Carriers reject kill switch for stolen smartphones (Update)

November 19 2013, by Terry Collins

Samsung Electronics, the world's largest mobile phone manufacturer, has proposed installing a built-in anti-theft measure known as a "kill switch" that would render stolen or lost phones inoperable, but the biggest U.S. carriers have rejected the idea, according to San Francisco's top prosecutor.

District Attorney George Gascon said Monday that AT&T Inc., Verizon Wireless, United States Cellular Corp., Sprint Corp. and T-Mobile US Inc. rebuffed Samsung's proposal to preload its phones with Absolute LoJack anti-theft software as a standard feature.

The wireless industry says a kill switch isn't the answer because it could allow a hacker to disable someone's phone.

Gascon, New York Attorney General Eric Schneiderman and other law enforcement officials have been demanding that manufacturers create kill switches to combat surging smartphone theft across the country.

Almost 1 in 3 U.S. robberies involve phone theft, according to the Federal Communications Commission. Lost and stolen mobile devices—mostly smartphones—cost consumers more than $30 billion last year, according to a study cited by Schneiderman in June.

Samsung officials told the San Francisco district attorney's office in July that carriers were resisting kill switches, and prosecutors have recently reviewed emails between a senior vice president at Samsung and a

software developer about the issue. One email in August said Samsung had pre-installed kill switch software in some smartphones ready for shipment, but carriers ordered their removal as a standard feature.

"These emails suggest that the carriers are rejecting a technological solution so they can continue to shake down their customers for billions of dollars in (theft) insurance premiums," Gascon said. "I'm incensed. ... This is a solution that has the potential to end the victimization of their customers."

Samsung said it is cooperating with Gascon, Schneiderman and the carriers on an anti-theft solution but declined to comment specifically about the emails.

"We are working with the leaders of the Secure Our Smartphones (SOS) Initiative to incorporate the perspective of law enforcement agencies," said Samsung spokeswoman Jessica Redman. "We will continue to work with them and our wireless carrier partners toward our common goal of stopping smartphone theft."

Although the popular Samsung Galaxy smartphones are shipped across the country without LoJack as a standard feature, users can pay a subscription fee for the service.

CTIA-The Wireless Association, a trade group for wireless providers, said it has been working with the FCC, law enforcement agencies and elected officials on a national stolen phone database scheduled to launch Nov. 30.

The CTIA says a permanent kill switch has serious risks, including potential vulnerability to hackers who could disable mobile devices and lock out not only individuals' phones but also phones used by entities such as the Department of Defense, Homeland Security and law

enforcement agencies.

"The problem is how do you trigger a kill switch in a secure manner and not be compromised by a third party and be subjected to hacking," said James Moran, a security adviser with the GSMA, a United Kingdom wireless trade group that has overseen a global stolen mobile phone database and is helping to create the U.S. version.

Last year, about 121 million smartphones were sold in the U.S., according to International Data Corp., a Massachusetts-based researcher. About 725 million smartphones were sold worldwide, accounting for $281 billion in sales, IDC said.

Samsung Electronics Co., with its popular Galaxy S4 smartphone, shipped 81 million phones—more than the next four manufacturers combined—during the most recent sales quarter for a market share of 31 percent, IDC reported in October. Apple Inc. shipped 34 million iPhones for a market share of 13 percent.

In June, Gascon and Schneiderman held a "Smartphone Summit" in New York City to call on representatives from smartphone makers Apple, Samsung, Google Inc. and Microsoft Corp. to adopt kill switches that would be free to consumers.

That week, Apple said such a feature, an "activation lock," would be part of its iOS 7 software that was eventually released this fall. The new activation lock feature is designed to prevent thieves from turning off the Find My iPhone application, which allows owners to track their phone on a map, remotely lock the device and delete its data.

The activation lock requires someone to know the user's Apple ID and password to reactivate a phone, even after all the data on the device is erased.

In July, prosecutors brought federal and state security experts to San Francisco to test Apple's iPhone 5 with its activation lock and Samsung's Galaxy S4 with LoJack.

Treating the phones as if they were stolen, experts tried to circumvent their anti-theft features to evaluate their effectiveness, and that work is continuing.

One Silicon Valley technology security expert said he thinks Apple's activation lock is the first kill switch that meets law enforcement's desire to protect iPhone users and other smartphone manufacturers should follow suit.

"Thieves cannot do anything with the device unless they have the user's ID, which they don't," said Ojas Rege, vice president of strategy at Mobile Iron, a technology software security company in Mountain View, California.

"The activation lock addresses this issue without the carriers having to do anything," Rege said, adding that he does not believe resistance to implementing kill switch technology is fueled by profits.

"That is not the number one priority for manufacturers. They're driven by creating the next great feature for their smartphones," he said.