

SUMMARY—Requires certain cellular telephones sold in Nevada to be equipped with “kill-switch” antitheft technology. (BDR 52-471)

FISCAL NOTE: Effect on Local Government: No.

Effect on the State: Yes.

AN ACT relating to telecommunications; requiring certain cellular telephones that are sold in Nevada to be equipped with “kill-switch” antitheft technology; providing a penalty; and providing other matters properly relating thereto.

Legislative Counsel’s Digest:

“Kill-switch” antitheft technology is technology by which a “smart” cellular telephone (smartphone) may have its essential features disabled in the event of theft. **Section 9** of this bill requires that kill-switch antitheft technology be included in certain smartphones sold in Nevada on or after July 1, 2015. In addition, **section 9** requires that the kill-switch technology be enabled as a factory default setting of the smartphone; however, it must allow an authorized user of the smartphone to disable the kill-switch technology if they so choose. **Section 10** of this bill exempts certain secondhand sales of smartphones from the requirement to include kill-switch technology. **Section 11** of this bill provides for a civil penalty to be imposed for a violation of the requirement to include kill-switch technology, and grants to the Attorney General, district attorneys and city attorneys the exclusive right to bring an action to enforce the civil penalty.



Section 12 of this bill grants to distributors and retailers of smartphones limited immunity from civil liability in instances where the kill-switch technology failed to work as the result of third-party intervention, commonly known as hacking. **Sections 13 and 14** of this bill require a government official who desires to use kill-switch technology to disable the essential features of a smartphone to first obtain a court order authorizing such action, unless there exists an extreme emergency that threatens death or severe bodily injury to members of the public. **Section 15** of this bill limits the civil liability of manufacturers of smartphones and providers of wireless telecommunications who use kill-switch technology to disable the essential features of a smartphone in good-faith reliance upon a request from a governmental agency or official. **Section 17** of this bill prohibits a local governmental entity from enacting an ordinance relating to any subject covered by the provisions of this bill.

WHEREAS, The Federal Communications Commission has estimated that smartphones are now involved in approximately 30 to 40 percent of robberies that occur in many major cities across the country; and

WHEREAS, Many such robberies can become violent, sometimes resulting in the loss of life; and

WHEREAS, *Consumer Reports* estimates that 3.1 million Americans were victims of smartphone theft in 2013; and



WHEREAS, The *New York Times* has reported that 113 smartphones are lost or stolen each minute in the United States; and

WHEREAS, Various press reports indicate that the international trafficking of stolen smartphones by organized criminal groups has grown exponentially in recent years due to the highly profitable nature of the trade in stolen smartphones; and

WHEREAS, To be effective, antitheft technological solutions need to be ubiquitous, so that potential smartphone thieves cannot distinguish between smartphones that possess such technology and those that do not; and

WHEREAS, Any antitheft technological solution must be able to withstand a hard reset or operating system downgrade and be provided as a standard, default feature of the smartphone; and

WHEREAS, In the interest of providing maximum choices to consumers, any antitheft technological solution should provide to the consumer the option to voluntarily disable the technology after being fully informed of the risks of doing so; now, therefore,

THE PEOPLE OF THE STATE OF NEVADA, REPRESENTED IN
SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

Section 1. Chapter 597 of NRS is hereby amended by adding thereto the provisions set forth as sections 2 to 17, inclusive, of this act.



Sec. 2. As used in sections 2 to 17, inclusive, of this act, unless the context otherwise requires, the words and terms defined in sections 3 to 8, inclusive, of this act have the meanings ascribed to them in those sections.

Sec. 3. “Authorized user” means a person who:

- 1. Owns a smartphone;*
- 2. Possesses a smartphone lawfully pursuant to a lease, agreement for service or other contractual agreement with the owner of the smartphone or a provider of wireless telecommunications; or*
- 3. Possesses or uses a smartphone with the express permission of a person described in subsection 1 or 2.*

Sec. 4. “Essential features” means the features of a smartphone which allow the smartphone to be used for:

- 1. Voice communications, including, without limitation, digital voice service;*
- 2. Text messaging;*
- 3. Browsing the Internet; and*
- 4. Accessing and operating mobile software applications.*

Sec. 5. “Hard reset” means the restoration of a smartphone to its state when it was originally manufactured.

Sec. 6. “Kill-switch technology” means a technological feature which, once initiated by an authorized user of a smartphone, renders the essential features of the smartphone inoperable to a person who is not an authorized user of the smartphone.



Sec. 7. “Provider of wireless telecommunications” has the meaning ascribed to it in NRS 707.620.

Sec. 8. 1. “Smartphone” means a handheld device for wireless telecommunications which utilizes a mobile operating system and which:

(a) Possesses the capability to:

(1) Utilize mobile software applications;

(2) Access and browse the Internet;

(3) Send and receive text messages;

(4) Utilize digital voice service; and

(5) Send and receive electronic mail;

(b) Has wireless network connectivity; and

(c) Is capable of operating on a long-term evolution network, or a successor standard for wireless telecommunications of high-speed data for mobile devices.

2. The term does not include:

(a) A tablet computing device;

(b) A laptop computer;

(c) An electronic reader that is designed exclusively for downloading and reading books and other texts; or

(d) A cellular telephone that does not possess all the features of a smartphone described in subsection 1.



Sec. 9. 1. Except as otherwise provided in section 10 of this act, a smartphone manufactured on or after July 1, 2015, and sold within this State, must include kill-switch technology. Such kill-switch technology must include, without limitation:

(a) The ability of an authorized user of a smartphone to remotely render the essential features of the smartphone inoperable to a person who is not an authorized user of the smartphone, while retaining the ability of the smartphone to:

(1) Access emergency services by calling or sending a text message to a 911 operator;

(2) Receive wireless emergency alerts and warnings; and

(3) Call an emergency phone number that has been predesignated by an authorized user of the smartphone;

(b) The ability to withstand a hard reset or operating system downgrade attempted by a person who is not an authorized user of the smartphone;

(c) The ability to prevent, once the kill-switch technology has been activated, the reactivation of the smartphone on a wireless network by a person who is not an authorized user of the smartphone; and

(d) The ability of an authorized user of the smartphone to restore the essential features of the smartphone.

2. The kill-switch technology described in this section must be enabled automatically at the time the smartphone is purchased and activated for use and must include, without limitation, the ability of an authorized user of the smartphone to voluntarily disable the kill-



switch technology, after affirmatively verifying the identity of the authorized user through the use of a password or other unique identifier.

3. The smartphone must be designed to provide to an authorized user of the smartphone, a warning of the consequences and risks associated with disabling the kill-switch technology.

Sec. 10. *The provisions of section 9 of this act do not apply to:*

1. The resale of a smartphone by an original end-user consumer or successor in title to an original end-user consumer.

2. The sale of a smartphone by the holder of a debt for which the smartphone has been pledged as security.

3. The sale of a model of smartphone that was introduced on the market before July 1, 2015, and cannot reasonably be reengineered or updated to include kill-switch technology.

Sec. 11. *1. A manufacturer, distributor or retailer of smartphones who knowingly violates the provisions of sections 2 to 17, inclusive, of this act is subject to a civil penalty of not less than \$500 or more than \$2,500 per violation.*

2. A distributor or retailer of smartphones is not subject to the civil penalty pursuant to this section for the failure of the kill-switch technology to operate as required pursuant to section 9 of this act as a result of alteration or circumvention by a third-party unless, at the time of the sale of the smartphone, the manufacturer had previously notified such retailer or distributor that:

(a) The smartphone was vulnerable to such failure; and

(b) No technological solution exists to eliminate or cure the risk of such failure.



3. *An action brought to enforce the provisions of sections 2 to 17, inclusive, of this act may be brought by the Attorney General, a district attorney or a city attorney.*

4. *Nothing in this section creates a private right of action against any manufacturer, distributor or retailer of smartphones for a violation of the provisions of sections 2 to 17, inclusive, of this act.*

Sec. 12. *1. A distributor or retailer of smartphones, or any employee or agent of a distributor or retailer of smartphones, does not incur any civil liability resulting from the failure of kill-switch technology to operate as designed, including, without limitation, any failure resulting from alteration or circumvention by a third party, unless, at the time of the sale of the smartphone, the manufacturer had previously notified the retailer or distributor that:*

(a) The smartphone was vulnerable to such failure; and

(b) No technological solution exists to eliminate or cure the risk of such failure.

2. Nothing in this section shall be construed as precluding a civil suit for damages against a distributor or retailer of smartphones, or any employee or agent of a distributor or retailer of smartphones, on any other basis, including, without limitation, a suit alleging a claim of false advertising.

Sec. 13. *1. Except as otherwise provided in section 14 of this act, a request by an employee, agent or officer of a state or local governmental agency to a manufacturer of a smartphone or a provider of wireless telecommunications to use the kill-switch technology installed on a smartphone to disable the essential features of the smartphone must be*



accompanied by an order issued by a court or magistrate that includes, without limitation, the following findings:

(a) That probable cause exists that the smartphone is being, or will be, used for an unlawful purpose or to assist in the violation of the law;

(b) That absent immediate and summary action to disable the essential features of the smartphone, a serious, direct and immediate danger to the public health, safety or welfare will result; and

(c) That the disabling of the essential features of the smartphone is narrowly tailored to prevent the unlawful infringement of speech that is protected by the Constitution or laws of the United States or the Constitution or laws of Nevada.

2. Any order issued by a court or magistrate pursuant to this section must be narrowly tailored to the specific circumstances under which the order is made and must not interfere with more communications than is necessary to achieve the purpose of the order. In addition, the order must:

(a) Authorize the disabling of the essential features of the smartphone only for the length of time that is reasonably necessary; and

(b) Require that the disabling of the essential features of the smartphone cease after the danger specified in the order is abated.

Sec. 14. *Notwithstanding the provisions of section 13 of this act, an employee, agent or officer of a state or local governmental agency may request that a manufacturer of a smartphone or a provider of wireless telecommunications use the kill-switch technology*



installed on a smartphone to disable the essential features of the smartphone without first obtaining an order from a court or magistrate pursuant to section 13 of this act if:

- 1. The request is made pursuant to the provisions of NRS 179.525; or*
- 2. The employee, agent or officer reasonably believes that an extreme emergency situation exists that involves the immediate danger of death or great bodily injury and there is insufficient time, with due diligence, to first obtain an order from a court or magistrate pursuant to section 13 of this act.*

Sec. 15. The good faith reliance of a manufacturer of a smartphone or provider of wireless telecommunications upon a request made pursuant to section 13 or 14 of this act shall constitute a complete defense against any action brought against the manufacturer or provider as a result of the disabling of the essential features of a smartphone.

Sec. 16. 1. Nothing in the provisions of sections 2 to 17, inclusive, of this act shall be construed to prohibit a manufacturer of a smartphone from offering any features in addition to the kill-switch technology required pursuant to section 9 of this act.

2. Nothing in the provisions of sections 2 to 17, inclusive, of this act shall be construed to require a manufacturer of a smartphone to take any action or provide any features on a smartphone that make it impossible to comply with existing obligations under state and federal law related to:

(a) The provision of emergency services through an emergency 911 service, including text messages to a 911 operator, bounce-back messages and location accuracy requirements;

(b) Participation in the wireless emergency broadcast alert system; or



(c) Participation in state and local emergency alert and public safety warning systems.

Sec. 17. *A political subdivision of this State shall not impose any additional requirements on manufacturers of smartphones or providers of wireless telecommunications relating to any subject covered under the provisions of sections 2 to 17, inclusive, of this act.*

Sec. 18. This act becomes effective on July 1, 2015.

