Remember, Apple AirTags and ‘Find My’ app only work because of a vast, largely covert tracking network

Paul Haskell-Dowland, *Edith Cowan University*

Apple recently launched the latest version of its operating system, iOS 14.5, which features the much-anticipated app tracking transparency function, bolstering the tech giant’s privacy credentials.

But iOS 14.5 also introduced support for the new Apple AirTag, which risks doing the opposite.

For the uninitiated, an AirTag is a small device (similar to a Tile) that can be attached to personal items such as keys, wallets or luggage. The tag periodically sends messages that can be used to track its location, letting you find any lost or missing items with the help of an app.

While clearly useful, AirTags can also potentially be misused. Concerns have been raised they might facilitate stalking, for example.

And there’s also a more fundamental issue with this technology. Its euphemistic description as a “crowdsourced” way to recover lost items belies the reality of how these items are tracked.

What you won’t find highlighted in the polished marketing statements is the fact that AirTags can only work by tapping into an Apple-operated surveillance network in which millions of us are unwitting participants.

So, how exactly do AirTags work?

AirTags are small, circular metal discs, slightly larger and thicker than an Australian one-dollar coin. Once paired with your Apple ID, the tag’s location will be shown in the “Find My” app, whenever location data are available.

Apple airtag.
Apple newsroom

Each tag transmits a unique identifier using Bluetooth. Any compatible Apple device within range (up to 100 metres in ideal conditions) will then relay that identifier to Apple's servers, along with its own location data. The tag's owner can then log onto the Find My app and access those location details, and bingo — you now have a pretty good idea of where your lost bag is.

The AirTags themselves have no positional location capability – they do not contain GPS technology. Rather, they merely "ping" the nearest Bluetooth-enabled device and let that device's location data do the rest.

Besides Bluetooth, AirTags also use a relatively new technology called Ultra Wideband. This new feature is supported only by recent Apple devices such as iPhone 11 and 12, and allows for much more precise location tracking.

This precision extends to directional finding – now, your phone can literally point you towards the missing tag.

While the actual nature of the data transmitted is not too concerning (tag ID and location), what makes it worrying is the sheer scale and number of devices involved. By using an AirTag, you are effectively availing yourself of a global monitoring network containing millions and millions of devices.

Everyone's iPhone (assuming Bluetooth is enabled) is listening for AirTags. When it "hears" one, it uploads details of that tag's identifier and the phone's location to Apple's servers.

Besides any privacy concerns, this also likely uses small amounts of your data allowance. That's probably fine most of the time, but if you are travelling internationally you might be hit with unexpected charges if you've forgotten to disable data roaming.

Stalking technology?

Apple says it has implemented a range of safeguards to detect and prevent attempts to use AirTags for

stalking, including an alert triggered when an AirTag seems to be accompanying someone who's not its owner. The alert can appear on the victim's phone (if they use an iPhone) but can also raise an audible alert on the tag itself. But these measures are relatively easy to circumvent.

One experiment showed a tag can be placed on a person and would not trigger any of the safeguards if reconnected to the stalker's device regularly enough. This could be done by the victim returning home or within range of their stalker within a three-day window.

More concerningly, the alerts can be turned off – which a victim of domestic violence may be coerced into doing by their aggressor. What's more, as AirTags and similar devices become more common, we will inevitably encounter more warnings of tags appearing around us. Just like other commonly encountered alerts, many users will tire of seeing them, and dismiss the prompts.

It is also presumably only a matter of time until these devices are hacked and put to other nefarious purposes.

Apple isn't the only technology company drawing unwitting users into large networks. Amazon's SideWalk creates a network that allows your neighbours' doorbell to connect through your Echo device (if their WiFi doesn't extend to the front door), effectively sharing your internet connection!

All of this functionality (and the inherent privacy risks) are covered in the standard terms and conditions. That lengthy, legalese document we never read allows tech companies to hide behind the claim that we have willingly opted into all this.

Can we opt out?

A simple option to avoid your device acting as a cog in Apple's machine is to turn off Bluetooth and location services. With Bluetooth disabled, your device won't "see" the beacons coming from AirTags, and without location services you can't report the proximity of the tag.

Of course, turning off this functionality means losing useful capabilities such as hands-free kits, Bluetooth speakers and satellite navigation, and of course makes it harder to find your phone if you lose it.

Ultimately, if we want to benefit from the ability to locate missing keys, wallets and luggage through AirTags, we have to accept that this is only possible through a global network of sensors – even if those sensors are our own phones.

Paul Haskell-Dowland, Associate Dean (Computing and Security), *Edith Cowan University*