KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

March 14, 2014

Committee on Commerce and Consumer
Protection Finance and Policy
Minnesota House of Representatives
100 Rev. Dr. Martin Luther King Jr. Blvd.
Saint Paul, MN 55155

Dear Chair Atkins, Vice Chair Fritz, Representative Hoppe,
and Members of the Committee on Commerce and
Consumer Protection Finance and Policy,

The Center for Democracy & Technology writes to express concern regarding the implications of mandatory "kill switch" legislation, and HF 1952 in particular.[1]

We oppose passage of such legislation for the following reasons:

Kill Switch Applications Are Already Widely Available to Mobile Device Users, Making a Legislative Mandate Unnecessary

Smartphone theft is a serious problem across the United States. According to the Federal Communications Commission, theft of mobile devices accounts for one of every three robberies in the United States and costs consumers over $30,000,000,000 per year.

The presence of kill switches – which can render a stolen phone inoperable and thus worthless on the black market – can reduce the frequency of smartphone theft. However, the kill switch function is already widely available to consumers, making a legislative mandate unnecessary. For example, Apple currently includes in all new devices a Find My Phone feature[2] that allows users to go online to locate a missing or stolen phone, erase all data from it, and lock it down. A host of third party applications with similar features are available for other mobile devices. According to the CTIA, there are over 30 companies that provide applications giving consumers the capacity to remotely lock down a stolen Android or Blackberry device.[3] T-Mobile, for example, has partnered with one

[1] CDT is a non-profit, non-partisan public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the Internet. One of our priorities is to expand the rights of consumers online.

[2] For details on the functionality of this application, visit http://www.apple.com/icloud/find-my-iphone.html.

[3] CTIA, Anti Theft and Loss Protection Apps for Wireless Handsets (March 23, 2012), *available at* http://blog.ctia.org/2012/03/23/data-theft-protection-apps-for-wireless-handsets-2/.

such company, Lookout, to preinstall its anti-theft software in new devices.

In addition, cellular network operators have created a system to globally blacklist stolen cell phones, such that handsets added to the database will receive no service anywhere in the world.[4]

With these theft-response applications and features readily available, a kill switch mandate offers little to protect consumers and deter smartphone theft. However, it could result in a range of problems.

A Kill Switch Mandate Could Discourage Innovation

It is clear that the competitive marketplace has already developed and is continuing to innovate a range of responses to the epidemic of smartphone theft. Mandating installation of a kill switch through legislation could discourage the continued development of other innovative solutions and could actually "lock in" the use of less effective applications. While a range of application developers currently compete to develop more effective anti-theft technology and partner with manufacturers and wireless providers, a mandate might encourage companies to seek out the lowest common denominator now and reduce incentives to improve in the future.

Further, a statutory mandate with a short implementation period could force hasty adoption of less effective solutions. Requiring all device manufacturers and wireless providers to install a kill switch by the start of next year – as HF 1952 requires – could lead to sloppy technical hardware and software development.

Requiring a Kill Switch Could Create a Data Retention Mandate

HF 1952 requires that the proposed kill switch include the capacity to "wipe" a device of all stored data (Subd. 2(b)(1)) and also that device manufacturers and wireless providers be able to reverse such action if a device is recovered (Subd. 2(b)(5)). The bill does not define "wipe," which itself causes a problem. The dictionary definition of "wipe" is to "remove or eliminate (something) completely" or to "expunge," but in the case of digital data "wipe" could mean resetting the encryption key on the device so the data is completely inaccessible. The difference is significant. If "wipe" means "remove" or "expunge," that is highly difficult to actually do, and the only means of restoring data that have been fully deleted from a device would be for manufacturers and wireless providers to externally store all data for all mobile devices.

Such a data retention mandate would create significant privacy problems. A database of all mobile device data would be a prime target for hackers and clandestine operations of foreign governments. Further, such a database would be regularly subpoenaed for information by federal, state and local enforcement, as well as an endless stream of civil litigants. As a

[4] For example, in the case of relatively ubiquitous GSM cellular networks, the GSM Association maintains the International Mobile Equipment Identity (IMEI) Database, which is a list of unique equipment identifiers that are associated with mobile devices that should be denied service on mobile networks because they have been reported as lost, stolen, faulty or otherwise unsuitable for use. *See:* International Mobile Equipment Identity Database, GSM Association, available at: http://www.gsma.com/technicalprojects/fraud-security/imei-database (last visited 13 March 2013).

separate concern, the cost of building and maintaining such a database – let alone attempting to protect it from malicious actors – would be an enormous burden on companies.

A "Remote On-Switch" Could Become a Backdoor for Hackers or Government Surveillance

HF 1952 requires that a kill switch be able to disable a mobile device even if it is turned off (Subd. 2(b)(4)). It is our understanding that such a feature could only be accomplished through the installation of a "Remote On-Switch" in all new mobile devices. Requiring such a feature in mobile devices is disturbing, as it effectively mandates creation of a backdoor for hackers or for government surveillance. The mere act of turning on a phone can reveal sensitive private data about its owner, such as geolocation information (as one of the first functions a phone performs when it is turned on is to register with the cellular network via the closest cell tower). To require that device manufacturers and wireless providers install a "Remote On-Switch" – a necessary feature of remotely turning on a phone – would be to mandate all mobile devices be created with a backdoor which facilitates government surveillance or snooping by any malicious party that learns how to activate the "Remote On-Switch." Such a measure is deeply troubling from a privacy perspective and sets an unacceptable precedent for government manipulation of technology.

A Mandatory Kill Switch Could Be Co-Opted to Suppress Free Speech

HF 1952 does not require that the kill switch feature be designed in such a way that it can be activated only by the user. This leaves open the possibility that the mandatory kill switch could be co-opted by government officials to shut off phones en masse in order, for example, to disrupt a public protest. Although such an action seems grossly at odds with our rights to free speech, in 2011, officials in San Francisco shut down cell service at BART subway stations in an effort to suppress planned demonstrations. If someone other than the device's owner could activate a kill switch, a government could use it to disrupt free expression and association. Again, while this may seem unlikely in the United States, policymakers should recognize that the market for cell phones is global. If equipment makers were required to build in the capability for sale in the United States, it might be easiest for them to build the capability into all their phones, and the "Minnesota kill switch" could end up in phones sold in China and other rights abusing countries where governments might be much more likely shut down phones to suppress democratic activity.

Conclusion

Kill switch legislation is unnecessary in general, and in the case of HF 1952 poses serious risks to data security, privacy, and free speech. For these reasons, we urge the Committee to reject HF 1952, and any other kill switch legislation that would create risks to innovation and privacy without benefitting users.

Sincerely,

Jake Laperruque
Fellow on Privacy, Surveillance, and Security