wiley

NEWSLETTER

Varied "Kill Switch" Legislation Could Balkanize National Mobile Device Markets

March 2014

Concerns about mobile device theft are leading to consideration across the nation of legislation to mandate incorporating "kill switches" in a variety of wireless devices. These proposals are deceptively simple-sounding, but could have much broader impacts than many companies recognize.

A variety of proposals abound. Some are focused more on wireless carriers, and others on device manufacturers, and sellers more broadly. But all could directly or indirectly impact manufacturers, refurbishers, and retailers of a variety of consumer products. They may apply to smartphones, tablets, laptops, and virtually any connected devices in the so-called "Internet of Things"—potentially any device or connected, mobile consumer good that relies on computing and stores data.

At the federal level, Sen. Amy Klobuchar (D-MN) last month introduced SB 2032, the "Smartphone Theft Prevention Act" (STPA). The same bill also was introduced in the House of Representatives by Rep. Jose Serrano (D-NY) as HR 4065. It targets wireless carriers and manufacturers of smartphones and would require "a provider of commercial mobile service or commercial mobile data service" to "make available" functionalities to remotely lock, disable, and/or wipe a device—even when the device is turned off—and also allow for the device to operate again if the device owner reclaimed the device. In addition, manufacturers would be forbidden from domestically manufacturing or importing for use in the U.S. noncompliant devices. The law would take effect January 1, 2015, and noncompliant entities would be subject to a forfeiture penalty to be set by the Federal Communications Commission (FCC).

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Henry Gola
Partner
202.719.7561
hgola@wiley.law

Practice Areas

Internet of Things

Similar legislation is being considered in California, Illinois, New York, and Minnesota. Minnesota's H.F. 1952 would impose joint and several liability on manufacturers and sellers of devices that do not comply with "kill switch" mandates. In addition, Minnesota's bill and Illinois's SB 3539 would mandate that carriers provide free theft insurance. Both New York's S-6748 and California's SB-962 would levy civil fines for selling non-compliant devices, with S-6748 allowing penalties for "a pattern or practice" of violations of up to $3,000 per violation, plus attorneys' fees.

The reach of these bills could be sweeping, as some define "smartphone" or other covered devices broadly, potentially covering a variety of devices built on mobile operating systems. This legislation thus could reach far beyond iPhones and Android devices and impact such devices as appliances and automobiles.

Moreover, the bills' divergent approaches would pose significant implementation and compliance challenges. For example, inconsistent technical specifications at the state or federal level could complicate innovation and balkanize the national market for mobile devices and services, which is marked by national development, manufacturing, and distribution. Companies may find compliance difficult or impossible.

Some question the need for legislation or regulation at all, urging reliance on market forces and criminal law enforcement. An alternative approach to addressing device theft has been promoted by CTIA–The Wireless Association. In November, it announced the completion of a global, multicarrier stolen phone database with which users can contact their participating wireless providers and report their device stolen. Providers can then blacklist the device and prevent it from being reactivated.

But despite industry efforts, interest in legislative and regulatory solutions is likely to continue. Companies involved in the design, manufacture, and servicing of mobile consumer goods should monitor these bills, which, if successful, threaten to impose complex and potentially varied compliance challenges.