‘Kill Switch’ Has Merit in Theory More Than in Practice

Ben Munson

The debate whether Congress is over-reaching with proposed mandatory cell phone ‘kill switch’ technology [1] is important to consumers. Auto installing such a devastating nuclear option in people’s cell phones presents a real danger to personal—maybe sensitive, likely meaningful—information. Not to mention if the wrong hands get a hold of a device’s self-destruct button, the owner could be left with no form of communication.

But in the rush to push back against that required theft deterrent, it’s important to recognize how effective a threat deterrent it could be. Maybe not in practice, but definitely in theory. If a potential cell phone thief knows that the device will be rendered useless after they snatch it, it really throws the whole risk-reward thing out of balance.

We’re talking about a cell phone, an item people can and once did live without. And we’re talking about a protective measure that could possibly prevent a crime with the potential to turn violent.

Perhaps there’s a middle ground. GM’s OnStar in-vehicle communications and safety service has for more than five years offered a function that slows down a car that’s been reported stolen [2]. That doesn’t necessarily prevent car theft—though as awareness builds it might—but it can help to mitigate the chance for injury and damage following a theft. Maybe carriers could disable all but 2G connectivity in a stolen smartphone? The only thing worse than a smartphone that doesn’t work at all is one connected to 2G. And like OnStar, it could be subscription-based, meaning carriers could monetize the service. If Congress had a plan for monetizing mandatory kill switches, we probably wouldn’t be having this conversation.

U.S. carriers have working theft-deterrent alternatives like databases that help prevent stolen devices from being activated on other networks. And OEMs have made remote wipe capabilities available. But if the FCC’s numbers are accurate, smartphone owners are still inordinately targeted by thieves.

It’s likely that legislation forcing OEMs to install kill switches inside of cell phones is stepping over the line. But couldn’t a high-profile national campaign to bake self-destruct buttons into all the phones in the country put thieves on alert? If so, it could prevent people from being robbed and possibly assaulted. I think at least the legislation’s heart is in the right place and hopefully that might move the industry closer to a solution that keeps consumers safer.

Source URL (retrieved on *11/29/2014 - 1:25am*):
http://www.wirelessweek.com/blogs/2014/03/%E2%80%98kill-switch%E2%80%99-has-merit-theory-more-practice

Links:
[1] http://www.wirelessweek.com/blogs/2014/03/hasty-%E2%80%98kill-switch%E2%80%99-legislation-has-flaws
[2] https://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2013/Oct/1008-onstar.html