Opening the Surveillance Floodgates

This article is from the "Edifying the Body" section of the Church of God Big Sandy's website, churchofgodbigsandy.com. It was posted for the weekend of Aug. 14, 2021. (A version of the article was posted at cnsnews.com on Aug. 11.)

By Julian Sanchez

RESTON, Va.—In recent years, Apple has sought to brand itself as a strong defender of user privacy, boasting that it doesn't need to monetize your personal data—since its business model is based on selling pricey hardware—and admirably fighting off government pressure to weaken or break strong encryption on its devices. That's why it's so alarming to see the Cupertino-based tech giant has decided that a shockingly misguided surveillance apparatus will soon be built right into the company's widely used operating systems.

Laudable goal, dangerous repercussions

Apple in early August announced two major updates coming soon to its iOS, iPadOS, and macOS operating systems. Both have an unimpeachably laudable goal: fighting the spread of Child Sexual Abuse Material (CSAM) and victimization of children by online predators. But at least one of the two represents an extraordinarily dangerous idea that will be a dream come true for repressive regimes: that personal computing devices should be designed to spy on their users' activity—and report it to the authorities.

Since I've seen the two very different systems Apple announced conflated in some of the public reactions, it's worth distinguishing them briefly.

- First, Apple announced an optional parental control feature for its Messages app.

When activated, the app will scan messages sent on the device using machine learning algorithms to detect what it believes may be nude images. The child will see a notice that the message they are about to view may contain explicit content, and if they nevertheless choose to view it, a notification with a blurred copy will be sent to the parent. While I am not wildly enamored of training children to be accustomed to digital surveillance as a parenting strategy—especially when it runs the risk of outing gay or gender nonconforming teens to their parents before they are ready—this is not the truly dangerous tool. Parents who are inclined to do so already have plenty of options for installing spyware on their kids' devices, and failing that can usually just take the device and look through it.

- The really dangerous tool is the second one Apple announced—its "CSAM detection" system.

This one operates, not by attempting to detect nudity in novel images but by scanning the user's Photo Library for matches against a table of "hash values" of known child abuse images maintained by the National Center for Missing and Exploited Children (NCMEC). (A "hash value" is a short string derived by running a larger file through a mathematical algorithm, and routinely used to quickly determine whether two files are identical.)

If a certain "threshhold" of matches is reached—indicating a collection of child abuse imagery—the device notifies Apple, which in turn reports the user to NCMEC (and, by extension, the authorities). At least initially, this scan will only run on photos that have been designated for backup to Apple's iCloud service—which is to say photos that the user had already chosen to "share" with Apple.

This is, however, a design choice rather than a technical limitation: The system could easily be altered to scan all images in the library—and, for that matter, to scan for matches to content other than child abuse images. As with the parental control tool for Messages, this system of "Client Side Scanning" circumvents any encryption that may protect files in transit by running the scans on the device itself, where the files are unencrypted while the device is unlocked.

Pinpoint search

Apple's tool is based on an idea I called the "Pinpoint Search" (or "Zipless Search") in a cover story I wrote for *Reason* more than a decade ago: a method of "searching" for illegal activity that *only* reveals the presence or absence of illicit material, without incidentally revealing other private information, in the way a traditional physical search would. If catching pedophiles who traffic in images of child abuse were the only way such a system could be deployed, it might be difficult to object to in principle.

The trouble is that the algorithm doesn't know or care what sort of files it's looking for. The same architecture that looks for images of child abuse could just as easily search for copyrighted material or memes that ridicule government officials. North Korea's authoritarian regime already uses a similar system—mandated on all computing devices—to detect media the government considers "impure."

Surveillance program

Described more abstractly and content neutrally, here's what Apple is implementing: A surveillance program running on the user's personal device, outside the user's control, will scan the user's data for files on a list of prohibited content and then report to the authorities when it finds a certain amount of content on the list.

Once the architecture is in place, it is utterly inevitable that governments around the world will demand its use to search for other kinds of content—and to exert pressure on other device manufacturers to install similar surveillance systems.

Apple is, of course, already under significant government pressure to weaken encryption for the convenience of law enforcement—and this announcement is doubtless an attempt to relieve that pressure by demonstrating that the company is dedicated to combating a particularly loathsome misuse of its products. Companies like Facebook, after all, routinely scan the unencrypted

messages stored on their platform for CSAM, and it would not be surprising if this were a step toward resuming the plan—abandoned last year under FBI pressure—to store iCloud backups in an encrypted form.

Jeopardizing free society

From a strictly technical perspective, this approach probably does have fewer cybersecurity downsides than compromising encryption wholesale. From the point of view of privacy more broadly, however, this is at least equally dangerous. It is the endorsement by one of the largest industry players of the principle that ubiquitous spyware on consumer computing devices is normal and acceptable in free societies.

There are some more-mundane reasons to doubt the efficacy of these systems. Pedophiles and child abusers with a modicum of technical sophistication will quickly learn to shut off iCloud backups, or switch to other messaging applications. It's unclear yet how readily malicious actors may be able to deliberately create false positive reports by crafting innocuous looking images that yield "hash collisions" tricking the system into thinking it's found CSAM.

A scanning system implemented at the OS level with administrative privileges may be an attractive target for co-opting by other spyware, like the Pegasus tool deployed by many governments, which was recently found to have compromised the devices of numerous journalists and human-rights activists around the world.

Ultimately, however, these are secondary considerations. The core question is whether we wish to normalize the sale of personal-computing devices that come preinstalled with spyware outside the control of the user and owner, however noble the purpose to which that spyware is initially put. The answer free societies have given to that question for the past five decades is the right one: No.