The All-Seeing “i”: Apple Just Declared War On Your Privacy

Description

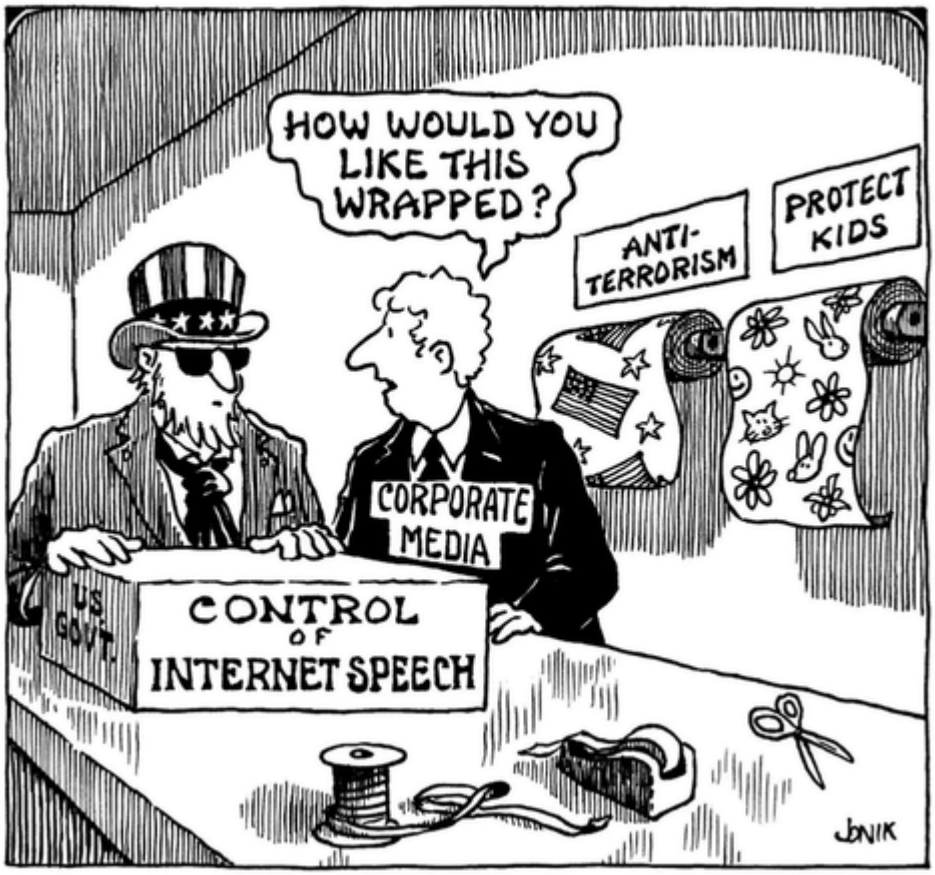
By now you’ve probably heard that Apple plans to push a new and uniquely intrusive surveillance system out to many of the more than *one billion* iPhones it has sold, which all run the behemoth’s proprietary, take-it-or-leave-it software. This new offensive is tentatively slated to begin with the launch of iOS 15?—almost certainly in mid-September?—with the devices of its US user-base designated as the initial targets. We’re told that other countries will be spared, but not for long.

You might have noticed that I haven’t mentioned which problem it is that Apple is purporting to solve. Why? Because it doesn’t matter.

Having read thousands upon thousands of remarks on this growing scandal, it has become clear to me that many understand it doesn’t matter, but few if any have been willing to actually say it. Speaking

candidly, if that's still allowed, that's the way it always goes when someone of institutional significance launches a campaign to defend an indefensible intrusion into our private spaces. They make a mad dash to the supposed high ground, from which they speak in low, solemn tones about their moral mission before fervently invoking the dread spectre of the Four Horsemen of the Infopocalypse, warning that only a dubious amulet—or suspicious software update—can save us from the most threatening members of our species.

Suddenly, everybody with a principled objection is forced to preface their concern with apologetic throat-clearing and the establishment of bonafides: *I lost a friend when the towers came down, however… As a parent, I understand this is a real problem, but*…



As a parent, I'm here to tell you that sometimes it doesn't matter *why* the man in the handsome suit is doing something. What matters are the consequences.

Apple's new system, regardless of how anyone tries to justify it, will permanently redefine what belongs to you, and what belongs to them.

How?

The task Apple intends its new surveillance system to perform—preventing their cloud systems from being used to store digital contraband, in this case unlawful images uploaded by their customers—is traditionally performed by searching *their systems*. While it's still problematic for anybody to search through a billion people's private files, the fact that they can only see the files you

gave them is a crucial limitation.

Now, however, that's all set to change. Under the new design, *your phone* will now perform these searches on Apple's behalf before your photos have even reached their iCloud servers, and—*yada, yada, yada*—if enough "forbidden content" is discovered, law-enforcement will be notified.

I intentionally wave away the technical and procedural details of Apple's system here, some of which are quite clever, because they, like our man in the handsome suit, merely distract from the most pressing fact—the fact that, in just a few weeks, Apple plans to erase the boundary dividing which devices work for you, and which devices work for them.

Why is this so important? Once the precedent has been set that it is fit and proper for even a "pro-privacy" company like Apple to make products that betray their users and owners, Apple itself will lose all control over how that precedent is applied. ??????As soon as the public first came to learn of the "spyPhone" plan, experts began investigating its technical weaknesses, and the many ways it could be abused, primarily *within the parameters of Apple's design.* Although these valiant vulnerability-research efforts have produced compelling evidence that the system is seriously flawed, they also seriously miss the point: Apple gets to decide whether or not their phones will monitor their owners' infractions for the government, but it's *the government* that gets to decide on what constitutes an infraction… and how to handle it.

For its part, Apple says their system, in its initial, v1.0 design, has a narrow focus: it only scrutinizes photos intended to be uploaded to iCloud (although for 85% of its customers, that means ***EVERY*** photo), and it does not scrutinize them beyond a simple comparison against a database of specific examples of previously-identified child sexual abuse material (CSAM).

If you're an enterprising pedophile with a basement full of CSAM-tainted iPhones, Apple welcomes you to entirely exempt yourself from these scans by simply flipping the "Disable iCloud Photos" switch, a bypass which reveals that *this system was never designed to protect children*, as they would have you believe, but rather to protect their brand. As long as you keep that material off their servers, and so keep Apple out of the headlines, Apple doesn't care.

So what happens when, in a few years at the latest, a politician points that out, and—in order *to protect the children*—bills are passed in the legislature to prohibit this "Disable" bypass, effectively compelling Apple to scan photos that *aren't* backed up to iCloud? What happens when a party in India demands they start scanning for memes associated with a separatist movement? What happens when the UK demands they scan for a library of terrorist imagery? How long do we have left before the iPhone in your pocket begins quietly filing reports about encountering "extremist" political material, or about your presence at a "civil disturbance"? Or simply about your iPhone's possession of a video clip that contains, or maybe-or-maybe-not contains, a blurry image of a passer-by who resembles, according to

an algorithm, “a person of interest”?

If Apple demonstrates the capability and willingness to continuously, remotely search every phone for evidence of one particular type of crime, these are questions for which they will have no answer. And yet an answer will come—and it will come from the worst lawmakers of the worst governments.

This is not a slippery slope. It’s a cliff.

One particular frustration for me is that I know some people at Apple, and I even like some people at Apple—bright, principled people who should know better. Actually, who *do* know better. Every security expert in the world is screaming themselves hoarse now, imploring Apple to stop, even those experts who in more normal circumstances reliably argue *in favor* of censorship. Even some survivors of child exploitation are against it. And yet, as the OG designer Galileo once said, it moves.

Faced with a blistering torrent of global condemnation, Apple has responded not by addressing any concerns or making any changes, or, more sensibly, by just scrapping the plan altogether, but by deploying their man-in-the-handsome-suit software chief, who resembles the well-moisturized villain from a movie about Wall Street, to give quotes to, yes, the *Wall Street Journal* about how sorry the company is for the “confusion” it has caused, but how the public shouldn’t worry: Apple “feel[s] very good about what they’re doing.”

Neither the message nor the messenger was a mistake. Apple dispatched its SVP-for-Software Ken doll to speak with the *Journal* not to protect the company's users, but to reassure the company's investors. His role was to create the false impression that this is not something that you, or anyone, should be upset about. And, collaterally, his role was to ensure this new "policy" would be associated with the face of an Apple executive other than CEO Tim Cook, just in case the roll-out, or the fall-out, results in a corporate beheading.

Why? Why is Apple risking so much for a CSAM-detection system that has been denounced as "dangerous" and "easily repurposed for surveillance and censorship" by the very computer scientists who've already put it to the test? What could be worth the decisive shattering of the foundational Apple idea that an iPhone belongs to the person who carries it, rather than to the company that made it?

Apple: "Designed in California, Assembled in China, Purchased by You, Owned by Us."

The one answer to these questions that the optimists keep coming back to is the likelihood that Apple is doing this as a prelude to finally switching over to "end-to-end" encryption for everything its customers store on iCloud—something Apple had previously intended to do before backtracking, in a dismaying display of cowardice, after the FBI secretly complained.

For the unfamiliar, what I'm describing here as end-to-end encryption is a somewhat complex concept, but briefly, it means that only the two endpoints sharing a file—say, two phones on opposite sides of the internet—are able to decrypt it. Even if the file were being stored and served from an iCloud server in Cupertino, as far as Apple (or any other middleman-in-a-handsome-suit) is concerned, that file is just an indecipherable blob of random garbage: the file only becomes a text message, a video, a photo, or whatever it is, when it is paired with a key that's possessed only by you and by those with whom you choose to share it.

Fig. 1a: Encryption in transit

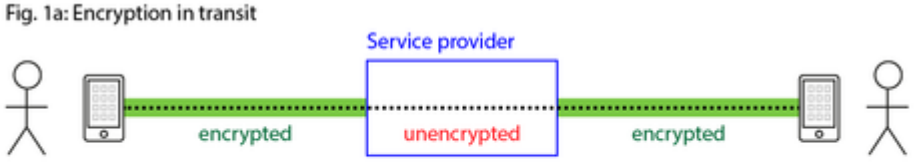


Fig. 1b: End-to-end encryption

Fig. 1c: End-to-end encryption (no service provider)

This is the goal of end-to-end encryption: drawing a new and ineradicable line in the digital sand dividing *your* data and *their* data. It allows you to trust a service provider to *store* your data without granting them any ability to *understand* it. This would mean that even Apple itself could no longer be expected to rummage through your iCloud account with its grabby little raccoon hands—and therefore could not be expected to hand it over to any government that can stamp a sheet of paper, which is precisely why the FBI (again: secretly) complained.

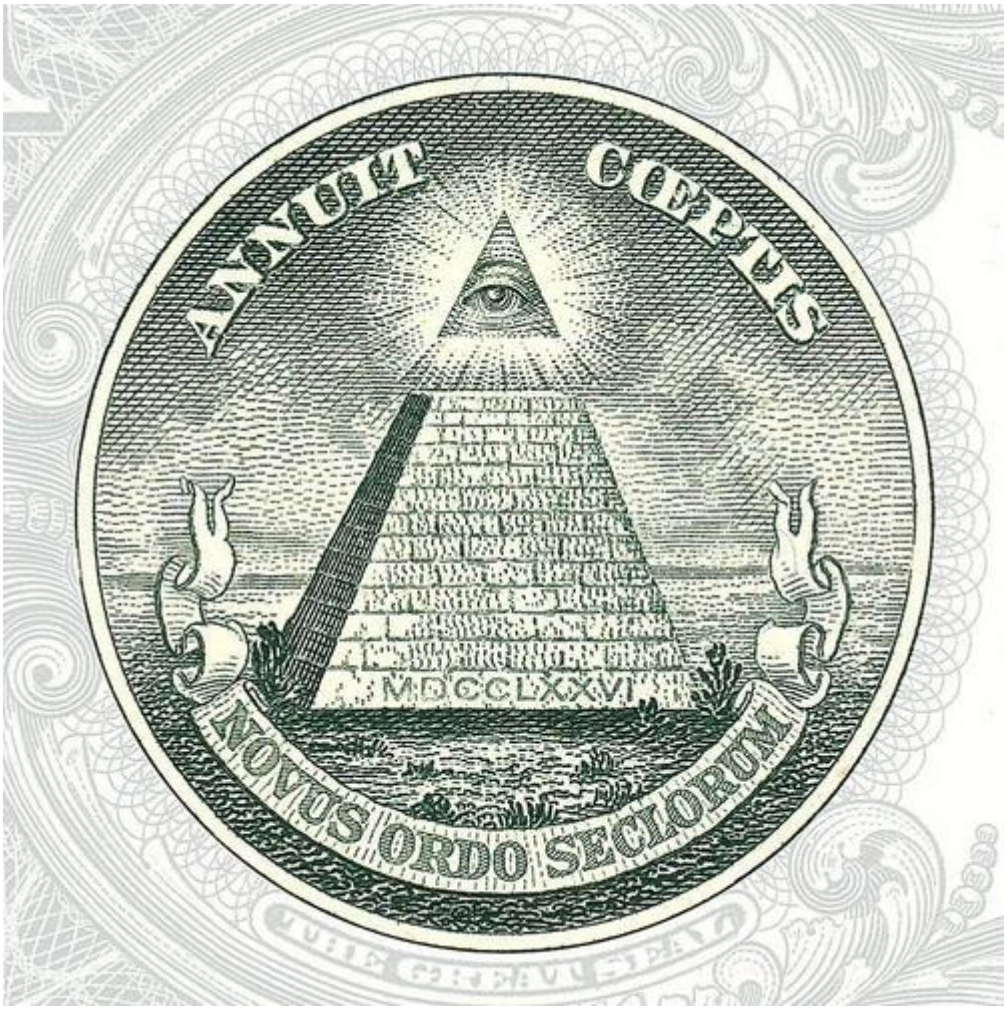
For Apple to realize this original vision would have represented a *huge* improvement in the privacy of our devices, effectively delivering the final word in a thirty year-long debate over establishing a new industry standard—and, by extension, the new global expectation that parties seeking access to data from a device must *obtain it* from that device, rather than turning the internet and its ecosystem into a spy machine.

Unfortunately, I am here to report that once again, the optimists are wrong: Apple's proposal to make their phones inform on and betray their owners marks the dawn of a dark future, one to be written in

the blood of the political opposition of a hundred countries that will exploit this system to the hilt. See, the day after this system goes live, it will no longer matter whether or not Apple ever enables end-to-end encryption, because our iPhones will be reporting their contents *before our keys are even used*.

I can't think of any other company that has so proudly, and so publicly, distributed spyware to its own devices—and I can't think of a threat more dangerous to a product's security than the mischief of its own maker. There is no fundamental technological limit to how far the precedent Apple is establishing can be pushed, meaning the only restraint is Apple's all-too-flexible company policy, something governments understand all too well.

I would say there should be a law, but I fear it would only make things worse.



We are bearing witness to the construction of an all-seeing-**i**—an Eye of *Im*providence—under whose aegis *every iPhone will search itself* for whatever Apple wants, or for whatever Apple is directed to want. They are inventing a world in which every product you purchase owes its highest loyalty to someone other than its owner.

To put it bluntly, this is not an innovation but a tragedy, a disaster-in-the-making.

Authored by Edward Snowden via Continuing Ed,

Date Created
09/07/2021