The Consumer Online Privacy Rights Act: What You Need To Know

OneTrust DataGuidance Research

Disclaimer:

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

The Consumer Online Privacy Rights Act: What You Need To Know

What has happened?

Senator Maria Cantwell announced, on 26 November 2019, that she, along with Senators Brian Schatz, Amy Klobuchar, and Ed Markey, had introduced a bill for the Consumer Online Privacy Rights Act ('COPRA') to the U.S. Senate.

Definitions

Section 2 of COPRA provides the definitions to provide clarity for terms used in COPRA, such as:

- **Algorithmic decision-making:** a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques that makes a decision or facilitates human decision making with respect to covered data.
- **Covered data:** information that identifies or is linked or reasonably linkable to an individual or a consumer device, including derived data. The term of covered data does not include de-identified data, employee data; and public records.
- **Process:** any operation or set of operations performed on covered data including collection, analysis, organization, structuring, retaining, using, or otherwise handling covered data.
- **Covered entity:** any entity or person that (i) is subject to the Federal Trade Commission ('FTC') Act (15 U.S.C. 41 et seq.); and (ii) processes or transfers covered data.
- **Large data holder:** an entity that, in the last calendar year, processed or transferred the covered data of more than 5,000,000 individuals, devices, or households; or processed or transferred the sensitive data of over 100,000 individuals, devices, or households.

Data privacy rights

COPRA establishes a duty of loyalty based on which covered entities **must not engage in a deceptive data practice** or a harmful data practice, **or process or transfer covered data in a manner that violates** any COPRA provisions.

In addition, COPRA grants **rights** to individuals to (upon verified request) **access, delete and correct inaccuracies** in their data which is held by covered entities.

COPRA also provides for the **right to data portability** whereby a covered entity, upon the verified request of an individual, shall export the individual's covered data, except for derived data, without licensing restrictions. The data needs to be in a human-readable format, allowing individual to understand such covered data; and

Copyright © 2019 OneTrust LLC. All rights reserved. Proprietary & Confidential.

in a structured, interoperable, and machine-readable format that includes all covered data or other information that the covered entity collected to the extent feasible.

In addition, COPRA introduces the right to opt-out of covered data transfers, whereby covered entities:

- must not transfer covered data to a third party if the individual objects to the transfer; and
- must not process or transfer sensitive covered data without the individual's prior, affirmative express consent.

COPRA provides for the **right to data minimisation** whereby a covered entity shall not process or transfer covered data beyond what is reasonably necessary, proportionate, and limited to:

- to carrying out the specific processing purposes and transfers described in the privacy policy made available by the covered entity;
- to carrying out a specific processing purpose or transfer for which the covered entity has obtained affirmative express consent; or
- for a purpose specifically permitted under an exception to affirmative consent.

The **right to data security** mandates that a covered entity shall establish, implement, and maintain reasonable data security practices to protect the confidentiality, integrity, and accessibility of covered data. Such data security practices shall be appropriate to the volume and nature of the covered data issue.

Furthermore, COPRA protects civil rights by **prohibiting processing or transferring data on the basis of the characteristics of an individual for certain purposes** or in a manner that unlawfully segregates, discriminates against, or makes unavailable to individuals the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation and by requesting entities that engage in algorithmic decision-making to annually conduct an impact assessment which would describe, evaluate and assess the algorithmic system.

It is also **generally prohibited for a covered entity to make the provision of its service or product conditional upon an individual or individuals' agreement to waive privacy rights** granted to them under COPRA.

According to the limitations and applicability provisions, a covered entity shall not permit an individual to exercise certain rights if it cannot be reasonably verified that the individual making the request to exercise the right is the data subject or has been authorised by them to make such a request on their behalf. Furthermore, the covered entity may deny an individual the opportunity to exercise their rights under COPRA if they reasonably believe that the request is made to interfere with a contract between the covered entity and another individual.

Copyright © 2019 OneTrust LLC. All rights reserved. Proprietary & Confidential.

Oversight and responsibility

COPRA introduces executive responsibility where executives of large data holders (or highest-ranking officer in the entity), shall **annually certify to the FTC**, that the entity maintains:

- adequate internal controls to comply with COPRA; and
- reporting structures to ensure that such certifying officers are involved in, and are responsible for, decisions that impact the entity's compliance with COPRA.

COPRA creates a requirement for executives of large data holders to annually certify to the Federal Trade Commission ('FTC') that the entity maintains adequate compliance controls and reporting structures to ensure that the certifying officers are involved in, and are responsible for, decisions that impact the entity's compliance It also provides that **an employee who is designated by a covered entity as a privacy officer or a data security officer** shall be responsible for, at a minimum:

- implementing a comprehensive written data privacy program and data security program to safeguard the privacy and security of covered data;
- annually conducting privacy and data security risk assessments, data hygiene, and other quality control practices; and
- facilitating the covered entity's ongoing compliance with this COPRA.

COPRA also includes details on the **duties of service providers and third parties**. A service provider shall not process service provider data for any purpose other than one performed on behalf of, and at the direction of, the covered entity that transferred such data to the service provider, except that a service provider may process data comply with a legal obligation or the establishment, exercise, or defence of legal claims. Furthermore, a third party shall not process third party data that is inconsistent with the expectations of a reasonable individual.

COPRA includes **protections for whistleblowers** and outlines that covered entities cannot directly or indirectly, discharge, demote, suspend, threaten, harass, or in any other manner discriminate against a covered individual of the covered entity.

Enforcement and preemption

Any violations of COPRA shall be treated as violations of a rule defining an unfair or deceptive act or practice as prescribed under Section 18 of the FTC Act and will be enforced by the FTC, state Attorneys General and individuals who may bring civil actions in any court of competent jurisdiction. It is also established that a new bureau would be created within the FTC which would assist it in exercising its authorities.

Copyright © 2019 OneTrust LLC. All rights reserved. Proprietary & Confidential.

Finally, COPRA establishes that **nothing in its provisions shall be construed to preempt, displace, or supplant State consumer protection laws**, civil rights laws, laws governing privacy rights or other protections of employees, employee information, or students or student information, data breach notification laws, contract or tort laws, criminal laws, laws specifying remedies or a cause of action to individuals, or public safety or sector specific laws unrelated to privacy or security.

However, it **provides that it shall supersede any State law to the extent such law directly conflicts with COPRA's provisions**, or a standard, rule, or regulation promulgated under COPRA, and then only to the extent of such direct conflict. Any State law, rule, or regulation shall not be considered in direct conflict if it affords a greater level of protection to individuals protected under COPRA.

Copyright © 2019 OneTrust LLC. All rights reserved. Proprietary & Confidential.