Twitter Thread by Thomas A. Fine ■■



Thomas A. Fine ■■
@thomasafine

So is Apple's anti-theft security a wonderful boon to users?

Or is it just another evil corporation strengthening it's monopoly power?

I had the misfortune of buying a 2018 Mac Mini on ebay a few days ago. Unfortunately, it had not been wiped, and it's security defaults had never been changed.

This essentially turns it into a very shiny paperweight.

And this is where everybody jumps to blame the victim. "But everybody knows you have to make sure the seller wipes the Mac."

My how the corporate overlords have trained us to be their apologists.

To be clear, I'm a software engineer. Part of my job is supporting Mac users. Where I work, people hold on to their computers for several years generally, and the T2 chips are only a couple of years old, so I hadn't run into this situation at work.

Of course, I'd read about them, but I was confident that whatever condition the computer arrived in, I'd likely be able to deal with it.

Unfortunately I hadn't read up enough to be an expert on their T2 chip and Activation lock.

The point is, I'm not an average user. I'm a very above average user. If I can find myself in this situation, almost anyone can.

It's not sufficient for the seller to wipe the mac. They have to do a number of iCloud-related steps to fully erase their identity from the mac. Thanks to the security chip, even a full erase and re-install doesn't do that.

If you don't do these steps, the new owner can not simply erase and reinstall the system. They can't boot into single user mode or boot from an external drive and wipe things that way.

Only a network reinstall, which verifies the iCloud status and requires an iCloud password will work to solve this problem.

So this leaves someone like me who has — entirely legally — purchased a used Apple computer stranded, with the only recourse to hope that I can explain to the seller what they now must do (which is now considerably more complicated) to get this system to be usable by me.

And frankly, the simplest option (which I do not advocate, but that many will use) is going to be to share their iCloud account and password with the buyer. This is of course a significant security hole.

Any security solution which encourages bad security practice is not in fact a security solution.

What they properly must do is to use one of their other Apple devices that they've logged into with the same iCloud account, and tell it to forget the device they've sold.

But there's a lot of assuming happening there.

Apple assumes that the seller owns other Apple devices. There's plenty of Macs for sale used that were bought by someone who wanted to try it, and didn't care for it, and so now they're selling it (and these people are among the most clueless).

Apple assumes that the seller knows the iCloud password. See the last tweet about clueless sellers. But also, laptops can legally come to you with no knowledge of the iCloud account that was used. Like an inherited computer for example.

Apple assumes that the seller gives a damn. Depending on the perfectly legal selling mode they used this may not be true.

Ah but the buyer should beware, right?

Really, imagine any other product, like a car, or a washing machine, or... ANYTHING where the buyer has to beware of the seller having a secret, permanent, unfixable lock that makes the product 100% unusable.

But it prevents theft right?

Maybe. We'll assume yes now for the sake of argument.

Great. Why does Apple care?

Like any corporation Apple only really cares about the bottom line. Does theft cost them money? Yes in theory some portion of stolen computer purchasers would otherwise buy a new computer.

But what if Apple could make ALL used selling of computers a pain the ass, not just stolen ones?

That'd be a MUCH bigger profit incentive for Apple than merely cracking down on stolen computers

And that's what's happened here. Let the buyer beware?

Any buyer who knows about this is going to be VERY worried about buying a used computer. Apple has effectively drastically reduced the used computer market for their computers.

https://t.co/0SIAdtuARJ

There is one other alternative to getting these old computers to work. It turns out that Apple has the ability to trivially reset them. You just have to bring it in to have it serviced.

Which costs money.

AND you have to have the ORIGINAL proof of purchase.

Again, this destroys the reseller market. But this particular loophole is even more sinister.

It turns out things can go wrong with the security chip. There are tales of people who've bought refurbished computers FROM APPLE, only to have a bug in the security chip fail on an update and make their computer unusable.

But because the purchaser did not have the ORIGINAL purchasing papers, Apple wouldn't reset these.

Hopefully that's an extreme example which is rare and which Apple has managed to address. But the knowledge that things like this are possible further dampens the market for used Macs.

It does however turn out that there is a way to hack the security chip in these Macs. It was discovered last fall.

This may provide me with recourse, because I have the expertise to do it (though it's unclear if I have the patience — I may just get my money back from ebay).

But you know who DOES have the patience to do something like this? Because they'll likely do it more than once?

People who steal computers.

So here's the final proof, the ultimate punch line. Computer theft rings are no longer stopped by this security. Only legitimate user-to-user reselling of computers remains as being substantially curtailed.

Of course, this was always the much larger chunk of their profit motive.

But it lays bare what Apple is doing. Your computer is no longer protected from theft. But it's going to be really hard to resell and lose a lot of value because of that. Which costs you money and makes Apple money.

Apple could reset any computer brought to them, no questions asked. If that sounds crazy to you, consider: has a car mechanic ever demanded you prove ownership before they'll fix your car?

Shouldn't it be insulting that their core assumption on every computer they see is to presume that it is stolen unless this can be otherwise proved?

And after all, if someone comes to them later on with proof of theft, Apple should still be able to find if this computer has been reused. This security lockdown doesn't add any real-world theft protection that they didn't already have with Find My Mac.

It just makes them harder to resell. Period.

I would love it if my Representative @RepKClark, and my Senators @SenWarren and @SenMarkey would read the above thread about corporate monopoly control.

I do want to clarify that the T2 chip does potentially add useful security mechanisms and protocols that are superior to previous technology.

It is Apple's administration of this new technology that is monopolist and outrageous.

Apple has the option to be much more lenient about resetting these systems, and it would have virtually no impact on Apple's ability discourage theft.