July 2021
Vol. XL, No 7

KEYSTONE MacCentral

printout

Keystone MacCentral Macintosh Users Group ❖ www.keystonemac.com

Keystone MacCentral July Program

July 20, 2021 06:30 PM

Join our Zoom Meeting by connecting with link in our email

Please see your membership email for the links to this month's Zoom meeting or email us at KeystoneMacCentral@mac.com.

This month we plan to discuss

- An astronomy app *SkyView Lite*
- iPhone Photography
- An introduction to Pages as a page layout program

We have virtual meetings via Zoom
on the third Tuesday of each month.

Emails will be sent out prior to each meeting. Follow the directions/invitation each month on our email – that is, just click on the link to join our meeting..

Contents

July Program 1

An M1 Mac Can't Boot from an External Drive If Its Internal Drive Is Dead *By Glenn Fleishman* ..... 3 - 5

The Two Faces of Find My *By Adam Engst* ..... 5 - 7

Consumer Desktop Mac Buying Guide: Which Is Right For You? *By Julio Ojeda-Zapata* ..... 7 - 12

13 AirTag Tra20cking Scenarios *By Glenn Fleishman* .....13 - 20

By Glenn Fleishman

An M1 Mac Can't Boot from an External Drive If Its Internal Drive Is Dead

Bombich Software recently updated Carbon Copy Cloner to version 6, and its founder, Mike Bombich, posted a blog entry explaining some of the intricacies involved with updating cloning software for Big Sur and M1-based Macs. One heading may have surprised those who haven't read all the technical details about M1 changes: "An Apple Silicon Mac won't boot if the internal storage has failed."

That might seem bizarre. A core aspect of dealing with system failures on Macs is that you could maintain an external bootable drive, perhaps a bootable duplicate of your startup volume, that lets you use your Mac even if an internal drive was corrupted or failed entirely.

In "The Role of Bootable Duplicates in a Modern Backup Strategy" (23 February 2021), Adam Engst presciently explained why bootable clones might be a thing of the past. Now Mike Bombich has confirmed with Apple that external bootable drives won't always work!

It's true, but it's not as terrible as it sounds. Let me first explain why you should be aware of it but not worry, and then explain the more technical details for those interested in the innards of macOS.

You're Unlikely To Have a Dead Internal SSD and a Live Mac

The fresh information here is that an M1-based Mac relies on its internal SSD to allow external drives to boot. If the internal SSD has failed or been entirely erased—it contains several hidden volumes—you can no longer boot from an otherwise valid volume on an external drive. Why would Apple do this? To increase security. And, maybe, to reduce its tech support costs.

Relying on details stored only on the internal SSD to control startup from external drives is a way to make it harder for nefarious parties to hijack a Mac's data. This approach is a shift from Intel-based Macs, which relied instead on firmware (software stored in programmable memory chips that can be updated). However, firmware updates can sometimes fail, causing temporary problems with a Mac or even "bricking" it. There may also be attack vectors related to firmware-based startup control that Apple hasn't disclosed.

On an Intel-based Mac, you can set a firmware password that prevents booting from anything but a "designated startup disk." Apple didn't include that feature with M1-based Macs because the company changed the startup and recovery processes to require knowing a password associated with the selected startup volume. An Apple support document notes: "a Mac with Apple silicon also won't require (or support) a firmware password—all critical changes are already gated by user authorization." If you don't have a valid account and password, you can't change the startup volume or perform most other recovery features.

We don't know to what degree problems with firmware updates or undocumented attack vectors contributed to Apple's switch. Perhaps it was just a simple architecture change, given the reliability of SSDs and the ease of updating them to shift aspects of security from programmable memory chips to SSD storage? You might intuit that Apple could have had high ongoing costs of technical support related to firmware update failures *and* knew of exploits that compromise data on a Mac's internal drive by starting up from an external drive. Maybe the cost of diagnosis and repair for Macs disabled or bricked due to firmware failures was high enough to be a consideration, too. But we don't know.

However, here are the reasons we're not too concerned about this change:

- A large majority of people don't possess a bootable external drive compatible with M1-based Macs and would never create a bootable backup. (We cognoscenti may love booting from external drives, but it's not a mainstream thing to do.)
- Modern SSDs are extremely reliable. The vast majority of people with Apple silicon Macs will never experience a failure of their internal SSD. Thus, they will never encounter a situation where they can't boot from an external drive due to an internal drive failure. Look no further than iPhones and iPads for evidence of this fact.
- Should the internal boot volume become corrupted, or the firmware in the Secure Enclave develop issues, Apple provides a range of recovery options, including recoveryOS with macOS Recovery (a separate bootable partition), fallback recoveryOS (another partition), and revive/restore via Apple Configurator via another Mac, as I explain in the next section.

Put another way, the only time you would encounter this problem is *if* you had set up a bootable external drive *and* your M1 Mac's internal drive became so damaged (at a hardware level, likely) that you would need an entire motherboard replacement.

What's going on at a relatively low level of macOS that makes this possible—even necessary? The nitty-gritty follows.

Apple Silicon Puts Security Policies on the SSD

I learned about this limitation while researching my book *Take Control of Your M-Series Mac*, during which I dug into the Apple Platform Security guide, which was published in February 2021 (and updated this month). Plus, I had read Howard Oakley's article "M1 Macs radically change boot and recovery," which interpreted some of the obscure aspects of new boot policy for M1-based Macs. Howard and I apparently alerted Mike Bombich to this in a Twitter thread—it's such a new idea, even he took some convincing!

As Howard notes in his article, Apple introduced the notion of the 1 True Recovery (1TR) partition with M1-based Macs. This additional partition, separate from a Big Sur startup volume group, holds the code and data that controls boot-time behavior. On Intel-based Macs, firmware serves this role.

One way 1TR differs from the firmware on Intel-based Macs is that the 1TR partition stores your decisions about startup security *policies*, the directives you set in the Startup Security Utility available in recoveryOS. You can set a separate policy for each external volume you allow to boot your Mac, but that policy is stored *only* on the internal drive in the 1TR partition. This technique prevents manipulation and trickery if you opt to vary from the highest level of security available, which is the default mode.

This reliance on 1TR is also why setting up an external bootable volume on an M1-based Mac sends you through a two-step process the first time you boot from it. After you select a volume on the external drive in the Startup Disk preference pane or through the recoveryOS startup process, your Mac restarts and makes you authenticate again. From then on, you can restart directly from that external volume. Because it only happens the first time, people often think it's an error rather than an intentional process. Here's what's happening.

The first step in recoveryOS invokes user authentication to validate the new security policy that will allow that volume to start up the Mac, which it *then writes* to the 1TR partition. But because the policy hasn't yet been *read* from the 1TR partition (which is necessary to know that it's valid), a second restart happens so that 1TR can read that policy during the boot process and validate that the external volume can be used as the system startup volume.

You can encounter trouble if you erase the internal SSD. If you erase all the partitions, including 1TR, you won't be able to boot from an external drive. However, if you haven't erased all the partitions, you can reinstall macOS in one of two ways:

- **Use recoveryOS:** Shut down your Mac. Then press the power button for 10 seconds and release it only after the startup options window appears. Click Options, authenticate, and reinstall macOS. If that fails…
- **Use fallback recoveryOS:** Apple added a second recovery partition to macOS for M1-based Macs in case something happens to the main recoveryOS partition. Fallback recoveryOS should start up automatically when the main recoveryOS fails. But you can also trigger it manually: Shut down your Mac. Instead of pressing and holding the power button, press the power button twice in succession, holding it down the second time for 10 seconds until the startup options window appears. With fallback recoveryOS, volume policies aren't loaded. However, it does let you reinstall macOS, and it silently repairs the main recoveryOS. After reinstalling macOS, you can restart and get back to normal. (In fact, if the main recoveryOS has failed, Apple promotes the fallback recoveryOS to become the main recoveryOS and installs a new fallback recoveryOS in its place. If your head is spinning, join the club.)

If recoveryOS can't be used, you have to use the revive or restore firmware processes, which require the free Apple Configurator app, a particular cable depending on which M1-based Mac you have, and a second Mac. Apple describes the process in extreme depth. The firmware involved here is the Secure Enclave Process's operating system (sepOS), which manages what Apple calls the Secure Boot process, involving elements described above. (You've probably never heard of sepOS before, but it's a thing.)

If the revive or restore process fails, that's likely an indication of a significant hardware failure. Your Mac will need to be serviced, and Apple might replace either the motherboard or the entire computer.

By Adam Engst

The Two Faces of Find My

In the conversation that followed Glenn Fleishman's "13 AirTag Tracking Scenarios" (15 May 2021), it became clear that Apple's terminology choices and user interface design have engendered confusion over precisely what constitutes "Find My." To wit: Find My is *two* services packaged into one and named almost identically. It's worth understanding the difference between these distinct, intertwined Find My services because an individual user—much like one of Glenn's fictional characters—might not want to participate in the global crowdsourced Find My network for philosophical reasons.

(We're not going to get into that question here. Suffice it to say that, as far as we can tell, the Find My network protects your privacy well; there are no concerns about it revealing anything about you to anyone else. But if you don't wish to be a part of the Find My network such that your devices can help other people find their lost items, that's your business.)

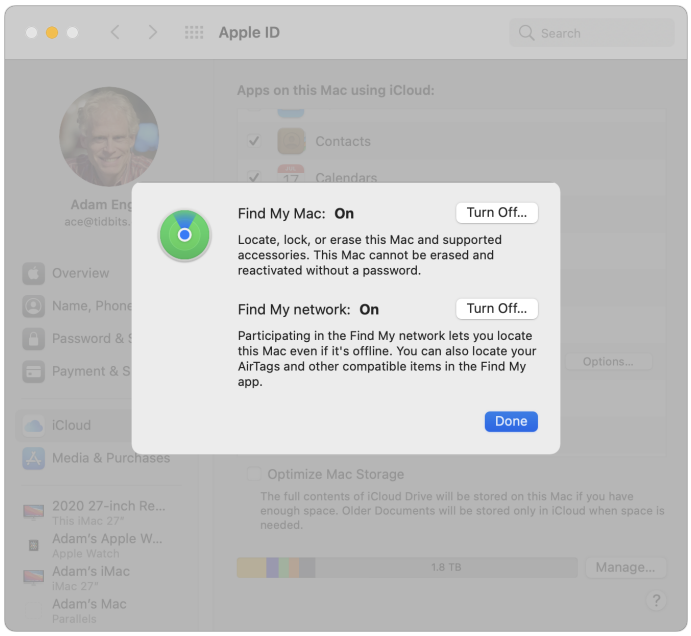
The key is to realize is that there are two distinct aspects to Find My:

- **Find My *device* (Internet):** If you lose one of your Apple devices, having Find My turned on for that device lets you locate, lock, and erase it, as long as it can access the Internet. You can use the Find My app in iOS, iPadOS, or macOS, or via iCloud.com. Find My *device* is bi-directional: your device can report its location, and you can send it those commands. In addition, turning on Find My

iPhone enables Activation Lock, which prevents anyone from erasing and reactivating the device without your Apple ID password. The only reason not to turn on Find My *device* is if you're working with a test device that you reset frequently. (Been there, done that—see "Extracting Data from an Old iOS App Broken by iOS 14.5," 20 May 2021.) Find My *device* works with the iPhone, iPad, iPod touch, Apple Watch, and Mac.

- **Find My network (crowdsourced):** Devices using Find My *device* rely on connecting with Apple's servers over the Internet. In contrast, devices that use the Find My network don't need a direct Internet connection. Instead, they broadcast Bluetooth signals, like a lost cat meowing in the dark, without knowing if the signals are heard—it's a one-way transfer of information. If any iPhone, iPad, or Mac is nearby, running a recent-enough version of its operating system and connected to the Internet, it can pick up and relay the Bluetooth information, pairing it with any location information it can derive. The Find My network setting is optional for all the hardware that can also use Find My *device*, but it's necessary to locate AirTags and third-party Find My accessories and can't be disabled for them—that's just like turning them off. If you don't use AirTags and don't want your Internet-connected devices to participate in the Find My network, you can turn this setting off on those devices. The only downside is that doing so will also prevent you from being alerted if someone tries to track your movement with a hidden AirTag. One additional difference: you can track your hardware via the Find My network only using a native Find My app for security reasons; you cannot use iCloud.com's Find iPhone Web app.

Part of the confusion stems from how Apple grouped these settings under (for instance) Settings > *YourName* > Find My > Find My iPhone. If you assumed that the Find My iPhone option related purely to finding your iPhone, you might think using Find My iPhone required that you participate in the Find My network. You have to disable Find My network at that level of settings to end your participation in the Find My network. (On a Mac, that option is System Preferences > Apple ID/iCloud, available by clicking Options next to the Find My service name.)



Adding to the confusion, the Find My app bundles together finding devices like iPhones, items like AirTags, and people who have shared their location with you. That's likely the correct approach for a good user experience, but it muddies the distinction between Find My *device* and the Find My network.

As a final bit of confusion, the AirPods and some Beats headphones also appear in the Find My app's list of devices, but they connect only locally over Bluetooth and don't broadcast their locations to

anything but the devices with which they're paired. Thus, you can find them only when they're in range of their associated iPhone or iPad.

We'd like to see Apple enhance AirPods charging cases, or even the AirPods themselves, with support for the Find My network. They're the Apple devices we misplace the most (see "AirPods Versus AirPods Pro: Apple's Earbuds Go Head-to-Head," 3 July 2020). It's also ridiculous that Apple would introduce a beautifully redesigned Siri Remote at the same time as the AirTag without adding support for ultrawideband locating using the Find My app (see "Apple Updates Apple TV 4K; Introduces New Siri Remote," 20 April 2021).

By Julio Ojeda-Zapata

Consumer Desktop Mac Buying Guide: Which Is Right For You?

Most Mac users buy laptops, but Apple hasn't neglected those who prefer desktop Macs. Its recently released M1-based iMac has a brand-new design in an array of lively colors, a thin profile, better performance than its Intel precursor, enhanced webcam image quality, and more (see "Apple Releases New M1-Based 24-inch iMac in Spring Colors," 20 April 2021).

If you are in the market for a desktop Mac, as I am, you might find the M1-based iMac to be tempting. I've been using an Apple review unit for a few weeks, and I'm smitten—even though it has a physical flaw that I'll explain in a bit.

Before dropping $1299 or more for one of these Macs, however, you should consider all your desktop Mac choices, as I have been. I'm focused on consumer-level options for those with limited budgets, so you'll see no further mention in this article of the Mac Pro with its Pro Display XDR for a combined minimum of $10,998, or even the 27-inch iMac with 5K Retina display ($1799 and up).

But the Mac mini, retrofitted late last year with the same M1 chip now found in the iMac and other newer Macs with Apple silicon, is worth a look (see "Apple M1 Chip Powers New MacBook Air, MacBook Pro, and Mac mini," 10 November 2020). The Mac mini starts at $699, not including a display, keyboard, or pointing device.

Then there is the M1-based MacBook Air, starting at $999. Yes, it's a laptop, but many users plug it into a display, attach external input devices, and get busy in desktop mode at least part of the time. The M1-based 13-inch MacBook Pro starts at $1299, but I don't see it as a good deal if you're on a budget for reasons I'll explain a bit later.

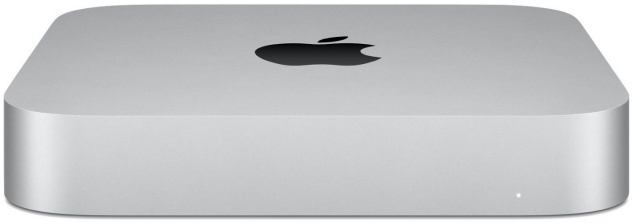
I'm guessing you are at least superficially familiar with all of these Mac options, but I hope to dig into details and nuances you may not have considered. I had not made my buying decision as I typed these words, so writing this article has been a helpful exercise.

Modular Mac

My last Mac was the space gray Mac mini, announced in 2018, with an eighth-generation Intel i5 processor, 8 GB of memory, and 256 GB of storage

for $799. It served me nicely until last year, when I received $460 for it from Phobio, Apple's hardware trade-in partner.

I had intended to replace the Intel-based Mac mini with its M1 equivalent for $699, but the new iMac put my buying plans on pause. I might still end up going with the Mac mini, however. It has some benefits: choosing your own display, easy swapping in the future, and access to legacy ports.



You get to choose your own display. Separating the Mac from its screen opens up a world of options. If you are on a tight budget, you can get a decent-enough display for a few hundred dollars for a combined cash outlay under $1000, which is substantially less than the cost of an entry-level iMac. Better yet, you might already have a display to press into service, so the Mac would be your only significant expense.

I like my midrange display, the $699 UltraFine 4K Display, made by LG with Apple's input and sold via Apple's online and physical stores (see "Apple Debuts LG's All-New 23.7-inch UltraFine Display," 20 May 2019). The 23.7-inch display connects to a Mac via a Thunderbolt 3 port and doubles as a hub with a second Thunderbolt port and three USB-C ports.

TidBITS managing editor Josh Centers bought a different LG display, the 27UK850-W 27-inch (see "LG 27UK850-W: An Acceptable 27-inch Display for the Mac," 18 December 2020). It doesn't do Thunderbolt 3 but does have a USB-C port for linking to a Mac. The display's price varies, often topping $600, so keep an eye out for deals; Josh paid $380.

If you want to use your Mac mini with two displays, things get a little complicated. The Mac mini supports only a single display via Thunderbolt, but you can connect a second display via its HDMI port. That may require the use of an adapter.

Of course, you also need to add external input devices—the Mac mini doesn't come with any. Choices abound; you can't go wrong with Apple's Magic Keyboard and Magic Trackpad, which I've

been using for years. I dislike the Magic Mouse, though, so I use Logitech's MX Master 3.

One great thing about the Mac mini is how easy it is to transport if, for instance, you have to take it to an Apple store's Genius Bar—detach it from its display and go. Any sort of transport is more of a chore with the iMac, thanks to its integrated display.

The Mac mini is easy to swap out. After decades of using all-in-one Macs, ranging from the Mac Classic and the Color Classic to every flavor of iMac, my switch to a Mac mini was jarring but logical. If I bought a nice-enough display, I reasoned, it would last me through at least two or three Mac generations. I'd just exchange one Mac mini for another as a sort of brain transplant, thereby saving money.

The Mac mini has legacy ports. Most M1-based Macs offer limited port options, forcing users to invest in dongles or docks. The Mac mini is the exception with two USB-A ports, an HDMI port, and an Ethernet port, along with the standard two Thunderbolt ports.

Clamshell Mac

I've never owned a Mac laptop, but whenever Apple sends me one for review, I plug it into my LG UltraFine display. Sometimes I keep the laptop open and perch it on Twelve South's Curve stand for use as a secondary display. At other times, I'll keep the laptop closed in "clamshell" mode.

Such an arrangement can have huge ergonomic benefits. Many laptop owners experience neck strain by continually hunching over their laptop screens. I often run into Mac laptop users who do not seem to grasp the health implications of such an arrangement. I am happy to educate them.

The other obvious benefit of connecting a MacBook to a desktop display is more screen space to work, especially if you position the laptop alongside as a secondary screen.

A laptop-with-display arrangement is also helpful in an office or home where a workspace is shared. Imagine Mom, Dad, and the kids moving about the house with their laptops, which is fine most of the time. But if a household member wants better ergonomics and increased screen real estate for a serious work session, they can jack into a communal display.

Pairing a Mac laptop with an external display doesn't have to be expensive. Begin with a $999 MacBook Air and add a decent monitor to keep the combined outlay under about $1400, or roughly the cost of a mid-range iMac.

Want two external screens? The M1-based MacBook Air, unlike its Intel-based predecessor, does not have native support for dual displays—but there are workarounds. Companies such as Kensington offer hardware and software to get around this issue. If you have an iPad, that can be one of your external screens via Apple's Sidecar feature (see "Catalina's Sidecar Turns an iPad into a Second Mac Monitor," 21 October 2019), or using third-party options such

as Luna Display or Duet Display (see "Luna Display Turns an iPad into a Responsive Mac Screen," 7 December 2018 and "Attach an iPad to Your MacBook as a Second Display with Mountie," 22 February 2019).

Need legacy ports? The MacBook Air has only two Thunderbolt ports along with an audio jack, but you can get more ports with an external display (the LG model that Josh bought includes two HDMI ports and two USB-A ports along with its headphone jack and a single USB-C port) or a Thunderbolt 3 dock (I favor Elgato's model with two Thunderbolt ports, three USB-A ports, a Gigabit Ethernet port, and a DisplayPort, along with headphone and microphone ports).

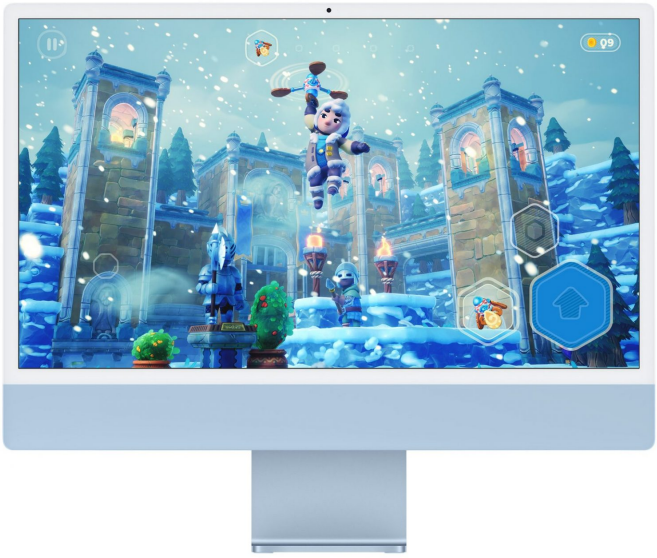
The 13-inch MacBook Pro is another laptop option, but I'd suggest avoiding it unless you're enamored with its Touch Bar (not many people are). Its screen is only marginally brighter than the MacBook Air's. It has minimally better performance thanks to a fan that the MacBook Air lacks but would rarely need in everyday use. It's bulkier and heavier than the MacBook Air. And of course, it's more expensive.

Some might be reluctant to buy an M1-based MacBook Air or MacBook Pro because of their dated designs (all but identical to their Intel-based predecessors), but it may be a while before redesigned consumer MacBooks arrive. Pro-level laptops with fresh looks are rumored to be first up—perhaps later this year—with consumer models possibly due by the end of the year or in 2022. If I were in the market for a consumer laptop, I would wait it out, but I realize not everyone has that luxury.

Pretty Mac

Apple's original iMacs back in the 1990s are famous partly for introducing bright colors to enliven what until then had been a mostly beige personal computer era. Now, after a long interregnum with many generations of iMacs in subdued white, silver, and gray shadings, colors are back with the 24-inch iMac.

The color is one reason I love my loaner iMac, with its dark blue on the back and a lighter blue shade on the front "chin" beneath the display. I'm even more taken with the purple model because it makes me think of Minnesota's Prince. Apple also sells the iMac in green, yellow, orange, pink, and silver. (Only blue, green, pink, and silver are available with the entry-level configuration, but higher-end configurations get the full rainbow.)



Yes, the colors are cool, but there are more practical reasons to consider going with the M1-based iMac over an alternative.

Convenience. You get everything you need in a self-contained package that maximizes desk space and minimizes cable clutter. That has been the case since the original iMacs, but the new models push the envelope with a body that is so thin that it looks a bit like an iPad mounted on a stand (it's thinner than the original iPhone). It achieves its thinness partly due to the space-saving nature of the M1 internals and the external power supply with an optional Ethernet jack.

At under 10 pounds (4.5 kg), the iMac is lightweight enough to move around easily. It may be more awkward than a Mac mini or a MacBook Air, but it's undoubtedly easier to move than any other Mac with an integrated display.

Better webcam. Ever since I switched from an iMac to the Mac mini, I have struggled with videoconferencing, which is unfortunate since the pandemic made it so important. It's clunky to

balance an external webcam atop my display, which lacks an internal camera, and I don't like the cable clutter. Even worse, the various third-party webcams I've tried have had difficulty providing consistent image quality in my unevenly illuminated home office, forcing me to tinker with software utilities that never fully solved my problem. You may have faced similar issues; webcams can be finicky beasts.

Improved video quality is one of the big reasons I am considering buying a 24-inch iMac. I was blown away by the image quality during my first video chats on my loaner unit. It's the first iMac webcam with a 1080p resolution. It has a larger sensor for improved low-light performance, along with computational image enhancement. Apple has worked wonders here. If I were to nitpick, I'd wonder why Apple did not go full 4K, but I don't know if I'd really notice that resolution.

External display support. TidBITS publisher Adam Engst recently encouraged me to try dual-display computing via an iMac paired with an external monitor. Such a setup isn't new (iMacs have supported the feature for years), but it has been a revelation for me, and I may not be able to go back to a single screen again.

Setup is super easy; just connect the iMac and the display with a Thunderbolt 3 cable. My LG UltraFine and 24-inch iMac loaner have worked flawlessly together. I'm limited to one external display with the M1-based iMac, but older iMacs natively support up to two displays. (Realistically, it can be hard to work on three displays because the edges end up quite far away.)

So, if you already have an external display you like, buying an iMac and placing it alongside your monitor will introduce you to the wonders of dual-display productivity.

Legacy port scarcity is almost as much a problem with the 24-inch iMac as it is with the MacBook Air. The entry-level iMac has only two Thunderbolt ports (along with a headphone jack), and higher-end configurations add two USB-C ports. The Ethernet port is in the external power brick, but only with the higher-end configs; the brick with the entry-level iMac lacks the port unless you pay extra for it. It's obvious why Apple left out the Ethernet port and other legacy ports: the iMac is too thin to accommodate them.

Again, an external display could add legacy ports that are absent on the iMac, so that's another reason to consider a secondary display. Or get a Thunderbolt 3 dock.

Touch ID support. The Touch ID sensor found on recent Apple laptops is helpful for unlocking (and locking) the Mac and for password autofill, Apple Pay transactions, and purchases on Apple's iTunes, App Store, and Books storefronts. It's also handy for fast user switching.

However, Touch ID hasn't been an option for desktop Mac users so far. Now Apple has brought Touch ID to the desktop with its Touch ID Magic Keyboard, although there's a catch: it's available only with purchases of the M1-based 24-inch iMac. Apple bundles it with the higher-end configurations and offers it as an option with the entry-level model. But it will work with any M1-based Mac and should eventually be available as a standalone purchase.

The Touch ID Magic Keyboard, which is color-matched with the iMac, puts its touch sensor on the upper right corner and has worked as expected.

One thing to keep in mind if you're excited about unlocking your Mac automatically—an Apple Watch provides the same capability, so you may not need Touch ID.

Sound quality. The speakers built into the 24-inch iMac are the best ever for an iMac, and they sound great. This saves you the hassle of procuring external speakers. Sound from the M1-based Mac mini, MacBook Air, and 13-inch MacBook Pro isn't as good, so you might end up wanting a HomePod mini or other external speakers.

There is one possible problem with the 24-inch iMac. When I first unpacked my iMac and put it on my standing desk, I was puzzled that it seemed a bit askew. I attributed this to my uneven floor and imperfections in my office wall, which have tended to throw me in the past. I tucked a few Post-Its under one side of the iMac stand and put it out of my mind.

It turns out my sample is one with a well-documented physical flaw: its screen is a bit crooked in how it attaches to its base. Reports I've seen on the degree of skew vary from one millimeter to several millimeters. In my case, it's off by about a millimeter, enough to drive me nuts—now that I've seen it, I can't unsee it. Nevertheless, my iMac has functioned flawlessly in every other way, so I would not urge you to forgo a purchase. But you should check your iMac with a ruler upon unpacking it and insist on an exchange or your money back if it is not level. (Apple has a 14-day, no-questions-asked refund policy.)

This is why ultra-cautious Apple users wait a while before spending money on any brand-new hardware design. Apple's overall track record is good, but imperfections like this occasionally crop up, and it can be worth waiting to see if others report any issues before ordering. We'll have to see if Apple acknowledges the problem and establishes a repair program to address it.

Which Mac?

Shopping for a desktop Mac got more interesting—and complicated—with the arrival of the M1-based 24-inch iMac. But Apple made one aspect of the decision simple: all the Macs use the same M1 processor, so they are nearly identical in performance. So your choice of Mac will be based on other factors.

- Do you fancy a modular approach to computing with a compact desktop Mac that is easy to swap out for a newer model and combine with a display or displays exactly to your liking and within your budget? The Mac mini may be for you.
- Do you like the idea of desktop computing for improved comfort and productivity with an external display and input devices, perhaps in a shared environment, but require the option to unplug for computing on the go? The MacBook Air might be exactly what you need.
- Do you crave some color in your Mac life, perhaps with fond memories of Bondi blue, along with the tidiness that comes with an all-in-one machine that sports a better webcam and the option to plug in a second monitor? Apple's 24-inch iMac could be just the ticket.

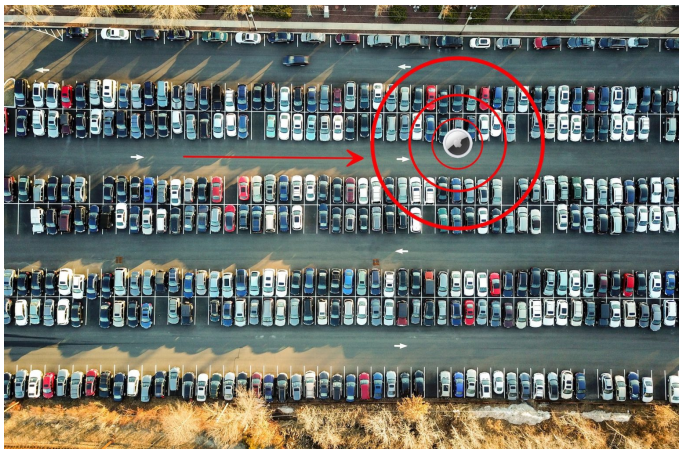
I'm not in the market for a laptop because I prefer to use an iPad for my mobile computing, so I'm vacillating between a Mac mini and a 24-inch iMac. It's a tough call. The Mac mini approach is less expensive but would have only a single display unless I wanted to spend more on a second screen. The iMac is a more considerable investment, but I'd get two displays and Touch ID along with the brand-new design. But if I get an iMac, its screen had better be level.

By Glenn Fleishman

13 AirTag Tracking Scenarios

Apple's AirTag is an odd product from a company that typically makes devices designed for interaction. It's an inert button designed to be tracked passively across Apple's crowdsourced Find My network, in which every iPhone, iPad, and Mac that opts into the Find My network provides privacy-protecting location information about wayward hardware.

Because AirTags are small, easy to conceal, and have a long battery life, they're ideal for those of us who accidentally leave things behind, lose our keys, can't find our car in a parking lot, or worry about having stuff stolen. With an iPhone 11 or 12, you can easily find an item attached to an AirTag around the house, too.



Apple, Omer Rana on Unsplash

AirTags contrast sharply with GPS-based tracking devices, often used to keep tabs on people with dementia and track children. Such GPS devices work best outdoors, require frequent charging, are somewhat bulky (relative to an AirTag, at least), and have a recurring service fee. (The competing Tile products have the same advantages as AirTags, but Apple's network of nearly a billion devices on its Find My network gives it a leg up in ubiquity. Of course, that ubiquity introduces safety concerns, too.)

We've written previously about the Find My network in general and how it works, Apple's move to expand access to third parties, and the introduction of the AirTag. See:

- "How Apple's New Find My Service Locates Missing Hardware That's Offline," 21 June 2019
- "Apple Opens "Find My" Crowdsourcing to Third-Party Accessories," 9 July 2020
- "Apple Opens "Find My" Crowdsourcing to Third-Party Accessories (For Real This Time!)," 7 April 2021
- "Apple's AirTag Promises to Help You Find Your Keys," 20 April 2021

Now that I've had a chance to experiment with some AirTags, and Apple has released specifics on the intention and limitations of tracking, this article focuses on scenarios that attempt to think through the consequences of how people will use and misuse AirTags. There are many terrific ends to which AirTags will be put, and I believe those represent the vast majority of cases of how they'll be used.

But Apple built in privacy for both the people who own AirTags and those who find an AirTag near them, including anti-stalking measures. These choices may prevent both legitimate and illegitimate uses. I get into the technical details in the latest version of *Take Control of iOS & iPadOS Privacy and Security*, with a significantly revised chapter on the Find My network and complete details on pairing and using AirTags, as well as other Apple hardware.

In this article, however, let's dig into how people will use AirTags, starting with items that are lost, moving on to items that are stolen, and finishing with thoughts about stalking.

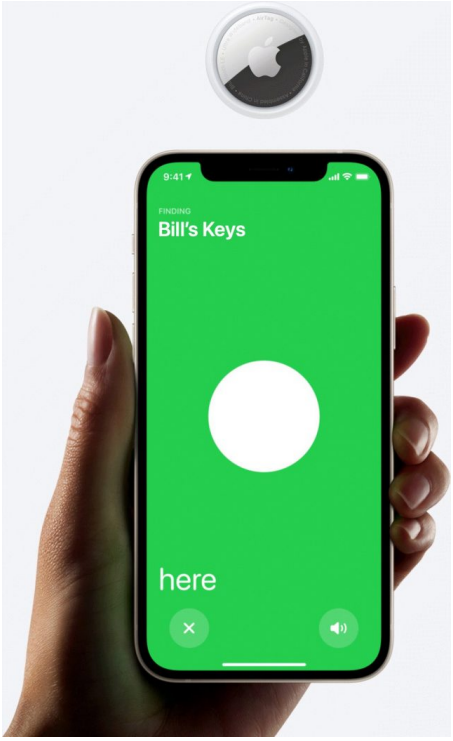
Something Lost

Bill's Wayward Keys

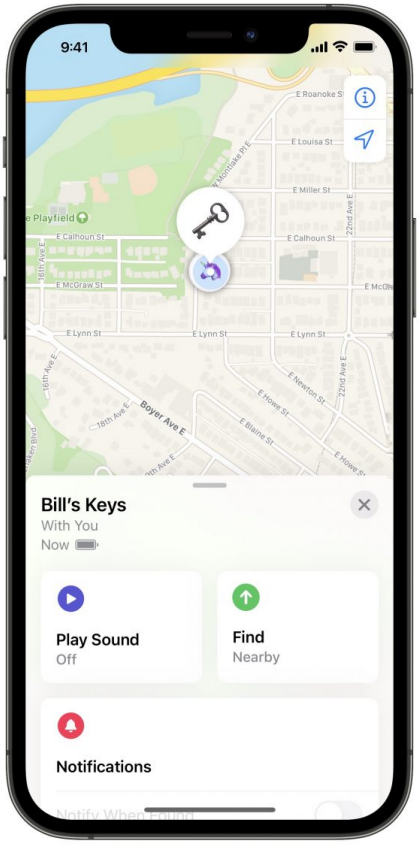
Bill can never find his keys. He knows he should pick a consistent place to put them down or mount a hook inside the front door. Instead, he leaves them in a coat pocket, plops them on a table and drops mail on them, or somehow leaves them somewhere unexpected—like the bread drawer?!

Like this morning, when he searched fruitlessly after finishing breakfast. But this time, Bill had an AirTag attached to his keychain and an iPhone 11 Pro. He launched the Find My app, selected his keychain AirTag, and tapped Find Nearby. The Find My app started listening for the ultrawideband broadcast from his AirTag. Once it locked on, Bill walked around his home, looking like he was dowsing for water, as the Find My app nudged him in the right direction and lit up green when he was on track.

The app showed the distance as he closes in on his AirTag and displayed "here" when he was on top of it. He still couldn't see it, so Bill tapped the speaker icon, and the item played some pleasant, recognizable tones to provide a little more guidance. Ah, there it is! Under the jean jacket in the pile of laundry.



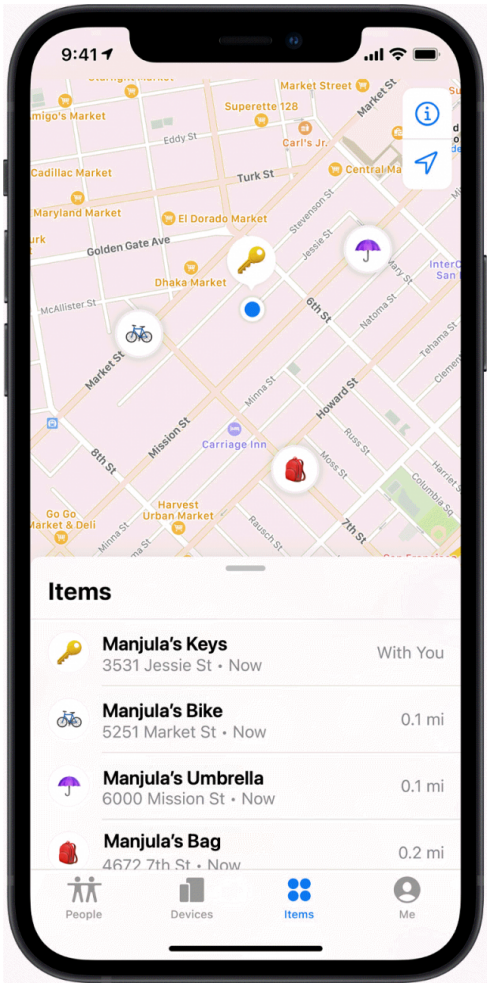
Should Bill have been too far from the AirTag, or if there were too many obstructions in the way—like walls, books, or laundry—Find My would have picked up the more powerful but non-directional Bluetooth signal and provided some general directional aid. As he got closer, he could try tapping Find Nearby again to see if the ultrawideband signal could reach his phone.



Manjula and the Missing Messenger Bag

Meanwhile, Manjula knew she put her messenger bag down somewhere after setting out to drive home, but she wasn't sure where. She remembered that she had it with her in the car but couldn't seem to find it in the house. Fortunately, she had an AirTag zipped into a pocket for just this reason.

She brought up the Find My app on her phone and tapped her bag's AirTag. It showed up on a map a couple of blocks away, where she parked her car, with the most recent update just a few minutes before. "Of course!" she thought, "I never brought it in!"



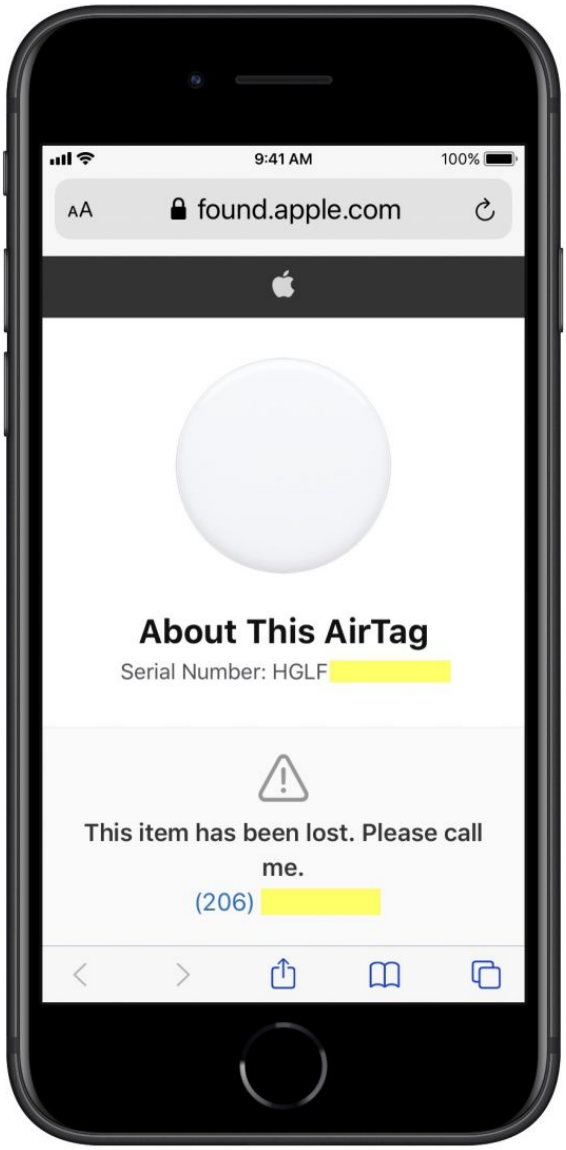
While AirTags rely on ultrawideband and Bluetooth for nearby location finding, enough people carrying iPhones had passed by Manjula's parked car that the Find My network updated the position.

Nic's Missing Laptop Bag

Across town, Nic was slightly frantic. They can't figure out where their laptop bag is. The college student wondered: "Did I leave it in the library? At the coffee shop? In my friend's room? On the tram? Aieee!"

Firing up Find My, Nic didn't see a recent location for their laptop bag's AirTag, so they tapped Enable under Lost Mode and entered their phone number. Through troubled sleep, they wondered if their computer was gone for good. But a phone call woke them up in the morning with good news: a library staffer found their bag while opening up the library. Because the staffer only had an Android phone, the AirTag wasn't able to update its location with the Find My network.

However, the library staffer looked through the bag for ID, found the AirTag, and held it up to their Android phone, which read the AirTag's RFID tag over NFC (near-field communication). The staffer then followed the link that the Android phone displayed to the AirTag's serial-number page and called the number Nic had posted. Nic arranged to get it later from lost-and-found and fell back into a dreamless slumber.



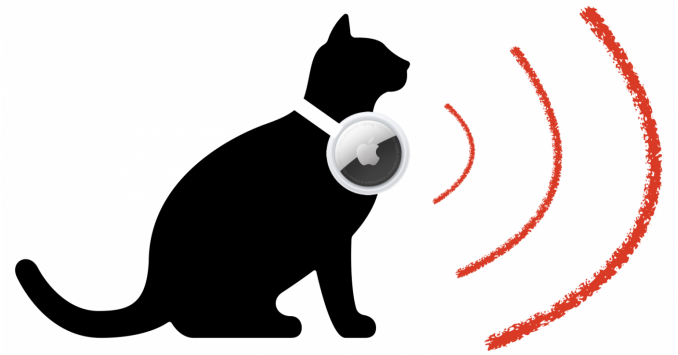
Martyn's Post-Bender Panic

Speaking of slumber, Martyn woke blearily after a bender with his friends. While he got home safely after getting a ride from a friend who hadn't been drinking—and avoided making a mess in the backseat—he couldn't find his jacket, which had his money, wallet, and other important possessions zipped into it, along with an AirTag. He had no memory of where he wound up as the previous night progressed.

Martyn's iPhone rang—at least that was in his trouser pocket. It was his friend Rafael, who was driving around when his iPhone displayed an alert that an AirTag was "moving" along with him. He tapped the notification, tapped Play Sound, and found Martyn's jacket balled up under the passenger seat. "Do you want it back now?" Rafael asked. Whew!

Ruth Bader Ginspurr Escaped the House

Tracy was despondent. Her cat, Ruth Bader Ginspurr, had apparently slipped out the door when nobody was watching. She was not an outdoor cat, and the last time she'd gotten out, it was a week before a neighbor found her, hungry, pitiful, and worse for wear.



Ruth wore ID tags, but Tracy had also recently equipped her with a collar designed to hold an AirTag. In the Find My app, she saw that Ruth's AirTag was most recently seen in a grove of trees in a park full of iPhone-toting runners. With Ruth's favorite squeaky mouse in hand, Tracy went to the park, squeezed the toy a few times, and spotted Ruth—and grabbed her for the walk home.

Something Stolen

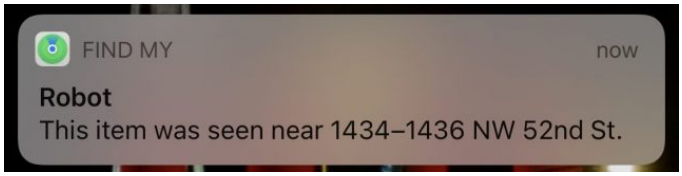
Chai's Snagged Bag

It was only a minute. After waiting two weeks after her second COVID-19 vaccination shot, Chai had ventured out to sit in a café for the first time. She set her bag down under a table for a moment in a mostly empty coffee shop and went to wash her hands. When she came back, the bag was gone. The barista had been leaning down to clean the espresso machine and didn't notice someone come in and snatch it.

Chai's MacBook Air, sketchbook, and various sundries were in the bag, along with an emergency $20 bill and an AirTag, but she had taken her phone with her to the restroom. She pulled up the Find My app, marked the AirTag as lost, and watched for updates. Minutes later, she received a ping. She thought about calling the police but figured they wouldn't come fast enough to help and decided to look for the bag on her own, promising herself that she wouldn't put herself in potential danger by getting too close.

As she approached the location marked on the map, she tapped Find Nearby and started to get

location information. Surely it couldn't be down an alley? And that seemed dangerous. But when she got closer, she realized her bag was on the ground, and there was nobody nearby. She grabbed it and found that her MacBook Air and emergency cash were gone, but the sketchbook and everything else remained in place. She used Find My to send a signal to erase her MacBook Air, should the thieves connect it to the Internet again, and called her insurance company.



Sorry, Charlie

Charlie was less lucky. His backpack containing an AirTag was taken by someone who spotted an open window, climbed up part of a wall, and grabbed it out of his house. He could see briefly where it went in Find My, but then it disappeared. He never found the backpack or received any tracking updates, so he assumed the thief was clever enough to search the backpack and either remove the AirTag battery or smash it.

Fenchurch's Double AirTag

Fenchurch left not one but two AirTags in her car. Living in a city with a high rate of car theft, she thought perhaps hiding AirTags could be an extra deterrent in addition to the car alarm, the electronic ignition–disabling technology, and the steering wheel lock. Sadly, her car was stolen—but her bet was good. The AirTag that she'd placed in the glove compartment, where it was easily found, must have been tossed out the window since Find My helped her find it in the mud on a parking strip.

But she'd hid the other AirTag with the spare tire. She assumed the thieves didn't receive alerts that would have made them aware of the AirTag's presence—they must not have owned iPhones—but enough people passed nearby to produce location updates. Fenchurch called the police, who became interested when they realized that the car was ostensibly located in a seedy industrial area. They checked out the address and were able to recover Fenchurch's car while shutting down the chop-shop operation.

Bad News, Vicente

The hidden AirTag strategy worked for Fenchurch, but Vincente had less luck. He had taped an AirTag to the underside of his dashboard, figuring it would be hard to find. However, the thieves who stole his car one night must have been carrying an iPhone that was recent enough to display an alert.

He deduced that because when he woke up, even before he could mark the AirTag as lost and call the police, he saw that the location in the Find My app of the AirTag was several blocks from the parking lot where he'd left it, tagged with a timestamp of 11:53 PM the previous evening. While waiting for a call back from the police, he went to the location on the Find My map, and his car wasn't there—nor was an AirTag lying on the ground. He figured the thieves received an alert about an unknown AirTag "moving" with them as they drove off in the purloined vehicle. They probably then found and destroyed the AirTag before any other iPhone could reveal its location.

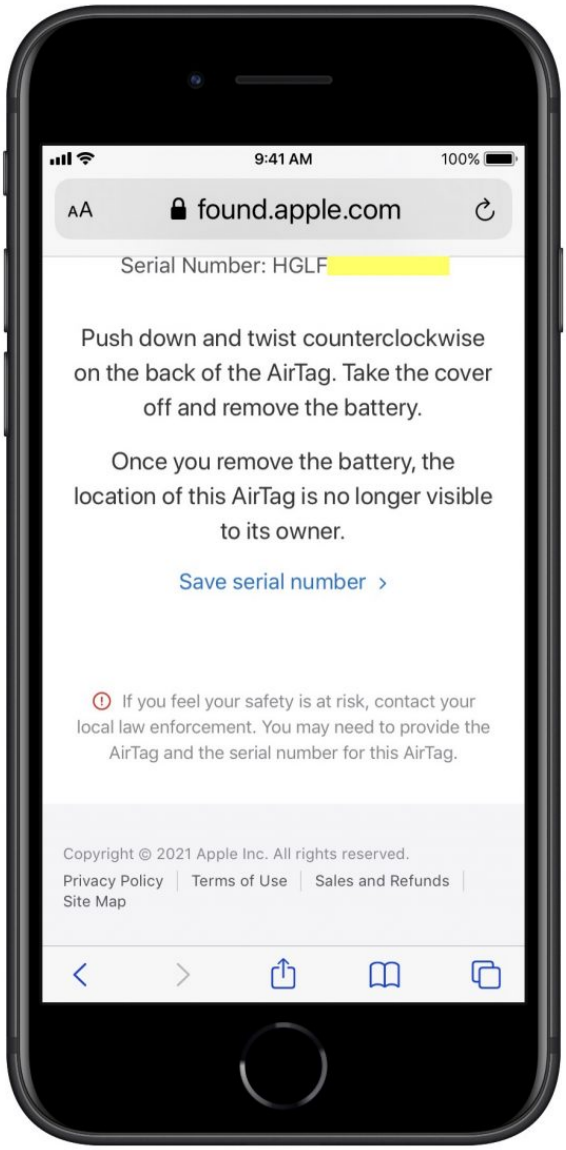
Whatever the case, the AirTag never appeared again. Nor did his car!

Someone Stalked or Tracked Yuen's Ex-Boyfriend

"Where was that beeping coming from," Yuen wondered. He couldn't figure out what he owned that could be making the noise. He finally unzipped and emptied out every last pocket in his backpack—and discovered something he didn't remember. A small bag, cinched tight. When he opened it, he found a round button with an Apple logo.

Searching via Google, Yuen discovered it was an AirTag—and that he could scan it with his Android phone. When he tapped it to his phone to view the associated Web page and realized what it was being used for, his blood ran a little cold. Was this planted by his jealous ex-boyfriend? The controlling person

he broke up with for just this sort of reason? Yuen noticed the link Apple provided about contacting law enforcement.



With the help of a law clinic and local police, Yuen was able to prove that his ex had purchased the AirTag—the serial number helped—which led to charges and a restraining order.

Annelise's Nosy Neighbor

Annelise had had enough. A neighbor kept conveniently showing up "accidentally" at regular intervals in other parts of town when she went out for coffee, to meet a friend, or to shop. It was too much, and she suspected that she was being stalked. She had read online about how her iPhone could be used to track her and consulted some technical friends, too. But between her online research and her friends' analysis, it didn't seem to be hacked. Sometimes she left her iPhone at home and just relied on her Apple Watch, and the neighbor still appeared.

Then she realized she ran into the neighbor only when she drove somewhere, not when she walked, biked, or rode with someone else. With the help of a friend and a Bluetooth-scanning app for her iPhone (like BLE Scanner), she scoured her car and eventually found an AirTag hidden inside the lining of one of the seats. "Well, that's creepy," she thought. She must have left the car unlocked at some point, allowing him an opportunity to hide the AirTag inside—or, worse, he'd broken in without her knowing.

Reading up on Apple's website, Annelise thought that she should have been notified or that the AirTag would have made a sound at various times. But after checking her iPhone's settings, she realized that she had disabled the Find My network option in Settings > *Account Name* > Find My > Find My iPhone. When Apple added the Find My network in iOS 13, she was weirded out by the thought of participating in a global tracking network. But that choice also meant her iPhone wasn't monitoring for AirTags that traveled with her.

And, because Annelise parked her car near both her house and the neighbor's, the AirTag reassociated at least once a day with the neighbor's phone. If she had taken an extended trip with her car, the AirTag might have started beeping. Due to the pandemic, she rarely drove anyone in her vehicle, so no friend with an iPhone would have seen the alert, either.

She was about to move out of town in any case, and she decided to leave her apartment and stay at a friend's place for the remaining time she had—after she removed the AirTag, visited the police station, and filed a report.

A Package for Betsy

Betsy had never liked people she didn't know well having her home address. She was a private person and had had incidents with over-eager boyfriend and girlfriend wannabes. Nothing terrible, but it still put her off having her address in circulation. So she used a package-delivery storefront for her mail, which provided the added benefit that her packages were never stolen from her apartment building's mailbox area.

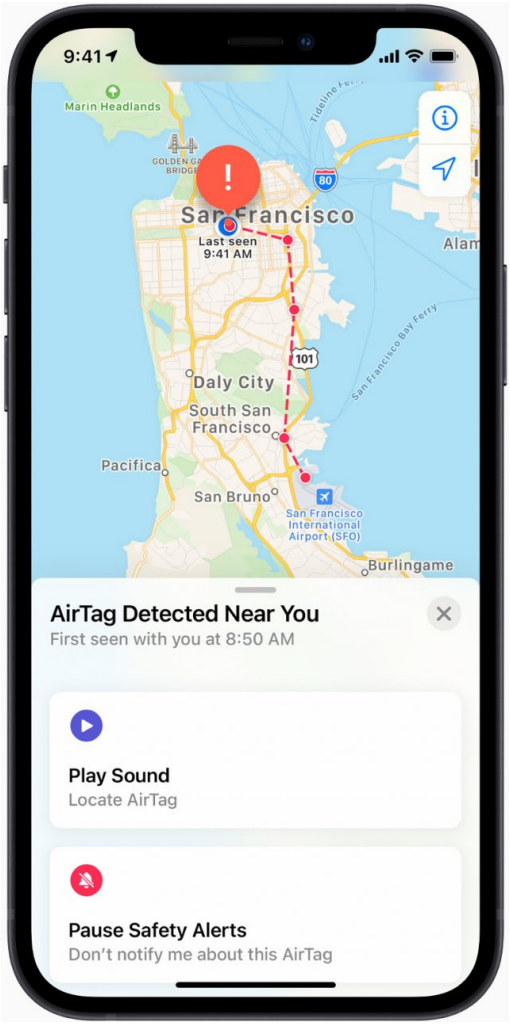
But one day, she picked up a small box from an unknown sender. When she brought it home and opened it, she found it contained a relatively expensive purse she'd mentioned on Facebook but felt she couldn't afford. A secret admirer who asked around for her address and got it from a friend?

While checking out the purse, she felt an odd lump. Sewn into the lining was an AirTag. She knew what it was from Apple's marketing and found the experience unsettling. Someone could have known when she arrived at the package store, her path home, and where she lived. Who would do that?

She looked up the AirTag's serial number, removed its battery, and decided against calling the police for the time being. But she did post a subtle message on Facebook that made it clear she'd found the tracker and was perfectly capable of taking the next step to identify the sender. Fortunately, nothing ever came of it.

Florian's Mystery AirTag

Florian had a disturbing message pop up on his iPhone: "AirTag Found Moving with You," with the annotation "The location of this AirTag can be seen by the owner." He panicked for a moment. Who wanted to know where he was? Why was someone keeping tabs on him? He tapped the notification, and a more complete message appeared, including the first time the AirTag was found near him—1:30 PM—and the message that it "may be attached to an item you are borrowing."



"D'oh!" Florian slapped his forehead. He had borrowed a duffel bag from his friend Asok. He looked inside a zipped pocket, and there was an AirTag. He texted Asok: "Busted! Dude, you're tracking me!" Asok texted back an emoji of a tongue sticking out and the message, "Sorry! I forgot I always leave that in there!" Florian tapped Continue on his phone and tapped to disable notifications for a day.

Better for Some Uses Than Others

I'm just scratching the surface of the cases in which AirTags will be used and abused. It seems clear that Apple needs to refine some of the features in the system. The length of time before an AirTag makes noise, how quickly you're alerted to an AirTag traveling with you, and the fact that a setting can disable such alerts all need more thought.

Some of the gaps in knowing whether you're being tracked are large enough to enable abusive behavior that Apple wants to prevent. The Washington Post's Geoffrey Fowler tested being tracked with permission, and he found a number of loopholes and exceptions that clever stalkers and abusers could exploit.

On the plus side, the record keeping and association of AirTags to individuals makes it relatively easy to figure out who owns an unwanted tracker and what behavior that person has engaged in. A stalker would, at a minimum, have to create a throwaway iCloud account and use it with a disposable iPhone or iPad to track an AirTag to avoid creating an overt trackable connection. That's a lot of money and effort, and it might still be difficult to avoid providing identifiable information unintentionally. (Abusive people aren't always great at anticipating consequences, but some are keenly aware of how readily they can be identified.)

AirTags also don't help much when it comes to deterring or tracking theft. They aren't a deterrent because they have to be hidden to avoid being destroyed. And when it comes to tracking a stolen item, the combination of iPhone alerts and general suspicion will probably result in the thieves finding and destroying the AirTag in quick order. Though, as I pointed out above, you might be able to recover a stolen bag minus its cash and electronics.

Happily, Apple seems to have designed the system to be open to adapting, maturing, and improving. The overwhelming majority of uses of AirTags and the Find My network will certainly be positive ones. The goal will be to block malicious uses more effectively without diminishing the value of the entire system.