People's Privacy Act

HB 1433 – Corporate F.A.Q.

Question: Is my organization covered under this Act?

Your organization is a covered entity if it is a non-governmental entity, conducts business in Washington, processes personal information (e.g., collect, use, or share personal information), and:

- during the course of a calendar year: earns at least $10 million annually through at least 300 transactions;
- or processes and/or maintains the captured personal information of 1,000 or more unique individuals.

Provisions regarding biometric information and protections against discrimination apply also to Washington governmental entities.

Question: Does my organization need to get opt-in consent to process personal information for every transaction or interaction with individuals?

No, covered entities may process an individual's personal information without obtaining opt-in consent, but only to the extent necessary to complete a specific transaction affirmatively requested by that individual.

- For example, if an individual purchases a book from an online retailer that qualifies as a covered entity, the retailer does not need to ask permission to collect and use the individual's shipping address to mail the book. The retailer may not, however, use any of the individual's personal information gathered in the sale for any other purpose beyond the specific request by the individual. For example, the retailer may not use information from the sale to target the individual with advertising about similar books, unless it has specifically asked and received the individual's voluntary and informed consent to do so. Covered entities must provide individuals in advance with a short and easy-to-understand privacy policy that explains what information they are asking permission to collect, for what purpose they seek to use it, how long they intend to retain it, and with whom they wish to share that information.

Question: If an individual does not provide consent for my organization to process their data, can my organization refuse to serve that individual?

No, under the Act, individuals have the right to refuse consent for any processing of their personal information beyond the particular transaction they have specifically requested (e.g., purchasing a book) and cannot be denied service for refusing consent.

- Examples:
  - Covered entities may not increase the price or diminish the quality of a product or service if individuals refuse consent.
  - Covered entities may create "frequent shopper" or "loyalty" programs where individuals get a discount because they are loyal customers, but covered entities cannot use personal information about individuals (e.g., shopping habits) for any other reason or sell or give it to anyone else without the individual's affirmative, opt-in consent.

Question: I'm a covered entity, what obligations does my organization have?

Covered entities must:

- Create both a long-form and short-form privacy policy that is persistently and conspicuously available on the covered entity's website, mobile application, at the primary physical place of business, and any offline equivalent.
- Ask for and obtain the freely given, specific, informed, and unambiguous opt-in consent from an individual prior to processing the individual's personal information or making any changes in the processing of the

Eric González Alfaro, *Legislative Director* | egonzalez@aclu-wa.org | www.aclu-wa.org

ACLU Washington

individual's personal information that would necessitate a change to the covered entity's short-form privacy notice.

- Make the process of withdrawing consent as conspicuous and easy as granting consent.
- Use practices that at a minimum satisfy the reasonable standard of care within the covered entity's industry for protecting personal information from disclosure.
- Provide individuals with a reasonable means to access their personal information including all personal information obtained about the individual from them or a third-party, all information about where or from whom the covered entity obtained personal information, and the types of third parties to which the covered entity has disclosed or will disclose personal information.
- Provide individuals with a reasonable means to correct inaccurate or incomplete personal information processed by the covered entity.
- Not disclose captured personal information to a third party unless that third party is contractually bound to the covered entity to meet the same privacy and security obligations as the covered entity.
- Not activate the microphone, camera, or any other sensor on a device in the lawful possession of an individual that is capable of collecting or transmitting personal information, without providing the required privacy notices and obtaining the individual's freely given, specific, informed, and unambiguous opt-in consent.

Question: Are there special protections for biometric information?

Yes, neither covered entities nor government agencies in Washington may collect, use, or share individuals' biometric information without getting their affirmative opt-in consent.

- Covered entities and Washington governmental agencies may not monetize or profit from a person's biometric information *unless* it is to provide that person with actions or products that that person has specifically requested, provided that that biometric information is not used for any other purpose. For example, after obtaining an individual's opt-in consent to analyze their biometric information and sell them a fitness report, a fitness tracking company may charge that individual for that report but may not use that report for other things like targeted advertising or sell that individual's data to any other entity or for any other purpose.

Question: Does this Act prohibit any specific data practices?

Yes. This Act prohibits covered entities and Washington governmental agencies from:

- Using personal information to illegally discriminate on the basis of: age, race, creed, color, national origin, sexual orientation, gender identity or expression, sex, disability, predisposing genetic characteristics, or domestic violence victim status.
- Using or installing face recognition technology or equipment incorporating artificial intelligence-enabled profiling in any place of public accommodation (e.g., restaurants, hotels, theaters, pharmacies, parks, schools, and stores).
- Using artificial intelligence-enabled profiling to make decisions that produce legal effects or similarly significant effects concerning individuals (e.g., denying financial or lending services, housing, insurance, educational enrollment, criminal justice, employment opportunities, health care services, and access to basic necessities, such as food and water).
- Monetizing or profiting off biometric information, except to provide an individual with actions or products that have been specifically requested by the individual, provided that the biometric information shall not be shared or used for any other purpose.

Eric González Alfaro, *Legislative Director* | egonzalez@aclu-wa.org | www.aclu-wa.org

ACLU Washington

Question: What enforcement options do people have?

Under this Act, individuals have a private right of action.

- For every successful enforcement suit, the violator must pay reasonable attorney's fees and costs, and a court may award the larger of $10,000 per violation or actual damages, as well as punitive damages and other appropriate relief.

The Washington State Attorney General, city attorneys, and county prosecutors are empowered to bring enforcement lawsuits. In such lawsuits, a court may award civil penalties, injunctions, restitution, and other appropriate relief.

Eric González Alfaro, *Legislative Director* | egonzalez@aclu-wa.org | www.aclu-wa.org

ACLU Washington