

# CSHB 159: Consumer Data Privacy

*An Act establishing the Consumer Data Privacy Act; establishing data broker registration requirements; making a violation of the Consumer Data Privacy Act an unfair or deceptive trade practice; and providing for an effective date*

# CSHB 159 Overview

- Duty of data brokers and businesses to inform consumers they will be collecting their data, and requiring their consent.
- CSHB 159 creates four consumer rights governing the collection and use of their personal data:
  - The right to request what information was collected.
  - The right to request a list of who that data was shared with.
  - The right to request that certain information not be shared, sold or disclosed.
  - The right to request for their information to be deleted.
- It adds protections for the data of minors: those 13 and younger must have a parent or guardian opt-in for them or give explicit consent to their information being collected.
- Provisions included for enforcement and enactment of those rights.
- Protections for bona fide businesses not engaged in sale, disclosure of information.
- Allows for consumers to use a global privacy signal or control.

## Article I, Sec 22 of the State Constitution:

*“The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.” [Amended 1972]*

# CSHB 159: Personal Information: Shared, Bought and Sold

Department of Law: *“In 2018, it was disclosed that Facebook has shared access to users' data with other tech firms, including Amazon, Apple, Microsoft, Netflix, and Spotify. Examples given by the New York Times include allowing others' products the ability to read users' private messages and to see the names, contact details, and activities of their friends....Facebook maintained they are not selling user data, but we must challenge that claim and ensure consumers can determine what is done with their personal data.”*

# CSHB 159: Personal Information: Shared, Bought and Sold (con't)

The information a consumer shares-knowingly or unknowingly- online creates thousands of data points showing often intimate details of a consumer or household, including health information, hobbies, religion, political views, personal loans, income, employment, political views, commercial preferences, age sex and gender-on almost any facet of daily life.

While data brokers insist that data in and of itself is anonymized or deidentified, specific information such as geolocation can be used to dramatically reduce anonymity-especially in combination with the thousands of other data points that may be attached to one consumer profile.

# CSHB 159: Personal Information: Shared, Bought and Sold (con't)

Once this information is collected, it can be bought, sold or shared; where it has been known to be used to:

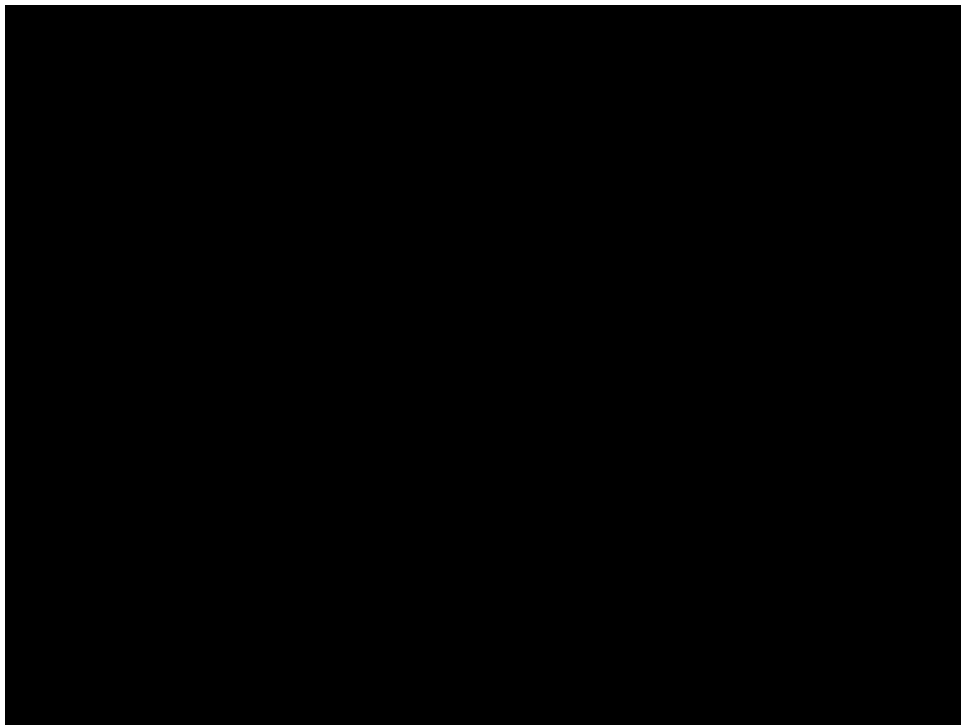
- Target high vulnerability audiences and markets such as seniors, tweens and teenagers;
- Perpetuate systematic racism in housing, lending, and deny coverage for certain types of insurance;
- Market pregnancy products to a consumer because numerous data points determine that they have a high chance of recently had sex, likely become pregnant, or changed sexual partners;
- Collect and market data of consumers, even if those consumers thought they had opted out of such data sharing;
- Collect precise geolocation data that can rapidly remove anonymity: In 2019, the NYT used one 2<sup>nd</sup> hand tranche of geolocation data to unmask numerous individuals, including journalists, Department of Defense officers, and software engineers interviewing at new firms.

# Personal Information: Shared, Bought and Sold (con't)

Video: Courtesy of NYT, the Privacy  
Project: *Twelve Million Phones,  
One Dataset, Zero Privacy.*

Pictured: Senior Defense  
Department official and his wife  
identified at the Women's March,  
Jan 21<sup>st</sup>, 2017.

*Originally posted 12.19.2019*



# An Industry without (much) Regulation

---

**MOTHERBOARD**  
TECH BY VICE

## Inside the Industry That Unmasks People at Scale

Unique IDs linked to phones are supposed to be anonymous. But there's an entire industry that links them to real people and their address.



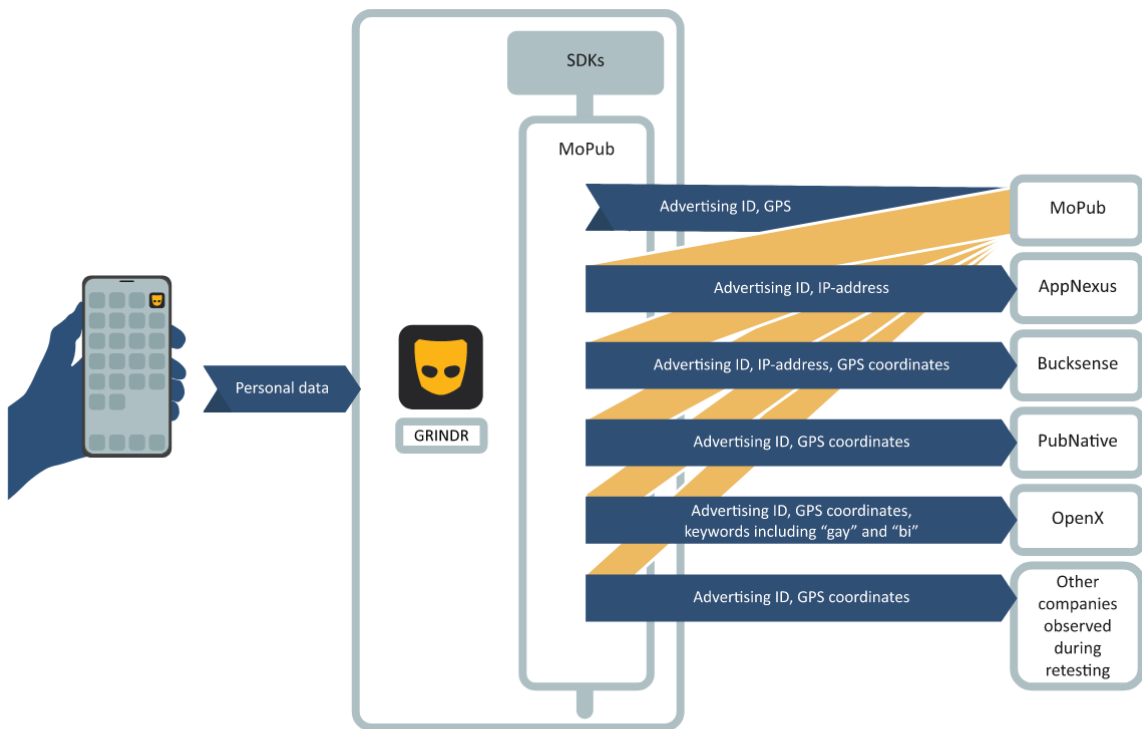
By [Joseph Cox](#)

It is not hyperbolic to state that consumer's information is sensitive personal information: it has immense value at scale, and data brokers are not necessarily harmless actors.








# Norwegian Privacy watchdog: dating apps sharing sensitive information with dozens of vendors.

- Dating apps such as Grindr made it very hard to opt out of location sharing with third party advertisers.
- The apps were sharing specific personal information such as precise GPS coordinates, sexual preferences, IP address, mobile advertising ID, answers to dating screening questions.



*35 Third parties receiving personal data through Twitter's MoPub mediation.*

## Other State models:

State	Right of Action	Consumer Rights	Employment Protections	Thresholds
CA	Y	Y	Y	\$25m/revenue, Data: 50k 
VA	N	Y	Y	50% revenue Data: 100k 
CO	N	Y	Y	Rev: 25k+  Data: 100k 
AK	Y	Y	Y	50% revenue Data: 100k 

# Enforcement

- Like the original draft, the consumer retains a right to private action if their personal information is subjected to unauthorized access, destruction, use, modification or disclosure. (Best practice from other states)
- Establishes a Consumer Privacy Account in General Fund. This is funded in part by civil actions brought by attorney general, subject to appropriation by legislature. Purpose is to fund Dept of Law attorneys for enforcement and oversight, as well as data broker fees.
- Requires businesses that meet legal threshold of collecting, sharing or selling personal information of 100,000 consumers or households (or 50% of their annual revenue from these activities) to register with DCCED as a data broker, and pay 3% fee of the revenue received by the business from the buying, sharing, or selling of the personal information of consumers or households to State for Consumer Privacy Account.

# Stakeholders

- Electronic Frontier Foundation
- Electronic Privacy information Center
- Consumer Reports
- Ashkan Soltani, California Privacy Bureau
- Lynden
- Banking companies
- Insurance providers

# Questions?

# Resources:

[Unique in the Crowd](#): The Privacy Bounds of Human Mobility 2013

[Out of Control](#): How consumers are exploited by the online advertising industry: Report by Norwegian Consumer Council, 2020

[New York Times: The Privacy Project](#) 2020

[Vice.com](#): Inside the Industry that Unmasks People At Scale 2021

[The Verge](#): Why Apple's New Privacy Feature Is Such a Big Deal 2021

[The Facebook Files](#): Wall Street Journal 2021