Published on *The National Law Review* https://natlawreview.com

Will NeuralHash Make a Hash of Privacy?

Article By:

Theodore F. Claypoole

Our personal technology is so complex that making a change in one aspect is likely to affect us in many ways. When tech companies step into social issues, we are likely to see unintended consequences.

Apple announced this week introduction of new programs aimed at reducing incidences of child sexual abuse. This is an unquestionably laudable goal that we all support. However, some people question whether such affirmative social action is appropriate for computer companies, and others are concerned that the technology can be used for multiple purposes, eventually to expand into Apple policing less noxious user behavior in the future.

Apple's strategy includes a tool called "NeuralHash" that scans images prior to uploading the images to the cloud. If NeuralHash finds that a picture meets its criteria for child sexual abuse, then the user's account will be disabled and Apple will notify law enforcement and the Center for Missing and Exploited Children. The system is only supposed to call out images that match the Center's database of known child pornography, so new abuse photos will not be recognized and parents are in little danger from innocently photographing their own children. Apple claims that NeuralHash can match images despite alterations like cropping and colorization, and that the hashing system provides safeguards against false positive identifications.

In addition, Apple will also scan encrypted messages for sexually explicit content, and offer a service to parents that can identify issues and provide parental notice when their children send or receive any nude photos in text messages. No word on whether Apple will allow a phone account holder to be alerted and notified of nude photos in text messages for adults on the same Apple account. Divorce lawyers would likely be interested in this feature.

The goal behind these systems is saving children from abuse. However, Wired Magazine describes certain experts' reaction to the programs as "introducing new forms of privacy invasion" and "a dangerous capitulation to government surveillance." The Wired author writes, "Other cloud storage providers, from Microsoft to Dropbox, already perform detection on images uploaded to their servers. But by adding any sort of image analysis to user devices, some privacy critics argue, Apple has also taken a step toward a troubling new form of surveillance and weakened its historically strong privacy stance in the face of pressure from law enforcement."

Privacy advocates are concerned that once Apple places software on your phone that scans for child

abuse and notifies police, that governments will pressure Apple to scan your phone for more political content, which would be provided to the government. In a world where China has instituted a dystopic surveillance society and other countries would like to do the same, knowing that Apple phones scan the pictures you take or send makes people worry. China could demand Apple provide political information, or it could hijack the tool and bypass Apple's consent to grab political data of dissidents.

In a world where China has instituted a dystopic surveillance society and other countries would like to do the same, knowing that Apple phones scan the pictures you take or send makes people worry.

Also, in a world where people harass their adversaries by sending SWAT teams to their homes, the new Apple tools could be turned against phone owners. The Washington Post reports, "Matthew Green, a top cryptography researcher at Johns Hopkins University, warned that the system could be used to frame innocent people by sending them seemingly innocuous images designed to trigger matches for child pornography. That could fool Apple's algorithm and alert law enforcement. 'Researchers have been able to do this pretty easily,' he said of the ability to trick such systems." So don't offend any sophisticated tech workers or you could find yourself at the center of a child abuse investigation with no basis in fact.

A few of the experts interviewed in the press about this program suggested that this is a preliminary step to Apple introducing full end-to-end encryption through its hardware and cloud platforms. Law enforcement has been pushing back against that step for years, but knowing that Apple provides a window into its encrypted world may blunt the opposition. End-to-end encryption is the holy grail for privacy advocates, but building this window into the system blunts its privacy effect.

There is history on the internet of implementing change on behalf of a good cause, only to see problematic, unintended consequences. In the summer of 2018 the federal government passed a set of anti-sex trafficking laws known as FOSTA/SESTA, which among other provisions, removed the safe harbor provision of Section 230 of the Communications Decency Act for online advertisements for prostitution. This provision led to Craig's List and many other online fora removing sexually related advertisements for local publication, cleaning up this corner of the internet that many people found to be unsavory.

There is history on the internet of implementing change on behalf of a good cause, only to see problematic, unintended consequences.

What could be wrong with that? According to the Business Insider, "The law … has been an abject failure. It hasn't done what it set out to do, fight sex trafficking, and instead has made the lives of sex workers, the very people the law hoped to protect, more dangerous. FOSTA-SESTA holds websites accountable for any sex work facilitated on their platforms. Sex workers can no longer share information or warn each other away from violent clients." The Daily Beast reported that the law forces sex workers back out to the street and endangers their lives. It discussed a 2017 study that found internet advertising of sex work led to a 17.4% reduction in the female homicide rate.

Similarly, Apple's recent announcement may help fight child sexual abuse, but it also creates a giant hole in Apple's device security which could be used for other purposes, including watching private adult conversations and crushing political dissent. I am not passing judgment on Apple's decision to institute the new system on its smartphones, but we should try to understand the consequences to device users – intended or otherwise. We should be careful when unassailable purposes – like protecting children from abuse – can lead to broader losses of privacy later.

Copyright © 2025 Womble Bond Dickinson (US) LLP All Rights Reserved.

National Law Review, Volume XI, Number 222

Source URL:https://natlawreview.com/article/will-neuralhash-make-hash-privacy