

AMENDED IN ASSEMBLY APRIL 17, 2013

CALIFORNIA LEGISLATURE—2013—14 REGULAR SESSION

ASSEMBLY BILL

No. 257

Introduced by Assembly Member Hall

February 7, 2013

An act to amend Section ~~22577~~ 22575 of, and to add Sections ~~22575.1, 22575.2, and 22575.3~~ to, the Business and Professions Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

AB 257, as amended, Hall. Privacy: ~~mobile devices~~. *commercial Web sites and online services.*

Existing law requires an operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service to make its privacy policy available to the consumers, as specified, *including, among others, the requirement that the policy identifies the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers.*

~~This bill would define an online service for purposes of these provisions to include mobile applications designed to be downloaded to and installed on a mobile device. This bill would require the operator of a mobile application to satisfy various requirements, including specified privacy policy requirements, procedures to allow a consumer to access their own personally identifiable information collected and retained, safeguards to protect personally identifiable information, a requirement that the operator provide a supplemental privacy policy if an application collects information not essential to the application's~~

~~basic function, and a requirement that the operator provide a special notice if the application accesses specified devices and information. The bill would require a mobile application market, as defined, to comply with specified procedures allowing access to an application's privacy policy and a means for users to report applications in violation of the applicable terms of service or law. The bill would also establish specified requirements for an advertising network delivering an advertisement through a mobile application, including a privacy policy requirement, a requirement that the network obtain prior consent to display an advertisement in specified circumstances, a requirement that advertisements be clearly attributable to the host application in specified circumstances, and required procedures for identifying a consumer and transmitting information.~~

This bill would require that policy to identify the uses and retention period for each category of personally identifiable information, and to describe the process the operator maintains allowing an individual consumer to review and request changes to any of his or her personally identifiable information. The bill would also require the operator to use reasonable security safeguards to protect personally identifiable information from unauthorized access, use, disclosure, modification, or destruction, and to describe these safeguards in its privacy policy.

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

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

- 1 SECTION 1. Section 22575 of the Business and Professions
- 2 Code is amended to read:
- 3 22575. (a) An operator of a commercial Web site or online
- 4 service that collects personally identifiable information through
- 5 the Internet about individual consumers residing in California who
- 6 use or visit its commercial Web site or online service shall
- 7 conspicuously post its privacy policy on its Web site, or in the case
- 8 of an operator of an online service, make that policy available in
- 9 accordance with paragraph (5) of subdivision (b) of Section 22577.
- 10 An operator shall be in violation of this subdivision only if the
- 11 operator fails to post its policy within 30 days after being notified
- 12 of noncompliance.
- 13 (b) The privacy policy required by subdivision (a) shall do all
- 14 of the following:

1 (1) Identify the categories of personally identifiable information
2 that the operator collects through the Web site or online service
3 about individual consumers who use or visit its commercial Web
4 site or online service, *the uses and retention period for each*
5 *category of personally identifiable information collected*, and the
6 categories of third-party persons or entities with whom the operator
7 may share that personally identifiable information.

8 (2) ~~If the operator maintains a~~ *Describe the process for the*
9 *operator maintains allowing* an individual consumer who uses or
10 visits its commercial Web site or online service to review and
11 request changes to any of his or her personally identifiable
12 information that is collected through the Web site or online service;
13 ~~provide a description of that process.~~

14 (3) Describe the process by which the operator notifies
15 consumers who use or visit its commercial Web site or online
16 service of material changes to the operator's privacy policy for
17 that Web site or online service.

18 (4) Identify its effective date.

19 (5) *Describe the security safeguards used to comply with the*
20 *requirements of subdivision (c).*

21 (c) *An operator described in subdivision (a) shall use reasonable*
22 *security safeguards to protect personally identifiable information*
23 *from unauthorized access, use, disclosure, modification, or*
24 *destruction.*

25 ~~SECTION 1. Section 22575.1 is added to the Business and~~
26 ~~Professions Code, to read:~~

27 ~~22575.1. (a) The privacy policy for a mobile application shall~~
28 ~~specify and limit practices regarding information retention and~~
29 ~~collection, including the types of information collected, the use~~
30 ~~and retention period for each category of information, the~~
31 ~~categories of third parties with whom personally identifiable~~
32 ~~information will be shared, and the choices a consumer has~~
33 ~~regarding the collection, use, and sharing of personally identifiable~~
34 ~~information.~~

35 ~~(b) The operator of a mobile application shall:~~

36 ~~(1) Provide consumers access to their own personally identifiable~~
37 ~~information that the application collects and retains.~~

38 ~~(2) Use security safeguards to protect personally identifiable~~
39 ~~information from unauthorized access, use, disclosure,~~
40 ~~modification, or destruction.~~

1 ~~(3) Provide a supplemental privacy policy with enhanced~~
2 ~~measures if an application collects personally identifiable~~
3 ~~information that is not essential to the application's basic function.~~

4 ~~(4) Provide consumers with a special notice if the application~~
5 ~~accesses text messages, call logs, the camera, the dialer, or the~~
6 ~~microphone, or collects location information, financial information,~~
7 ~~medical information, or passwords. A special notice shall deliver~~
8 ~~notice to the consumer of the information collection. A special~~
9 ~~notice shall explain the intended uses of the information and~~
10 ~~disclose the type of third parties to whom the information may be~~
11 ~~disclosed.~~

12 ~~(e) The requirements for a mobile application privacy policy~~
13 ~~are in addition to the requirements specified elsewhere in this~~
14 ~~chapter.~~

15 ~~SEC. 2. Section 22575.2 is added to the Business and~~
16 ~~Professions Code, to read:~~

17 ~~22575.2. (a) In the application submission process for a new~~
18 ~~or updated mobile application, a mobile application market shall~~
19 ~~include either of the following:~~

20 ~~(1) An optional data field for a hyperlink to the application's~~
21 ~~privacy policy or a statement describing the application's privacy~~
22 ~~practices.~~

23 ~~(2) An optional data field for the text of the application's privacy~~
24 ~~policy or a statement describing the application's privacy practices.~~

25 ~~(b) A mobile application market shall:~~

26 ~~(1) Implement a means for users to report applications that do~~
27 ~~not comply with the applicable terms of service or law.~~

28 ~~(2) Implement a process for responding to reported instances~~
29 ~~of noncompliance with applicable terms of service or law.~~

30 ~~SEC. 3. Section 22575.3 is added to the Business and~~
31 ~~Professions Code, to read:~~

32 ~~22575.3. An advertising network delivering an advertisement~~
33 ~~through a mobile application shall:~~

34 ~~(a) Include a privacy policy governing the collection, use,~~
35 ~~disclosure, and retention of personally identifiable information.~~
36 ~~This policy shall be made available to users of mobile applications~~
37 ~~and application developers.~~

38 ~~(b) Obtain prior consent before displaying an advertisement~~
39 ~~delivered through an application and displayed outside the context~~
40 ~~of the application.~~

1 ~~(e) Provide clear attribution of the host application responsible~~
2 ~~for an advertisement delivered through an application and displayed~~
3 ~~outside the context of the application.~~

4 ~~(d) Obtain prior consent before accessing personally identifiable~~
5 ~~information.~~

6 ~~(e) Use application-specific or temporary device identifiers, not~~
7 ~~unchangeable device-specific identifiers.~~

8 ~~(f) Transmit user data securely, using encryption for permanent~~
9 ~~unique device identifiers and personal information.~~

10 ~~SEC. 4. Section 22577 of the Business and Professions Code~~
11 ~~is amended to read:~~

12 ~~22577. For the purposes of this chapter, the following~~
13 ~~definitions apply:~~

14 ~~(a) The term “personally identifiable information” means~~
15 ~~individually identifiable information about an individual consumer~~
16 ~~collected online by the operator from that individual and~~
17 ~~maintained by the operator in an accessible form, including any~~
18 ~~of the following:~~

19 ~~(1) A first and last name.~~

20 ~~(2) A home or other physical address, including street name and~~
21 ~~name of a city or town.~~

22 ~~(3) An e-mail address.~~

23 ~~(4) A telephone number.~~

24 ~~(5) A social security number.~~

25 ~~(6) Any other identifier that permits the physical or online~~
26 ~~contacting of a specific individual.~~

27 ~~(7) Information concerning a user that the Web site or online~~
28 ~~service collects online from the user and maintains in personally~~
29 ~~identifiable form in combination with an identifier described in~~
30 ~~this subdivision.~~

31 ~~(b) The term “conspicuously post” with respect to a privacy~~
32 ~~policy shall include posting the privacy policy through any of the~~
33 ~~following:~~

34 ~~(1) A Web page on which the actual privacy policy is posted if~~
35 ~~the Web page is the homepage or first significant page after~~
36 ~~entering the Web site.~~

37 ~~(2) An icon that hyperlinks to a Web page on which the actual~~
38 ~~privacy policy is posted, if the icon is located on the homepage or~~
39 ~~the first significant page after entering the Web site, and if the icon~~
40 ~~contains the word “privacy.” The icon shall also use a color that~~

1 ~~contrasts with the background color of the Web page or is~~
2 ~~otherwise distinguishable.~~

3 ~~(3) A text link that hyperlinks to a Web page on which the actual~~
4 ~~privacy policy is posted, if the text link is located on the homepage~~
5 ~~or first significant page after entering the Web site, and if the text~~
6 ~~link does one of the following:~~

7 ~~(A) Includes the word “privacy.”~~

8 ~~(B) Is written in capital letters equal to or greater in size than~~
9 ~~the surrounding text.~~

10 ~~(C) Is written in larger type than the surrounding text, or in~~
11 ~~contrasting type, font, or color to the surrounding text of the same~~
12 ~~size, or set off from the surrounding text of the same size by~~
13 ~~symbols or other marks that call attention to the language.~~

14 ~~(4) Any other functional hyperlink that is so displayed that a~~
15 ~~reasonable person would notice it.~~

16 ~~(5) In the case of an online service, any other reasonably~~
17 ~~accessible means of making the privacy policy available for~~
18 ~~consumers of the online service, except for a mobile application,~~
19 ~~which shall follow the requirements in Section 22575.1.~~

20 ~~(e) The term “operator” means any person or entity that owns~~
21 ~~a Web site located on the Internet or an online service that collects~~
22 ~~and maintains personally identifiable information from a consumer~~
23 ~~residing in California who uses or visits the Web site or online~~
24 ~~service if the Web site or online service is operated for commercial~~
25 ~~purposes. It does not include any third party that operates, hosts,~~
26 ~~or manages, but does not own, a Web site or online service on the~~
27 ~~owner’s behalf or by processing information on behalf of the~~
28 ~~owner.~~

29 ~~(d) The term “consumer” means any individual who seeks or~~
30 ~~acquires, by purchase or lease, any goods, services, money, or~~
31 ~~credit for personal, family, or household purposes.~~

32 ~~(e) The term “online service” includes, but shall not be limited~~
33 ~~to, a mobile application.~~

34 ~~(f) The term “mobile application” means an application designed~~
35 ~~to be downloaded to and installed on a mobile device, such as a~~
36 ~~mobile phone, a tablet, or a smart phone.~~

37 ~~(g) The term “mobile application market” means a computerized~~
38 ~~system where a person can purchase a mobile application and~~
39 ~~download the mobile application directly to a mobile device.~~

O