TAKE CONTROL OF
HOME SECURITY CAMERAS

by GLENN FLEISHMAN
$14.99

Click here to buy the full 166-page "Take Control of Home Security Cameras" for only $14.99!
# Table of Contents

**Read Me First** ................................................................. 4
  Updates and More ............................................................ 4
  What’s New in Version 1.3 ................................................. 5
  What Was New in Version 1.2 ............................................. 6

**Introduction** .................................................................. 7

**Home Security Cameras Quick Start** ............................. 8

**Which Camera to Buy** ................................................... 10

**Why Do You Want a Camera?** ...................................... 12
  Screen Approved Visitors and Workers ............................. 12
  Ding, Dong! Who’s There? ................................................. 15
  Deter and Report Crime ................................................... 17

**Rough Out Your Layout** ................................................ 21

**Choose Where Video Lives** .......................................... 24
  Where a Camera Stores Your Video ............................... 24
  How To Retrieve Video ................................................... 35
  Pick Your Storage Method .............................................. 38

**Consider Physical Parameters** ..................................... 40
  Pick a Brand Name? ....................................................... 40
  Choose a Network Connection ....................................... 42
  Mull Mounts and Pick Power ......................................... 48
  How Cameras Capture a Scene ..................................... 60
  Pick Camera-Based Features ....................................... 67
  Consider Extras Beyond Video .................................. 76

**Be Alert!** ................................................................. 79
  Configure Triggers ....................................................... 80
  Actions Respond to Triggers ....................................... 82
  Receive Alerts ............................................................ 83
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Your System</td>
<td>87</td>
</tr>
<tr>
<td>You Face Real Risk</td>
<td>87</td>
</tr>
<tr>
<td>Set Up an Account or Device Password</td>
<td>89</td>
</tr>
<tr>
<td>Secure Hardware and Data</td>
<td>93</td>
</tr>
<tr>
<td>Share Access</td>
<td>102</td>
</tr>
<tr>
<td>Protect Privacy</td>
<td>105</td>
</tr>
<tr>
<td>Keep Your Cameras and Video Private</td>
<td>105</td>
</tr>
<tr>
<td>Respect Other People’s Privacy</td>
<td>108</td>
</tr>
<tr>
<td>Are You Part of the Surveillance State?</td>
<td>114</td>
</tr>
<tr>
<td>Use Smart Home Ecosystems for Control</td>
<td>117</td>
</tr>
<tr>
<td>What Kind of Systems Exist</td>
<td>117</td>
</tr>
<tr>
<td>Look at Major Ecosystems</td>
<td>119</td>
</tr>
<tr>
<td>Camera Models</td>
<td>128</td>
</tr>
<tr>
<td>Amazon Blink</td>
<td>128</td>
</tr>
<tr>
<td>Amazon Ring</td>
<td>132</td>
</tr>
<tr>
<td>Canary</td>
<td>136</td>
</tr>
<tr>
<td>D-Link mydlink</td>
<td>138</td>
</tr>
<tr>
<td>Eufy</td>
<td>141</td>
</tr>
<tr>
<td>Eufy: Capture and Storage</td>
<td>142</td>
</tr>
<tr>
<td>Google Nest</td>
<td>144</td>
</tr>
<tr>
<td>Logitech Circle</td>
<td>147</td>
</tr>
<tr>
<td>NETGEAR Arlo</td>
<td>151</td>
</tr>
<tr>
<td>TP-Link Kasa</td>
<td>156</td>
</tr>
<tr>
<td>Wyze</td>
<td>159</td>
</tr>
<tr>
<td>About This Book</td>
<td>163</td>
</tr>
<tr>
<td>Ebook Extras</td>
<td>163</td>
</tr>
<tr>
<td>About the Author</td>
<td>164</td>
</tr>
<tr>
<td>About the Publisher</td>
<td>165</td>
</tr>
<tr>
<td>Copyright and Fine Print</td>
<td>166</td>
</tr>
</tbody>
</table>

Click here to buy the full 166-page “Take Control of Home Security Cameras” for only $14.99!
Welcome to Take Control of Home Security Cameras, version 1.3, published in January 2022 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 © 2022, 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.

• Download various formats, including PDF, EPUB, and Mobipocket. (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 1.3

This version incorporates the latest feature changes to home security cameras and software, and changes to the devices manufacturers make available in their line-ups.

Other changes include:

• **Doorbell cameras:** The section on doorbell cameras, Ding, Dong! Who’s There?, has been revised and expanded. I’ve 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, respectively) 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 to view video:** I’ve added a short section that explains 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.

• **Pandemic changes:** Earlier versions of this book made different assumptions about the behavior people might engage in under the...
pandemic when the form of its transmission was less well understood. The book has been updated to reflect how we live now.

- **Removed centralized camera systems:** In previous versions of this book, I covered camera systems that had a central wired or wireless hub with a network video recorder. In the past, such systems were the only affordable way to install a lot of cameras and record continuous video. “Smart” cameras, the kind covered throughout this book, and the ecosystems that support them, now come in enough variety and low-enough cost to avoid the many tradeoffs of centralized systems.

- **Reduced the scope of camera systems:** In previous editions, we tried to keep abreast of all the changes to pricing, features, and models across about a dozen different major camera systems. That’s proved to be impossible unless we updated the book monthly. Instead, we’ve improved recommendations and links to cameras throughout the book, and slimmed down Camera Models to provide the most useful information that isn’t constantly changing.

---

**What Was New in Version 1.2**

This update expanded coverage of end-to-end encryption (E2EE), which puts control in the hands of users, by storing encryption information only in devices under your control. This protects video as it streams or uploads to the cloud, and while stored in the cloud, from unwanted access. Someone has to both have an enrolled device—like a phone, tablet, or computer—and be able to unlock it to view video.

While Apple has already offered E2EE for its ecosystem via camera manufacturers who support Apple’s HomeKit Secure Video service (see Use HomeKit to Store Video and Trigger Alerts), what’s changed is that Amazon added E2EE support to several models of its Ring cameras.

You can read these new and updated section on end-to-end encryption, Encrypting with End-to-End Protection and Some Cameras Give You the Keys to Privacy, and read up on Amazon’s new options and which cameras are supported in Ring: Privacy.

---

Click here to buy the full 166-page “Take Control of Home Security Cameras” for only $14.99!
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. Otherwise I would have to consistently write “your camera or cameras,” which you would tire of as fast as I would! 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.

• Discover details about major camera systems; see Camera Models.

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

While this entire book provides you the background and information you need to make a smart decision about purchasing one or more home security cameras, some people like to flip to the end of the book for the big reveal, and then go back and find out the plot. For such readers, here are my top recommendations in different categories as of January 2022:

- **Highest-quality single camera with user-controlled encrypted cloud storage (Apple ecosystem only):** The Logitech Circle View ($159.99) offers a good camera with up to 180° field of view that works only with Apple’s HomeKit Secure Video, which offers end-to-end encryption (E2EE) that prevents anyone but you—including Apple—from decrypting your stored video clips or viewing the live stream. iCloud+ subscribers pay no additional fees for cloud storage required to hold the video, and 10 days of clips are retained. Apple devices are required for configuration, notifications, and viewing. Read about Logitech Circle models in Logitech Circle, and about Apple’s video storage system in 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. See Amazon Ring and Ring: Privacy.

- **Best overall security profile for all cameras (local, any platform; cloud, Apple ecosystem only):** Eufy offers several models of indoor-only and indoor/outdoor cameras that can store video on local storage (with strong encryption that locks the video
to the camera system for playback) and can also send video securely to Apple HomeKit Secure Video. See Eufy.

• **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 be 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. See Wyze.
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

Click here to buy the full 166-page “Take Control of Home Security Cameras” for only $14.99!
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).
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...
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?**

While you will hear the term “cloud” quite a lot, it’s rarely defined. I like to think of the cloud as any online storage or system in which I don’t have to manage physical hardware directly or connect to a specific server by name or number.

For cloud storage, that means having 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. You never manage or provision it.

Cloud storage can be proprietary, as described in this section, where a company runs it and it’s entirely a black box to you; or you can find your own, discussed in Personal Cloud/Internet Storage, such as Google Cloud, Amazon S3, or Backblaze B2.

Here are the characteristics of proprietary cloud storage for cameras:

• **Capacity:** It’s a large range, from 24 hours of free storage of motion-triggered clips up to weeks or months of continuous video storage.
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.

Click here to buy the full 166-page “Take Control of Home Security Cameras” for only $14.99!
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.
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!](image)

- **Activity zone:** If you can set up zones of motion, for either passive infrared (PIR) or CV, you can typically have custom triggers based
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 inter-
et—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 knowl-
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.
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, Logitech Harmony, 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.
Camera Models

In this final chapter, I take you through the approaches used by each of several major camera makers’ systems, and apply a standard rubric against each of them that combines elements discussed across the rest of the book.

The rubric is as follows:

- **Models**: What options are available for cameras?
- **Capture and Storage**: Where is video stored, how much can you retain, how do you access it, and what one-time or ongoing costs are involved? Does a camera let you capture only motion-triggered clips, continuous video, or some mix of both?
- **System price**: What does each camera or bundle of cameras cost, as well as an any add-on optional or required hardware?
- **Privacy**: What measures does the maker take to preserve your own privacy and that of others, and do they work with law enforcement to hand over stored video?
- **Platforms and integration**: Which software is required to configure cameras and access the system? Which smart-home systems does it work with, like Amazon Alexa, Apple HomeKit, and Google Home?
- **Bottom line**: Each rundown ends with a summary of for whom the system is useful and in what circumstances it shines.

Amazon Blink

Amazon’s [Blink cameras](#) stand in contrast to the Ring lineup in a few different ways: there are only three models, they don’t cost much, they record brief clips, and two are designed to work using replaceable—but
not rechargeable—lithium metal batteries (see Lithium-Metal Battery Warning) rated for what the company claims is two years of use.

Amazon released its third generation of Blink hardware in September 2020, which built on previous ideas of simplicity, but added a subscription option for cloud storage, while the previous generations included storage at no cost.

**Blink: Models**

Amazon revamped the Blink lineup by releasing a third generation and discontinuing previous versions in September 2020. The three models—Indoor, Outdoor, and Mini—all have a fairly narrow 110° angle of view and record 1080p. All three also have night vision, two-way audio, and motion-triggered alerts, and work with Alexa.

The Blink Indoor and Blink Outdoor are battery-powered and include two lithium metal batteries. You can also add a power pack that will double purported lifespan to four years (Figure 37).

![Figure 37: The Blink Indoor (shown) and Outdoor run for an estimated two years on included, replaceable lithium metal batteries.](image)

The battery-powered models are designed to allow short recordings and not a lot of them without draining all the juice. The estimate listed
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.

• Download various formats, including PDF, EPUB, and Mobipocket. (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 three popular formats: PDF, EPUB, and the Kindle’s Mobipocket. 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

As part of my historical interest in type and printing, I created a project in 2019 called the Tiny Type Museum & Time Capsule. It’s a real, tiny museum full of type and printing artifacts, new and old, in a handmade case, coupled with a letterpress-printed book, *Six Centuries of Type and Printing*, covering the development of printing from Gutenberg to the present (with some background on pre-Gutenberg printing). You can find out more about the museum and obtain your own (eight remain for sale in January 2022) at tinytypemuseum.com.
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

Click here to buy the full 166-page “Take Control of Home Security Cameras” for only $14.99!
Take Control of Home Security Cameras
ISBN: 978-1-7780439-6-3
Copyright © 2022, 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.