'Kill Switch' bill passes in California

By Steve Watson | Infowars.com
All phones sold in the State will be mandated to integrate controversial technology
Legislation introduced to the Californian Senate earlier this year mandating ?kill switches' on all smart phones has been passed and sent to the Governor's desk for approval.

Governor Jerry Brown is expected to sign bill CA SB 962 in the coming weeks, meaning that it will be against the law for any supplier or carrier in the State to sell a mobile phone that is not fitted with the technology.

Manufacturers will have until July 1, 2015 to ensure that all their phones are equipped with the means to ?render the essential features of the smartphone inoperable when not in the possession of the authorized user.?

The legislation, introduced in February, passed on a vote of 53-20.

Although the owner would have the option to disable the function under the language of the bill, many will likely believe it is essential, as users will be prompted to enable the feature upon initial setup of the device.

The bill also states that manufacturers must fit technology that will prevent phones from being re-activated on any network without the owner's approval. Phones must also be fitted with the ability to be reactivated, should they be returned to the rightful owner. Under the legislation, the State will levy penalties of between $500 and $2,500 on anyone discovered to be selling stolen phones.

While police departments and city officials have expressed support for the legislation, some manufacturers and rights groups have issued warnings regarding the move.

They suggest that while the ?kill switch' would ostensibly be included to discourage theft, it could also be ?exploited by malicious actors? as the Electronic Frontier Foundation explained in a letter written in June.

It is not difficult to envisage a scenario where authorities could hijack the technology to shut down communications in a sensitive area in order to limit photo and streaming video coverage, such as at a demonstration or at the scene of unfolding police brutality.

Infowars has previously reported on a Google patent for a system that would alert law enforcement authorities if a number of photos were taken in one specific location by smartphone users, raising questions as to what level of remote access companies like Google should have to people's personal devices.

Back in 2012, Apple also filed a patent allowing it to wirelessly disable cameras on iPhones by ?forcing certain electronic devices to enter ?sleep mode? when entering a sensitive area.?

The patent was registered in anticipation of giving police or government the power to impose a ?blackout? on all communications during certain times because cellphones can ?annoy, frustrate, and even threaten people in sensitive venues.?

The Californian bill is also likely to become a de facto national law, not only because it is the largest state in the US, but also because phone manufacturers are unlikely to spend more money tailoring just portions of their products to different states. It is much more likely that ALL phones will be fitted with the technology, in preparation for the technology becoming mandated elsewhere.

Indeed, in June, it was reported that Google and Microsoft have agreed to include kill switches in all new Android and Windows phones.

?Google, based in Mountain View, California, said in a statement today it will add a ?factory reset protection solution? to its next version of Android,? reported Bloomberg. ?Microsoft's Vice President for U.S. Government Affairs Fred Humphries said the Redmond, Washington-based company will offer new theft-deterrence mechanisms in an update for phones running its software, including those made by Nokia Oyj.?

The technology is also set to be implemented into computers and laptops. with NSA linked corporation IBM heading up the move.

The idea of companies, government officials and police having access to a ?kill switch? with no opt out process takes power away from the individual and leaves the door ajar for so called authorities to exploit such technology to target anything they perceive as dissent.

In a post-Snowden era, the idea of such entities having remote access to computers and mobile phones, which are used in every aspect of everyday life, represents a potential Pandora's Box of privacy violation.

This article originally appeared on Infowars.com.