Best Privacy Anywhere Act

Robert Gellman
bob@bobgellman.com
Version 1.11

Summary: A company must provide consumers in [State] the strictest privacy protections that the company applies in any other jurisdiction, domestic or foreign, where it conducts business online for substantially similar activities.

This draft uses language and definitions (with some modifications) from Cal. Business and Professions Code §§ 22575-22579 and from HIPAA 45 CFR § 160.202. Enforcement provision based loosely on the California's Shine the Light law, Cal. Civil Code § 1798.83 and its enforcement provision in § 1798.84.

Section 1. Definitions

For the purposes of this Act, the following definitions apply:

(a) The term "covered company" means any person or entity [that has 10 or more full-time or part-time employees regardless of the location of the employees] and that owns a Web site located on the Internet or an online service that processes personally identifiable information from a consumer residing in [State] who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner's behalf or by processing information on behalf of the owner.

(b) The term "consumer" means any individual who seeks or acquires any goods, services, money, or credit for personal, family, or household purposes.

(c) The term "personally identifiable information" means individually identifiable information about a consumer collected online by a covered company and maintained by the covered company in an accessible form, including any of the following:

(1) a first and last name.

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

(3) an e-mail address.

(4) a telephone number.

(5) a social security number.

(6) IP address.

(7) any other identifier that permits the physical or online contacting of a specific individual.

(8) information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this Act.

(d) The term “processing” means with respect to personally identifiable information the collection, use, disclosure, maintenance, storage, erasure, or destruction of the personally identifiable information.

(e) The term “Administrator” means [the state’s consumer protection office, Attorney General’s Office, or some other state office].

Section 2. Privacy Requirements

(a) Any covered company must provide, with respect to any activity involving the processing of personally identifiable information of a consumer, the most stringent privacy provision for the personally identifiable information about the consumer that the company provides, whether through an applicable legal requirement or a voluntarily adopted privacy policy, to any individual in another nation, state, or province where the company engages in a substantially similar activity.

(b) “Most stringent” means, in the context of an applicable legal requirement or a voluntarily adopted privacy policy:

(1) with respect to a use or disclosure of personally identifiable information, the privacy provision that prohibits or restricts use or disclosure of the personally identifiable information to the greatest extent;

(2) with respect to the collection of personally identifiable information, the privacy provision that results in the collection of the smallest amount of personally identifiable information and the maintenance of personally identifiable information for the shortest time;

(3) with respect to the rights of the individual who is the subject of the personally identifiable information regarding access to or amendment of the personally identifiable information, the privacy provision that permits greatest right of access, amendment, or erasure;

(4) with respect to disclosure to the individual who is the subject of the personally identifiable information of information about the use, disclosure, rights, remedies, or other aspects of processing of personally identifiable information, the privacy provision that discloses the most information and that discloses the information at the earliest time;

(5) with respect to the forms, substance, or need for express consent from an individual who is the subject of personally identifiable information for use of disclosure of the personally identifiable information, the privacy provision that most narrows the scope or duration of the consent, most increases the privacy protections afforded, and most reduces the coercive effect of the circumstances surrounding the consent;

(6) with respect to recordkeeping or requirements relating to the maintenance of records about the use or disclosure of the personally identifiable information, the privacy provision that provides for the longest retention of information, for the reporting of more detailed information, and for the longest duration of information;

(7) with respect to security, the privacy provision that provides the greatest technical, administrative, and physical protection against any anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to the individual who is the subject of the personally identifiable information;

(8) with respect to any other matter covered by a legal requirement or voluntarily adopted privacy policy, the privacy provision that provides the greater degree of privacy protection for the individual who is the subject of the personally identifiable information.

Section 3. Exceptions:

A covered company is not required to adopt or comply with a more stringent privacy requirement or policy that would otherwise apply under this Act –

(1) if a federal, state, or provincial law prohibits compliance with that privacy requirement or policy;

(2) if a federal, state, or provincial law requires an action that would be inconsistent with that privacy requirement or policy;

(3) if ordered by a court of competent jurisdiction in a written order signed by a judge;

(4) if a general exception applies;

(5) if an emergency exception applies;

(6) if a covered company obtains, within six months of the processing of any processing of personally identifiable information about an individual, consent from the individual for the processing that complies with Section 5(a) of this Act.

Section 4. Rules

(a) The Administrator shall, following public notice and comment, promulgate rules defining the circumstances and procedures under which it will authorize an emergency exception and the scope and duration of the exception. An emergency exception may only authorize processing of personally identifiable information for an activity likely to prevent or lessen a serious threat to health or safety of an individual or the public. Each emergency exception shall

be as narrowly drafted as possible. The Administrator shall publish on its website within seven days of granting an emergency exception a notice describing the particulars of the exception. The Administrator may defer publishing of the notice for as long as it determines that publication would undermine the purpose for which the emergency exception was sought.

(b) The Administrator shall, following public notice and comment, promulgate rules defining any general exception that it determines to be necessary. A general exception may address matters affecting public health or safety, conflicting obligations that a covered company may face in implementing this Act, or any other public interest determined to be sufficiently important to outweigh the protections that this Act seeks to enforce. Each general exception shall be as narrow as possible. Each general exception shall expire no later than four years after its promulgation unless the Administrator, following additional public notice and comment, renews the general exception.

(c) The Administrator shall, following public notice and comment, promulgate such other rules as it deems necessary or appropriate to implement this Act.

Section 5. Construction

(a) A consent under this Act is not valid unless (1) it informs the individual of each specific privacy requirement with which the consent authorizes the company to avoid compliance; (2) is voluntary; (3) is expressed through an affirmative action of the individual; and (4) remains in effect for no longer than one year unless renewed by the individual. If a privacy provision regarding consent that is more stringent than the provisions of this Act applies to a covered company under the terms of this Act, then the more stringent privacy provision applies. An individual may not through a valid consent under this Act waive any right provided by law unless the law expressly authorizes the individual to waive the right.

(b) All exceptions under this Act shall be narrowly construed.

(c) An exception under Section 3(a)(1) or 3(a)(2) shall only apply to the extent that an action required or prohibited is contrary to a legal requirement or privacy policy that would otherwise apply and if it would be impossible to comply with both the federal or [State] law and the otherwise applicable legal requirement or voluntarily adopted privacy policy.

(d) Two activities shall be considered to be substantially similar if they provide information or Internet search, electronic or voice or video mail, shopping, database, social networking, credit or other financial services, travel or accommodation arrangements, mapping services, music or other entertainment, software applications, or other online facilities or services to consumers in [State] that are generally comparable in scope, function, effect on consumer privacy, or processing of personally identifiable information to facilities or services provided to consumers in another jurisdiction, even if the facilities or services are not identical or are offered in different combinations or arrangements.

(e) In assessing the stringency of an applicable legal requirement or a voluntarily adopted privacy policy, each element shall be assessed separately. If a privacy provision applied by a

covered company in another nation, state, or province is more stringent in part and less stringent in part, the more stringent element shall apply unless that element is inextricably intertwined with the less stringent element.

Section 6. Enforcement

(a) Except as expressly provided in this Act, any waiver of a provision of this Act is contrary to public policy and is void and unenforceable.

(b) Any person injured by a violation of this Act may institute a civil action to recover damages.

(c) In addition, for a willful, intentional, or reckless violation of this Act, any person may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the person may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of this Act.

(d) A covered company whose published privacy policy fails to meet the requirements of this Act but that has not actually processed personally identifiable information in a manner that would have violated the privacy provisions that should have applied under this Act shall not be liable for the civil penalty applicable to a willful, intentional, or reckless violation of this Act if the covered company publishes a corrected privacy policy within 60 days of the commencement of litigation.

(e) Any business that violates, proposes to violate, or has violated this Act may be enjoined from violating this Act.

(f) A prevailing plaintiff in any action commenced under this Act shall also be entitled to recover his or her reasonable attorney's fees and costs.

(g) The rights and remedies available under this Act are cumulative to each other and to any other rights and remedies available under law.

Section 7. Effective Date

(a) This Act shall become operative on the earlier of 18 months after the date of enactment or 60 days after the promulgation by the Administrator of rules required by this Act.

(b) After the operative date of this Act, if a new or changed applicable legal requirement or a voluntarily adopted privacy policy of a covered company becomes effective in another nation, state, or province, the covered company shall bring its privacy policy for [State] consumers into compliance within 60 days after the date upon which it implements the applicable legal requirement or voluntarily adopted privacy policy in the other nation, state, or province.

Version History

Version 1.11 corrects citations in the introductory note. Adds a version history to the document.

Version 1.10. First public draft.