

AMENDED IN ASSEMBLY MARCH 8, 2016

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

**ASSEMBLY BILL**

**No. 1681**

---

---

**Introduced by Assembly Member Cooper**  
**(Coauthor: Assembly Member Gallagher)**  
*(Coauthors: Senators Bates and Hall)*

January 20, 2016

---

---

An act to add Section 22762 to the Business and Professions Code, relating to smartphones.

LEGISLATIVE COUNSEL'S DIGEST

AB 1681, as amended, Cooper. Smartphones.

Existing law requires that a smartphone that is manufactured on or after July 1, 2015, and sold in California after that date, include a technological solution at the time of sale, which may consist of software, hardware, or both software and hardware, that, once initiated and successfully communicated to the smartphone, can render inoperable the essential features, as defined, of the smartphone to an unauthorized user when the smartphone is not in the possession of an authorized user.

This bill would require a smartphone that is manufactured on or after January 1, 2017, and sold in California, to be capable of being decrypted and unlocked by its manufacturer or its operating system provider. The bill ~~would, except as provided, subject a seller or lessor~~ *would subject a manufacturer or operating system provider* that knowingly failed to comply with that requirement to a civil penalty of \$2,500 for each smartphone sold or leased. The bill would prohibit ~~a seller or lessor~~ *manufacturer or operating system provider* who has paid this civil penalty from passing any portion of the penalty on to purchasers of smartphones. The bill would authorize only the Attorney General or a

district attorney to bring a civil suit to enforce these provisions. *This bill would make findings and declarations related to smartphones and criminal activity.*

Vote: majority. Appropriation: no. Fiscal committee: yes.  
 State-mandated local program: no.

*The people of the State of California do enact as follows:*

- 1     *SECTION 1. The Legislature finds and declares all of the*
- 2     *following:*
- 3     *(a) Worldwide, human trafficking is a \$32 billion per year*
- 4     *industry.*
- 5     *(b) After drug trafficking and counterfeiting, human trafficking*
- 6     *is the world’s most profitable criminal activity.*
- 7     *(c) Although previously believed to be an international problem,*
- 8     *current statistics show that human trafficking is increasingly a*
- 9     *domestic issue.*
- 10    *(d) According to estimates by the Federal Bureau of*
- 11    *Investigation (FBI), human trafficking or the commercial sexual*
- 12    *exploitation of children in the United States currently involves*
- 13    *over 100,000 children. The San Francisco Bay area, Los Angeles,*
- 14    *and San Diego metropolitan areas comprise three of the nation’s*
- 15    *13 areas of “high intensity” child exploitation in this country, as*
- 16    *described by the FBI.*
- 17    *(e) Studies have estimated that anywhere from 50 to 80 percent*
- 18    *of victims of commercial sexual exploitation are, or were formerly,*
- 19    *involved with the child welfare system.*
- 20    *(f) Smartphones are increasingly becoming a weapon of choice*
- 21    *for criminals and criminal organizations involved in human*
- 22    *trafficking and sexual exploitation of children.*
- 23    *(g) In 2014, smartphones with full-disk encryption (FDE)*
- 24    *became available on the market.*
- 25    *(h) On smartphones with FDE, when a user creates a password,*
- 26    *that phrase generates a key that is used in combination with a*
- 27    *hardware key on a chip inside the phone, which blocks access to*
- 28    *all “data at rest” stored in the device.*
- 29    *(i) “Data at rest” on a smartphone is data that is parked, stored,*
- 30    *and no longer in motion, such as pictures and text messages.*
- 31    *(j) Only the password holder can unlock the FDE-equipped*
- 32    *smartphone and provide access to all “data at rest.”*

1 (k) Before 2014, when smartphones without FDE were used in  
2 crimes, law enforcement obtained and served a court order on the  
3 phone manufacturer and was able to have access to “data at rest”  
4 on the device, to aid in an investigation.

5 (l) In order to successfully access “data at rest” on smartphones  
6 in a criminal investigation, law enforcement must have physical  
7 possession of the phone.

8 (m) Since the introduction of FDE on smartphones in 2014,  
9 “data at rest” on FDE-equipped smartphones has become virtually  
10 impossible to access.

11 (n) A smartphone belonging to one of the shooters in the County  
12 of San Bernardino mass shooting, which left 14 people dead and  
13 many more injured, is equipped with FDE and has prevented law  
14 enforcement from accessing the phone’s content for evidence.

15 (o) Since 2014, FDE in smartphones has created a public safety  
16 crisis that has armed criminals and criminal organizations with  
17 a powerful weapon to conduct illicit activities while simultaneously  
18 providing a shield to conceal crimes and remain out of reach of  
19 law enforcement.

20 (p) Since 2014, FDE in smartphones has rendered court orders  
21 to access critical evidence on smartphones useless.

22 (q) Since 2014, FDE in smartphones has interfered with law  
23 enforcement human trafficking investigations and prosecutions.

24 (r) Smartphones play an essential role in facilitating cases of  
25 domestic minor sex trafficking. Human traffickers text logistical  
26 information, such as time, place, pricing, types of services, and  
27 descriptions of exploited minors using smartphones.

28 (s) Human traffickers rely on smartphones to communicate with  
29 each other, organize, and advertise their illicit business.

30 (t) Technology-facilitated sex trafficking networks rely upon  
31 anonymity of victims and traffickers in order to operate. Fully  
32 encrypted smartphones, immune to search warrants, make this  
33 possible.

34 (u) Individuals suspected of crimes are, upon the issuance of a  
35 court order, subject to search of their homes, vehicles, and even  
36 their bodies, but not their smartphones that are equipped with  
37 FDE.

38 **SECTION 1.**

39 **SEC. 2.** Section 22762 is added to the Business and Professions  
40 Code, immediately following Section 22761, to read:

1 22762. (a) For the purposes of this section, the following terms  
2 have the following meanings:

3 (1) “Smartphone” has the same meaning as in Section 22761.

4 (2) “Sold in California” has the same meaning as in Section  
5 22761.

6 (3) “Leased in California,” or any variation thereof, means that  
7 the smartphone is contracted for a specified period of time to an  
8 end-use consumer at an address within the state.

9 (b) A smartphone that is manufactured on or after January 1,  
10 2017, and sold or leased in California, shall be capable of being  
11 decrypted and unlocked by its manufacturer or its operating system  
12 provider.

13 ~~(c) Except as provided in subdivision (d), a seller or lessor that~~  
14 ~~sells or leases in California a~~ A smartphone manufactured on or  
15 after January 1, 2017, that is not capable of being decrypted and  
16 unlocked by its manufacturer or its operating system provider shall  
17 ~~be subject~~ *the manufacturer or operating system provider* to a civil  
18 penalty of two thousand five hundred dollars (\$2,500) for each  
19 smartphone sold or leased *in California* if the ~~seller or lessor~~  
20 ~~manufacturer or operating system provider~~ of the smartphone  
21 knew at the time of the sale or lease that the smartphone was not  
22 capable of being decrypted and unlocked by ~~its~~ *the* manufacturer  
23 or its operating system provider. ~~A seller or lessor~~ *manufacturer*  
24 *or operating system provider* who pays a civil penalty imposed  
25 pursuant to this subdivision shall not pass on any portion of that  
26 penalty to purchasers of smartphones by raising the sales or lease  
27 price of smartphones.

28 ~~(d) (1)~~ The sale or lease of a smartphone manufactured on or  
29 after January 1, 2017, that is not capable of being decrypted and  
30 unlocked by its manufacturer or its operating system provider shall  
31 not result in liability to the seller or lessor ~~if the inability of the~~  
32 ~~manufacturer and operating system provider to decrypt and unlock~~  
33 ~~the smartphone is the result of actions taken by a person or entity~~  
34 ~~other than the manufacturer, the operating system provider, the~~  
35 ~~seller, or the lessor and those actions were unauthorized by the~~  
36 ~~manufacturer, the operating system provider, the seller, or the lessor.~~  
37 *lessor.*

38 ~~(2) Paragraph (1) does not apply if at the time of sale or lease,~~  
39 ~~the seller or lessor had been notified that the manufacturer and~~

1 ~~operating system provider were unable to decrypt and unlock the~~  
2 ~~smartphone due to those unauthorized actions.~~

3 (e) A civil suit to enforce this section may only be brought by  
4 the Attorney General, for the sale or lease of a smartphone in  
5 California, or a district attorney for the sale or lease of a  
6 smartphone in the county represented by the district attorney. A  
7 ~~seller or lessor~~ *manufacturer or operating system provider* shall  
8 not be subject to more than a single penalty for each sale or lease  
9 of a smartphone.

10

11

12

**CORRECTIONS:**

\_\_\_\_\_

13

**Title—Line 1.**

14

\_\_\_\_\_

O