An Exclusive Cheat-Sheet
Curated By:
tsaaro. consulting

AMERICAN PRIVACY RIGHTS ACT CHEAT SHEET

SCOPE AND APPLICABILITY

1. Covered entities, either alone or jointly with others, determine the purposes and means of processing covered data.

a. Includes:

- *Businesses subject to the U.S. Federal Trade Commission's authority.*
- *Common carriers.*
- *Non-profits*

b. Excludes small businesses if all of the following apply:

- *They have **less than USD40 million** in annual revenue.*
- *They process covered data of **less than 200,000 individuals**, with exceptions.*
- *They do not earn revenue from the transfer of covered data to third parties.*

2. Service providers process covered data on behalf of, and at the direction of, a covered entity.

3. Note:

- Effective date: 180 days (about 6 months) after enactment of the Act.
- The Act does not change obligations under (the Children's Online Privacy Protection Act) COPPA.

ENFORCEMENT AND PRIVATE RIGHT OF ACTION

A. Enforceable by the FTC, state attorneys general, the chief consumer protection officer of a state, or an authorized officer or office of the state.

B. Individuals have a private right of action to enforce various provisions and can seek damages, injunctive relief, declaratory relief, and reasonable legal and litigation costs.

SELECTED DEFINITIONS

COVERED ALGORITHM

A computational process that makes a decision or facilitates human decision-making by using covered data.

COVERED DATA

includes information that identifies or is linked or reasonably linkable to an individual, including in combination with other information.

INDIVIDUALS

A natural person residing in the U.S.

THIRD PARTY

Any entity that receives covered data from another entity, except service providers. All 'covered entity' requirements apply to third parties, except sensitive data, 39(b).

SENSITIVE DATA

Defined broadly to include data related to government identifiers; health; biometrics; genetics; financial accounts and payments; precise geolocation; log-in credentials; private communications; revealed sexual behavior; calendar or address book data, phone logs, photos and recordings for private use; intimate imagery; video viewing activity; race, ethnicity, national origin, religion or sex; online activities over time and across third party websites; information about a minor under the age of 17; and other data the FTC defines as sensitive covered data by regulation.

KEY PRINCIPLES AND OBLIGATIONS

DATA MINIMIZATION-

Generally, processing of personal data is prohibited unless:

a. Necessary, proportionate and limited to provide or maintain either:
- A specific product or service requested by the individual.
- A reasonably anticipated communication to the individual.

b. For one of the 15 listed permitted purposes

c. Sensitive data requires opt-in consent for transfer. However, biometric and genetic information requires opt-in consent for collection and transfer as the permitted purposes are narrower.

SERVICE PROVIDERS AND THIRD PARTIES

Reasonable due diligence is required for selecting a service provider and transferring to a third party.

Service providers must adhere to the instructions of covered entities and implement reasonable safeguards.

Data practices to be ceased by service providers where they have actual knowledge of a covered entity being in violation of this Act.

Third parties may only process, retain, and transfer data and sensitive data received from another entity only adhering to the purpose disclosed in its privacy policy and the express consent by the consumer respectively.

CIVIL RIGHTS AND ALGORITHMS

Processing covered data in a way that discriminates on the basis of race, color, religion, national origin, sex or disability is prohibited with exceptions, including for testing to prevent discrimination.

Annual algorithm impact assessments for large data holders are required if there is a 'consequential risk of harm' to defined groups or outcomes, including minors, major life events and disparate impacts.

Prior evaluation of the covered algorithm before the deployment is necessary.

DATA SECURITY AND PROTECTION OF COVERED DATA

1.Reasonable data security practices proportionate to the size of the entity and nature/volume of its data practices, including regular training, are required.

2.Assessment of vulnerabilities and risks associated with the consumer data is necessary for covered entities and service providers.

3. It is also mandatory for covered entities to appoint one or more covered employees to serve as privacy or data security officers, and both for large data holders.

4. Large data holders to also conduct PIAs on a biennial basis.

TRANSPARENCY

Privacy policies must list prescribed information, including categories of third parties and service providers, names of any data broker transfer, and the retention period along with the effective date of such policy.

Material changes require pre-notification and means of opting out.

INDIVIDUAL CONTROL OVER COVERED DATA

Consumers have the right to access, correction, deletion and portability upon submitting a verifiable request. Compliance within specified time frames is obligatory by the covered entities.

Covered entries may also deny the individual's request if it is demonstrably impossible to perform.

OPT-OUT RIGHTS AND CENTRALIZED MECHANISM

The right to opt out of covered data transfers of non-sensitive covered data and targeted advertising is included.

INTERFERENCE WITH CONSUMER RIGHTS

Dark patterns are prohibited if they interfere with notice, consent or choice.

Conditioning the exercise of rights by the covered entities on materially misleading, false, fictitious, or fraudulent statements is prohibited.

PROHIBITION ON DENIAL OF SERVICE AND WAIVER OF RIGHTS

Retaliation for exercising consumer rights is prohibited.

Bona fide loyalty programs may also be provided to the consumers by the covered entities after seeking express consent for participation.

CONSEQUENTIAL DECISION AND OPT OUT

An entity that uses a covered algorithm to make or facilitate a consequential decision, further defined by future FTC rules, must provide notice and an opportunity to opt out.

ADDITIONAL OBLIGATIONS

- ***Large data holders***, whether covered entities or service providers, must also:
- Publish privacy policies from the past 10 years.
- Publish annual transparency reports about consumer requests.
- Provide annual CEO-signed certifications of compliance controls to the FTC.
- Submit impact assessments to the FTC when AI poses a consequential risk of harm,

- ***Data brokers***, a type of covered entity, must also:
- Provide special notices to consumers and register on the FTC-managed registry.
- Honor 'Do Not Collect' requests via the centralized opt-out mechanism established by the FTC. Once established, the private right of action applies to this obligation.
- Not rely on the 'bona fide loyalty program' exception to the prohibition on retaliation

- ***Covered high-impact social media companies*** must also:
- Treat individuals' activities on their platforms as sensitive data, even if it is not 'over time and across websites or services.'
- Treat any advertising 'over time' on the platform as targeted advertising, with exceptions.
- Not rely on the 'bona fide loyalty program' exception to the prohibition on retaliation

DATA SECURITY & PRIVACY MEASURES

- DATA ENCRYPTION
- ACCESS CONTROLS
- REGULAR DATA BACKUPS
- DATA BREACH NOTIFICATION
- PRIVACY BY DESIGN