amazon and others, changes in policies, and a lot of soul searching by people who were concerned about using the police to enforce a "that person doesn't look like they live here" policy.

While homeowners and business owners have often provided video willingly, when a warrant was issued, or under subpoena, it's a different matter when police have the ability to access video without going through an oversight process.

It gets to the heart of whether law enforcement (and national security) should be hyper-vigilant and sweep everyone into constant surveillance, or whether it should be in place to deter crime and other threats, react to it, and use non-discriminatory predictive models scoped to involve the fewest number of false positives.

By owning a camera at all, you may unintentionally add to the surveillance state. But you may want to consider whether or not you voluntarily contribute to it, too.

It might not even be useful. My friend Cyrus Farivar, an NBC News reporter, noted in an article in February 2020:

> *While about a quarter of the law enforcement agencies NBC spoke to said they believed the cameras, discreetly fitted inside internet-connected doorbells, deterred crime, none had data to link the overall drop in property crimes to their deal with Ring.*

Consider Unintended Uses

Video may help lead to solving burglaries, harassment—even murders. But there's always a double-edged sword where privacy and law-enforcement meet.

Consider the rise of genealogical crime fighting. That's the technique of using DNA recovered at a crime scene and matching it in online databases to close relatives based on identifiably shared traits. A number of long-dormant cases in the last two years, some involving murders and sexual assaults, have resulted in arrests and a few convictions. Families and communities can be at ease after sometimes decades of having no leads and no suspect.

But this is the best-case scenario. What if police decide that extending this from murder and rape to vandalism, petty theft, and shoplifting? If DNA testing becomes so simple and databases so huge, a network of relatives could pinpoint the least crime? The amount of investigative work in a murder is huge, and the resources devoted are often large; with minor theft, not so much.

It's a reasonable slippery-slope question to pose. If you install cameras that point outwards, you may capture an alleged crime, and then be part of the process of exposing it. It may put you in danger from someone upset that your video led to consequences for them, or it might place you in relationship to your government in a way you find uncomfortable.

Even if you don't offer the video up, you may be compelled to provide through a perfectly legal process. If you use a cloud-based camera service or even your own remote servers or cloud storage, the provider or host could be forced to give up the video.

You may be able to avoid this complications by ensuring your cameras don't point anywhere off your property, by relying on services or software that automatically dumps video or clips after short periods of time, or by purging video yourself after a period you deem worthwhile to retain it.

Consider Intended Uses

Some of us also live in neighbors in which occasional or regular crimes occur and we want to contribute for our sake or as private citizens to the reduction in such crime.

Ring is the most active on this front. Using the Neighbors by Ring system, you can share video that obscures your exact location with people in the vicinity of your home, which can include law enforcement for the entire region you're in. Law enforcement can also send a request associated with an active investigation to you for clips in a narrowly defined area and time.

Police may also more generally ask for video to help solve a crime or improve the odds of conviction in a variety of ways:

- Posting a request on NextDoor or other social media. Many services invite the police to be regular participants to pass on safety tips, answer questions about individual neighborhoods, or share crime information and statistics.
- Sending an appeal out through media, especially for heinous crimes.
- Knocking on doors. While it might be alarming to have an officer appear on your doorstep, if they are looking for footage around a scene, they may ask you directly and give you information about how to provide it.
- In some locales, police allow people and businesses to register their cameras' locations; this is especially the case in business districts. They can use this to contact owners to ask them to review footage and then go through the correct procedure to obtain it.

Use Smart Home Ecosystems for Control

Many cameras work within an ecosystem of devices, like smart switches, bulbs, sensors, alarms, and more. There are ever more of these systems, some of which are particular to one company and some open to all hardware manufacturers.

These systems typically let you not just control devices individually, such as turning a switch off and on with a tap or viewing the streaming feed from a camera, but also group devices together and schedule them. This can let you create a living room group to turn lights and your A/V system on or off with one virtual switch.

You might also want your furnace to kick in at 5 P.M. if it's below 68° F (20° C), have the front light and front walk's lights turn on, and start music playing. Or you might want a trigger from a camera system to flip on flood lights and play Cher's "Believe" at high volume through exterior speakers. (*"Do you believe in life after love!"*)

There are also ecosystems that allow voice control of cameras and other smart-home items via apps, smart speakers, smartphones, tablets, and computers. This chapter looks at all kinds.

What Kind of Systems Exist

In nearly every case, you have access to a camera's functions via dedicated apps on multiple platforms and a web app. The ecosystem support is typically on top of that. A few manufacturers use a single app for all their devices, whether or not you are controlling them in groups or via timed or triggered actions.

Cameras can be found that also work within several kinds of ecosystems, which break out roughly into three categories:

- **Proprietary company standard:** The company has its own ecosystem, but it's not open to third parties. You can use smartphone/tablet apps and a web app (and sometimes desktop apps) to manage cameras along with all the other devices. In some cases, the company works with a few partners, but most gear that works within the ecosystem is made by the company and there's no general program for other companies' to add their hardware, although other companies' products may be able to control devices that conform to these standards (see One Hub Rules Them All, below). This includes TP-Link Kasa and Lutron

ClearConnect. These systems sometimes involve proprietary networking or wireless standards.

> **Note:** Equipment that works with a company ecosystem often supports some or all of the feature available in a big-company environment.

- **Licensed big-company ecosystem:** Amazon, Apple, and Google each have an ecosystem that supports all the gear they make, but also encourage third parties to make compatible smart-home and other equipment through a licensing and certification program. Apps or interfaces made by each company across multiple platforms, including smart speakers (like the Amazon Echo, Apple HomePod mini, and Google Home), allow controlling devices. Things with screens allow streaming video from camera. Third parties may support one to three ecosystems in the same device.

- **Industry standard for interoperability:** Devices work according to a single standard, and a variety of apps or even company-controlled standards can manage and interact with standards-based devices. Some think the consumer-electronics industry is ultimately headed this way, at least for certain categories. This includes well-known trade standards, like Bluetooth, Wi-Fi, and ZigBee.

> **One Hub Rules Them All**
>
> There's an oddball category that doesn't quite fit the above. That's an agnostic hub designed to work with dozens or hundreds of smart-home devices.
>
> There are two major system like this. The $99 Wink Hub 2 supports smart-home devices, including cameras, from nearly every major manufacturer. It also works with standards like Bluetooth LE, ZigBee, and Z-Wave that have generic profiles for particular kinds of interactions, like audio or sensor reporting.
>
> Samsung's SmartThings is similar, including supporting standards-based wireless devices, and available in multiple versions.
>
> Wink and SmartThings hubs both come with apps, but both also work with Amazon Alexa and Google Assistant for voice control.

Look at Major Ecosystems

Let's take a look at the four big-company ecosystems, what they offer, and how they interact with cameras.

Amazon Alexa

Alexa is Amazon's voice-based home automation system. You speak commands and it carries them out. Amazon and third parties offer what are called *skills* in the system. These are actions

that Alexa knows how to carry out. Amazon offers a variety of hardware devices that include the Alexa system (**Figure 29**).

> **Note:** Ars Technica reported in November 2022 that Amazon was on track to lose $10 billion on the part of the company that includes Alexa, Amazon Prime Video, and some other components. The site said Alexa was the biggest source of losses. This makes it hard right to suggest you purchase Alexa-capable gear until its future is known.



Figure 29: The Amazon Echo Plus is one of many Alexa-supporting devices. (Source: Amazon)

When used with a camera, Alexa requires an Amazon device with a screen, like an Echo Show. You assign a name to each camera that Alexa uses to identify. Then you can say something like, “Show me the most recent event from the driveway” or “show me the front door.”

Apple HomeKit

Apple’s HomeKit is its glue to connect smart-home devices, including cameras. HomeKit allows control via the Home app, available for iOS, iPadOS, and macOS; the Control Center in tvOS; and voice command to any device that has Siri built-in, including Apple’s HomePod (discontinued original HomePod and newer HomePod mini).

Every HomeKit-compatible device has to have some hardware from Apple built in that allows it to communicate with devices and to a central hub I describe next.

Apple also offer a unique storage option for some cameras that let you swap out the camera maker’s proprietary cloud for one that Apple runs. Apple’s system stores video and analyzes for motion-triggered events, but it encrypts and performs analysis locally, keeping your video extremely secure.

> **Tip:** To learn more about using HomeKit, consult *Take Control of Apple Home Automation* by Josh Centers.

Use HomeKit To View and Organize Cameras

You can use the app on devices with a screen or speak commands to Siri on any supported device, like “turn on all lights in the living room.”

However, Siri doesn’t seem to support cameras very well. You can’t seem to tell it to start or stop streaming, engage privacy mode on supported cameras, or—on a device with a screen—get it to bring up the streaming interface in the Home app.

Instead, you use the Home app on supported devices to view live footage from HomeKit-connected cameras (**Figure 30**).

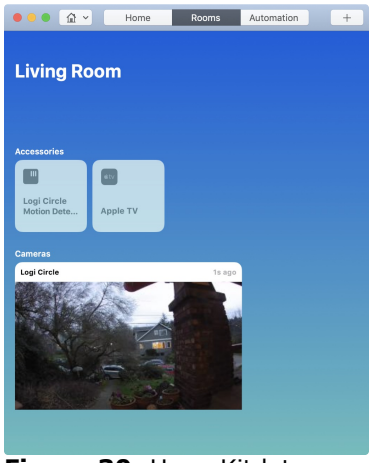


Figure 30: HomeKit lets you see live video from associated home security cameras.

Apple relies on strong end-to-end encryption to stream live video, whether your device with the Home app is on the local network (where it makes a direct camera-to-device connection) or remote.

HomeKit has an option to use a hub, too, but it doesn’t require a special device. Any iPad, HomePod, or Apple TV (3rd generation or later) on the same Wi-Fi network as other HomeKit device acts as the hub. With a hub, HomeKit allows remote access, shared access, and home automation. A hub is required for secure remote access to live video and to use HomeKit Secure Video.

View Video with an Apple TV

Apple TV puts a Home icon in Control Center, letting you bring up something like a Home app, even though Apple doesn’t label these controls as such. To view video in tvOS 13 or later, follow these steps:

1. Using an Apple TV remote, press and hold the TV ▭ button, which will reveal the Control Center at the right-hand side of the screen.

2. Select the Home icon.

3. Select a camera view (**Figure 31**). Navigate right to advance through other camera feeds; navigate left to see a grid overview.

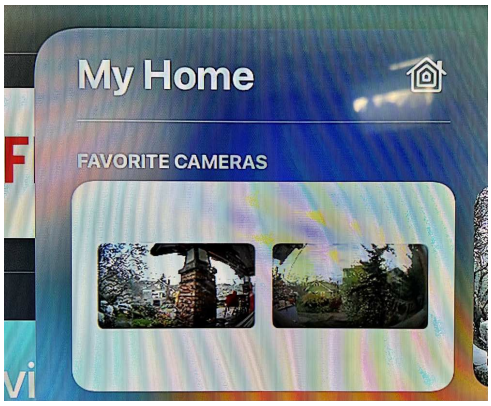


Figure 31: The tvOS Control Center shows live camera views.

4. Select to view an individual feed or the grid overview (**Figure 32**).

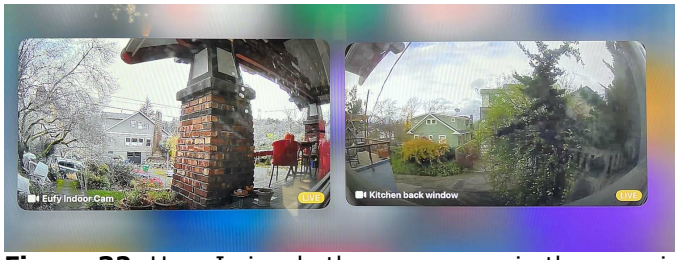


Figure 32: Here I view both my cameras in the overview.

Use HomeKit to Store Video and Trigger Alerts

Apple offers the gold standard for proprietary cloud video storage: HomeKit Secure Video. It has three requirements:

- A camera with HomeKit Secure Video-supporting firmware
- An iCloud+ plan, one of Apple's tiers of paid storage plans with extra services
- A HomeKit hub, as explained above

Apple made this technology available to camera makers to incorporate it into their cameras' firmware. As a result, they give up control of that part of the user experience and, for those who offered paid cloud-storage options, some revenue. Twelve models are available across six manufacturers in January 2023.

Apple has a list of HomeKit-supporting cameras on their site with a subtle • next to those with HomeKit Video Support. Each camera listed links to more information from the manufacturer. No new manufacturers or models have been added in years.

> **Note:** HomeKit Security Video appears limited to line-powered cameras, probably because of the amount of data transfer.

As I note in Proprietary Cloud and Encrypt Video Transfers, Storage, video transferred from your device to a cloud operated by a company that makes the camera should be encrypted in transit and encrypted when it's stored by the company in the cloud. However, that firm typically has all the encryption keys, which is a risk to your privacy from malicious employees, badly run systems, and outside hackers, as well as giving too much ability for unfettered government access to your video.

HomeKit Secure Video relies on an approach similar to how iCloud Keychain exchanges passwords. Each device creates its own encryption keys. Apple never sees these, and all devices linked to your same. See Encrypting with End-to-End Protection for a deeper explanation.

HomeKit Secure Video requires at least iOS 13.2, iPadOS 13.2, or macOS 10.14 Mojave. You can set up cameras with support in the Home app on any of those operating systems.

You also need an iCloud+ plan, which includes different levels of storage and numbers of camera at each paid tier along with features included at all tiers. HomeKit Secure Video storage of 10 days of motion-triggered events doesn't count against your overall data storage, however! Here are the tiers:

- $0.99 per month: one camera, 50 GB of non-camera storage
- $2.99 per month: up to five cameras, 200 GB of non-camera storage
- $9.99 per month: unlimited cameras, 2 TB of non-camera storage

> **Note:** Any iCloud+ paid plan counts, whether you pay for it as an individual account, it's paid as part of a Family Sharing group, or it's bundled with an Apple One subscription.

The camera uses its internal operating system to perform some operations, seemingly including motion triggering events. However, the HomeKit hub also has a role, as the cameras themselves don't (and can't) handle encryption or talk to your Photos library to match faces, if you have that feature enabled. The hub manages all that. Notifications appear on devices linked to your iCloud account; which kinds of notifications varies by the camera (**Figure 33**).

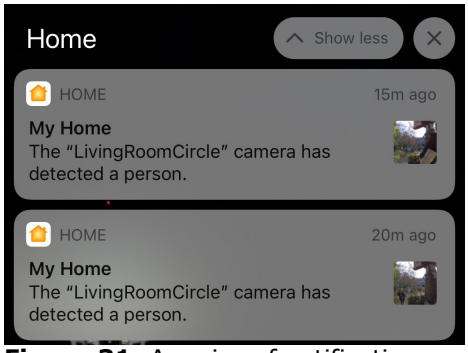


Figure 31: A series of notification comes in as people are detected.

The motion-triggered analysis can look for people, animals, packages, and vehicles (**Figure 34**). A corresponding icon appears on a timeline for each of those categories (**Figure 35**).

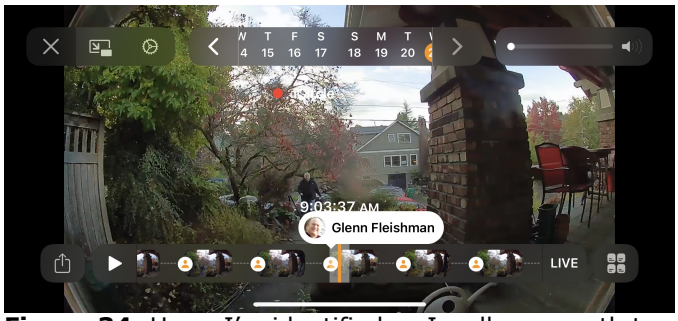


Figure 34: Here, I'm identified as I walk up a path to my house.

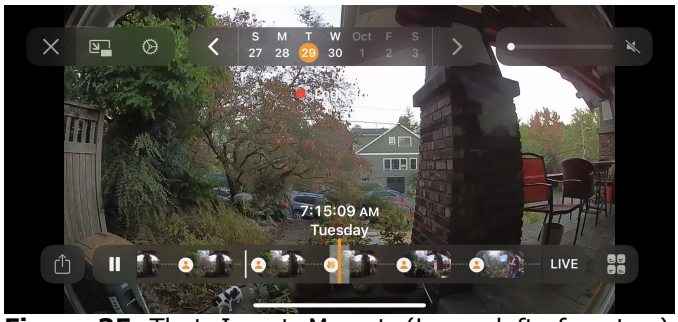


Figure 35: That. Is not. My cat. (Lower left of center.)

People on the same home network can view video streams via the Home app in macOS or via an Apple Watch, but the main Home app user can restrict that.

Facial recognition can be turned on or off, and it can be used just to recognize that faces exist and allow each Home app user to tag faces, or it can be matched against the Photo library of the person managing the HomeKit set of devices. Further, that person can choose whether to let other people on the network see matches against their library.

Google Assistant, Nest, and Home

It’s never simple with Google. Its smart-home and voice-recognition ecosystem has four components, some of which overlap:

- **Google Assistant:** Google Assistant is a widely available voice-recognition and -command system that, like Amazon Alexa, has a huge amount of third-party support through what Google calls “Actions.” Assistant is available through a number of Google devices and via Android.

- **Google Nest:** Nest is the company’s smart-home product line, which includes cameras, doorbell cams, sensors, alarm components, thermostats, and hubs that have a small display; and smart speakers and smart displays, like the Nest Audio and the Nest Hub Max. (Google calls it Google Nest, but all the products start with just the word Nest—no Google.)

- **Google Home:** Google Home is the name for the app they offer for universal control of their hardware. The Google Home app is used to set up and manage Google Nest and Chromecast devices.

> **Note:** Google Home used to refer to smart speaker hardware that included Google Assistant technology. Some older devices still use the name, like the Google Home mini, but newer smart speakers all use Nest in their names.

- **Chromecast:** Chromecast (no Google in the name) is what Google calls their streaming receiver line, which can be built into TV sets or added through a small stick that plugs in to a TV via an HDMI port.

Google loves having lots of different things that are very similar, but which have different names. And things that are *exactly* the same and have different names! And changing names!

To use a Nest or third-party camera with Google’s ecosystem, you use the Google Home app, which consolidates and controls all smart-home devices. You can view camera feeds through the Google Home app, as well as control settings, depending on the camera model.

To use voice control, you can use any Google Assistant-equipped hardware or app that’s associated with your same account, and it will have access to the range of devices you’ve associated.

If you associate a display in your Google Home app setup, you can then use Google Assistant to send video from a camera to it. This can include any Chromecast-enabled display or the Nest Hub or Hub Max.

If you have a doorbell camera, you can say something like, “What’s on *doorbell name*?” and Assistant streams it to your default device. Or you can say regarding any camera, “Show *camera*

name on *display name*.” You can also say, “Stop *display name*” to stop streaming.

About This Book

Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your comments.

Ebook Extras

You can access extras related to this ebook on the web. Once you're on the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy a subsequent edition at a discount.
- Access the book in both PDF and EPUB formats. (Learn about reading on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.
- Find out if we have any update plans for the ebook.

If you bought this ebook from the Take Control website, it has been automatically added to your account, where you can download it in other formats and access any future updates.

More Take Control Books

This is but one of many Take Control titles! We have books that cover a wide range of technology topics, with extra emphasis on the Mac and other Apple products.

You can buy Take Control books from the Take Control online catalog as well as from venues such as Amazon and the Apple Books Store. But it's a better user experience and our authors earn more when you buy directly from us. Just saying…

Our ebooks are available in two formats, PDF and EPUB, which are viewable on any computer, smartphone, tablet, or e-reader. All are DRM-free.

About the Author



Glenn has written oodles of books since the 1990s. Most recently, those include *Take Control of Your M-Series Mac*, *Take Control of Zoom*, *Take Control of iOS & iPadOS Privacy and Security*, and *Six Centuries of Type & Printing*. Glenn writes on topics as varied as the longest-

running metal foundry in America, the unique nature of sheriffs in America, and how syndicated cartoons were distributed to newspapers in the 1920s. (Photo credit: Lynn D. Warner)

Acknowledgments

My wife, Lynn, suggested this title, being both creeped out by security cameras and in-home listening devices (like Alexa and Siri), and wanting to know more about configuring devices to preserve privacy while also providing monitoring and deterrence.

Shameless Plug

In the last few years, I've devoted ever more of my time outside of writing Take Control books and how-to articles to type and printing history. You can find dozens of articles I've written at my Patreon site, where you can become a direct supporter, helping me defer travel and research costs to continue my work. You might also be interested in my book *Six Centuries of Type and Printing*, set in hot-metal type and printed by letterpress in London. It's also available as an ebook.

About the Publisher

alt concepts, publisher of Take Control Books, is operated by Joe Kissell and Morgen Jahnke, who acquired the ebook series from TidBITS Publishing Inc.'s owners, Adam and Tonya Engst, in 2017. Joe brings his decades of experience as author of more than 60 books on tech topics (including many popular Take Control titles) to his role as Publisher. Morgen's professional background is in development work for nonprofit organizations, and she employs those skills as Director of Marketing and Publicity. Joe and Morgen live in Saskatoon, Saskatchewan, Canada, with their two children and their cat.

Credits

- Editor and Publisher: Joe Kissell
- Cover design: Sam Schick of Neversink
- Logo design: Geoff Allen of FUN is OK

Copyright and Fine Print

Take Control of Home Security Cameras
ISBN: 978-1-7780439-6-3
Copyright © 2023, Glenn Fleishman. All rights reserved.

alt concepts, 419 8B-3110 8th St. East, Saskatoon, SK S7H 0W2 Canada

Why Take Control? We designed Take Control electronic books to help readers regain a measure of control in an oftentimes out-of-control universe. With Take Control, we also work to streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

Our books are DRM-free: This ebook doesn't use digital rights management in any way because DRM makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, they should buy a copy. Your support makes it possible for future Take Control ebooks to hit the internet long before you'd find the same information in a printed book. Plus, if you buy the ebook, you're entitled to any free updates that become available.

Remember the trees! You have our permission to make a single print copy of this ebook for personal use, if you must. Please reference this page if a print service refuses to print the ebook for copyright reasons.

Caveat lector: Although the author and alt concepts have made a reasonable effort to ensure the accuracy of the information herein, they assume no responsibility for errors or omissions. The information in this book is distributed "As Is," without warranty of any kind. Neither alt concepts nor the author shall be liable to any person or entity for any special, indirect, incidental, or consequential damages, including without limitation lost revenues or lost profits, that may result (or that are alleged to result) from the use of these materials. In other words, use this information at your own risk.

It's just a name: Many of the designations in this ebook used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no

intention of infringement. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

We aren’t Apple: This title is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc. Because of the nature of this title, it uses terms that are registered trademarks or service marks of Apple Inc. If you’re into that sort of thing, you can view a complete list of Apple Inc.’s registered trademarks and service marks.