OREGON CONSUMER PRIVACY TASK FORCE UPDATE AND LEGISLATION

DECEMBER 2022 LEGISLATIVE DAYS

Oregon Department of Justice Presenters:

Kimberly McCullough, Legislative Director

Kate Denison, Deputy Legislative Director

OREGON CONSUMER PRIVACY TASK FORCE

- Convened in June 2019
- Overall goal: Study and recommend comprehensive, state-level privacy protections for Oregon consumers
- Over 150 stakeholders
- Central table members:
  - ACLU of Oregon
  - OSPIRG
  - World Privacy Forum
  - Gazelle Consulting
  - Judiciary Committee staff
  - Technology Association of Oregon
  - State Privacy Coalition
  - Oregon Business & Industry
  - Electronic Frontier Foundation

CIRCUITOUS PATH: 2019-2023

- 2019-2020
  - Research, discuss, draft comprehensive legislation
  - COVID-19, wildfires & three special sessions
  - Challenges with legislative concept (LC) drafting
  - Emergency need: draft contact tracing legislation
- 2021
  - Long legislative session
  - Passage of contact tracing legislation
  - Pivot: drafting data broker registration
- 2022
  - Short legislative session, data broker legislation introduced
  - Return to drafting comprehensive legislation for 2023 session

DATA BROKER TRANSPARENCY

- LC 392 is a reintroduction of HB 4017A (2022)
- It will create a data broker registry for Oregon, housed at DCBS
- To do business in Oregon, a data broker will have to register with DCBS, and provide:
  - Contact information
  - Information about whether a consumer can “opt out” of the data broker’s collection and sale of their personal information
  - A method for requesting an opt out (if applicable)

OREGON CONSUMER PRIVACY ACT

- LC 390 applies to businesses who collect, use, store, disclose, analyze, delete, or modify personal data of:
  - ≥100,000 Oregon consumers and/or linkable devices; or
  - ≥25,000 Oregon consumers + ≥25% gross revenue from data sales
- Exemptions:
  - Public bodies
  - Deidentified data
  - Data already regulated under several federal laws
  - Conflict of law, legal process, law enforcement, security incident response, technical repairs, providing requested service, health & safety

OREGON CONSUMER PRIVACY ACT cont.

- Consumer rights
  - Right to know (categories of data processed, who data is disclosed to, and copy of the consumer's personal data)
  - Right to correction
  - Right to deletion
  - Right to opt-out (targeted advertising, sale, profiling)
  - Right to data portability

OREGON CONSUMER PRIVACY ACT cont.

- Heightened protections for "sensitive data"
  - Consent/opt-in required for processing of sensitive data
    - Personal data revealing racial or ethnic background, national origin, religious beliefs, mental or physical condition or diagnosis, sexual orientation, gender identity, crime victim status, or citizenship or immigration status
    - Genetic or biometric data
    - Precise geolocation data

OREGON CONSUMER PRIVACY ACT cont.

- Heightened protections for children and youth
  - Personal data from a child (under 13 years old)
    - Must follow requirements of the federal Children's Online Privacy Protection Act (COPPA)
  - Personal data from a youth (13 to 15 years old)
    - Consent/opt-in required for targeted advertising and sale

OREGON CONSUMER PRIVACY ACT cont.

- Controller obligations
  - Privacy notice, including:
    - Categories of data processed
    - Purposes for processing data
    - How to exercise consumer rights
    - Categories of data shared with third parties
    - Categories of third parties receiving data
    - Contact information

OREGON CONSUMER PRIVACY ACT cont.

- Controller obligations cont.
  - Limit the collection of personal data to what is adequate, relevant and reasonably necessary for purposes set out in privacy notice
  - Must obtain consent to process data beyond specified purposes set out in privacy notice
  - Maintain reasonable data security practices
  - Non-discrimination for exercising rights
    - Exception: loyalty rewards programs

OREGON CONSUMER PRIVACY ACT cont.

- Processors obligated to assist controller in meeting obligations set out in the Act
- Deidentified data must stay deidentified
- Data protection assessments required for activities that present a heightened risk of harm to a consumer
  - Targeted advertising
  - Sale of data
  - Profiling + risk of unfair treatment, disparate impact or injury
  - Processing sensitive data