
THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 576 Session of
2017

INTRODUCED BY DAVIS, DONATUCCI, BOBACK, THOMAS, GODSHALL, JAMES,
V. BROWN, D. COSTA, BULLOCK, O'NEILL, MILLARD, DRISCOLL AND
KORTZ, FEBRUARY 23, 2017

REFERRED TO COMMITTEE ON CONSUMER AFFAIRS, FEBRUARY 23, 2017

AN ACT

1 Establishing requirements for smartphone theft prevention; and
2 imposing penalties.

3 The General Assembly of the Commonwealth of Pennsylvania
4 hereby enacts as follows:

5 Section 1. Short title.

6 This act shall be known and may be cited as the Smartphone
7 Theft Prevention Act.

8 Section 2. Findings.

9 The General Assembly finds and declares that the enactment of
10 a uniform policy to deter thefts of smartphones and to protect
11 the privacy of smartphone users if the users' smartphones are
12 involuntarily acquired by others is a matter of Statewide
13 concern.

14 Section 3. Definitions.

15 The following words and phrases when used in this act shall
16 have the meanings given to them in this section unless the
17 context clearly indicates otherwise:

1 "Essential features." The ability to use a smartphone for
2 voice communications, text messaging and the ability to browse
3 the Internet, including the ability to access and use mobile
4 software applications. The term does not include functionality
5 needed for the operation of the technological solution or the
6 ability of a smartphone to access emergency services by a voice
7 call or text to 911, the ability of a smartphone to receive
8 wireless emergency alerts and warnings or the ability of a
9 smartphone to call an emergency number predesignated by the
10 owner.

11 "Hard reset." The restoration of a smartphone to the state
12 it was in when it left the factory through processes commonly
13 termed a factory reset or master reset.

14 "Smartphone." A cellular radio telephone or other mobile
15 voice communications handset device that includes all of the
16 following features:

17 (1) Utilizes a mobile operating system.

18 (2) Possesses the capability to utilize mobile software
19 applications, access and browse the Internet, utilize text
20 messaging, utilize digital voice service and send and receive
21 e-mail.

22 (3) Has wireless network connectivity.

23 (4) Is capable of operating on a long-term evolution
24 network or successor wireless data network communications
25 standard.

26 The term does not include a radio cellular telephone commonly
27 referred to as a feature or messaging telephone, a laptop, a
28 tablet device or a device that only has electronic reading
29 capability.

30 Section 4. Requirement.

1 (a) General rule.--Except as provided in section 6, a
2 smartphone manufactured on or after July 1, 2017, and sold in
3 this Commonwealth after that date shall include a technological
4 solution at the time of sale that:

5 (1) shall be provided by the manufacturer or operating
6 system provider; and

7 (2) once initiated and successfully communicated to a
8 smartphone, can render the essential features of a smartphone
9 inoperable to an unauthorized user when a smartphone is not
10 in the possession of an authorized user.

11 (b) Setup prompt.--A smartphone shall, during the initial
12 device setup process, prompt an authorized user to enable the
13 technological solution.

14 (c) Reversibility.--The technological solution shall be
15 reversible so that if an authorized user obtains possession of a
16 smartphone after the essential features of a smartphone have
17 been rendered inoperable, the operation of those essential
18 features can be restored by an authorized user.

19 (d) Nature of solution.--A technological solution:

20 (1) may consist of software, hardware or a combination
21 of both software and hardware;

22 (2) when enabled, shall be able to withstand a hard
23 reset or operating system downgrade; and

24 (3) shall prevent reactivation of the smartphone on a
25 wireless network except by an authorized user.

26 Section 5. Opt-out.

27 An authorized user of a smartphone may affirmatively elect to
28 disable or opt out of enabling the technological solution at any
29 time. However, the physical acts necessary to disable or opt out
30 of enabling the technological solution may only be performed by

1 the authorized user or a person specifically selected by the
2 authorized user to disable or opt out of enabling the
3 technological solution.

4 Section 6. Exception.

5 A smartphone model that was first introduced prior to January
6 1, 2015, that cannot reasonably be reengineered to support the
7 manufacturer's or operating system provider's technological
8 solution, including if the hardware or software cannot support a
9 retroactive update, is not subject to the requirements of this
10 section.

11 Section 7. Penalty.

12 The following shall apply:

13 (1) The retail sale of a smartphone in this Commonwealth
14 knowingly in violation of section 4 may be subject to a civil
15 penalty of not less than \$500 nor more than \$2,500 per
16 smartphone sold.

17 (2) A failure of the technological solution due to
18 hacking or other third-party circumvention may be considered
19 a violation for purposes of this section only if, at the time
20 of sale, the seller has notice from the manufacturer or
21 operating system provider that the vulnerability cannot be
22 remedied by a software patch or other solution. There is no
23 private right of action to enforce this section.

24 (3) The retail sale in this Commonwealth of a smartphone
25 may not result in any civil liability to the seller and its
26 employees and agents from that retail sale alone if the
27 liability results from or is caused by failure of a
28 technological solution required under this section, including
29 hacking or other third-party circumvention of the
30 technological solution, unless at the time of sale the seller

1 has notice from the manufacturer or operating system provider
2 that the vulnerability cannot be remedied by a software patch
3 or other solution.

4 (4) Nothing in this section precludes a suit for civil
5 damages on any other basis outside of the retail sale
6 transaction, including, but not limited to, a claim of false
7 advertising.

8 Section 8. Additional security.

9 The following apply:

10 (1) Nothing in this section prohibits a network
11 operator, device manufacturer or operating system provider
12 from offering a technological solution or other service in
13 addition to the technological solution required to be
14 provided by the device manufacturer or operating system
15 provider under section 4.

16 (2) Nothing in this section requires a technological
17 solution that is incompatible with, or renders it impossible
18 to comply with, obligations under Federal and State law and
19 regulations related to any of the following:

20 (i) The provision of emergency services through the
21 911 system, including text to 911, bounce-back messages
22 and location accuracy requirements.

23 (ii) Participation in the wireless emergency alert
24 system.

25 (iii) Participation in State and local emergency
26 alert and public safety warning systems.

27 Section 9. Preemption.

28 No city or county may impose requirements on manufacturers,
29 operating system providers, wireless carriers or retailers
30 relating to technological solutions for smartphones.

1 Section 10. Effective date.

2 This act shall take effect in 60 days.