ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

June 16, 2014

The Honorable Susan Bonilla
Chair, Assembly Business, Professions and Consumer Protection Committee
Legislative Office Building, Room 383
Sacramento, California 95814
Fax: (916) 319-3306

Re: SB 962 (Leno) – Oppose

Dear Assemblymember Bonilla,

The Electronic Frontier Foundation (EFF) is a non-profit member-supported civil liberties organization based in San Francisco, California, that works to protect rights in the digital world. EFF has more than 30,000 active donors across the country.

EFF respectfully opposes SB 962, a bill to mandate a so-called "kill switch" in smartphones manufactured sold in California. The bill attempts to address the serious problem of cell phone theft in the state by requiring smartphones to have an anti-theft solution that renders a device inoperable, but allows an "authorized user" to restore essential functionality.

We agree that anti-theft technical measures can play an important role in combating smartphone theft. But mandating a solution through legislation is not the right approach.

First, these technological measures already exist. Apple phones, for example, already have a Find My iPhone feature, and various other companies provide solutions for Android, Blackberry, and iOS phones (e.g. Lookout, Prey, Avast Mobile Security, and over 30 more).[1] Because of this hefty range of options already available for consumers, mandating a solution presents a host of problems. With an eye to the current landscape of security tools, if a "manufacturer or operating system provider" chooses a particular solution, innovation in this space may be discouraged—especially since the current number of "manufacturers or operating system providers" falls short of the number of security tools. Mandating any technological fix could "lock in" a less effective solution, preventing stronger third-party anti-theft applications from competing and innovating.

Second, such security solutions have a basic premise: allow the proper user of the phone to remotely activate the "kill switch" in order to render the phone unusable (barring basic emergency calls). But SB 962 is not explicit about *who* can activate such a switch. And more critically, the solution will be available for others to exploit as well, including malicious actors or law enforcement. While SB 962 adopts the requirements of Public Utilities Code § 7908 to regulate and limit the circumstances in which government and law enforcement officials can activate the "kill switch," the fact remains that the presence of such a mechanism in every phone by default would not be available but for the existence of the kill switch bill. In essence, SB 962 mandates the technical ability to disable every phone sold in California, and PUC § 7908

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

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

provides the necessary legal roadmap to do the same. Within two years, we would have legitimized a process that was seen to be quite extreme. While users have the ability to opt-out of such a tool, it is widely known that default settings are rarely changed.

Because it is difficult to implement a "kill switch" that can only be utilized at the behest of the device user but not third parties or the government, EFF strongly believes the state should not mandate this backdoor be installed into phones in California. Hence, we respectfully oppose SB 962.

Sincerely,

Hanni Fakhoury
Staff Attorney
Electronic Frontier Foundation

Adi Kamdar
Activist
Electronic Frontier Foundation

Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation