

\$5 per pound



16 October 2019

Third Parties and the CCPA: Data Sharing and Selling

Adriana Beach

Privacy & Data Protection Counsel, 23andMe

Darren Abernethy, PLS/FIP/CIPP

Senior Counsel, TrustArc

Gretchen Ramos, CIPP/E/US, CIPM

Co-Chair, Greenberg Traurig Data, Privacy &
Cybersecurity Group

- **The Basics - Setting the Groundwork**
 - CCPA Principles
 - Key Concepts
 - Third Parties, Personal Information, Selling
- **The Real Story**
 - Seamless Selling – the Digital Advertising Landscape
- **What's Not a Sale**
 - Exceptions to Selling
- **Paying for Data Permitted**
- **Opting Out Procedures**
- **Questions**



The Basics

Understanding the basics before we dig in to the really fun part!

the really fun part;

understanding the basics before we dig in to

The Purpose of the CCPA



California Legislature

- Determined “the law has not kept pace with rapid technological developments ... as a result, consumers are largely unable to control or even understand the collection and use of their personal information by a myriad of businesses and organizations.”
- Implemented the CCPA to resolve this issue requiring businesses provide consumers:
 - **Notice** - the right to know (a) details about how their personal information is collected, used and shared by a business, and (b) their rights in relation to their personal information
 - **Control** - the right to take control of their information by having businesses delete it and stop selling it
 - **Free Exercise of Rights** - the right to assert these rights without suffering discrimination in price or service

THIRD PARTIES



EXPLAINED

THE BEST
WE CAN



Third Parties – Sec. 1798.140 (w) & 1798.115 (d)

Who are Third Parties

- ✓ Defined in the negative as basically a person who is NOT a “business” (w)(1), or a “service provider” (w)(2).

Third Parties’ Obligations

- ✓ A Third Party shall not sell PI that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120. If a Third Party violates a CCPA provision, it shall be liable.

Responsibilities of Business Sharing Personal Information with a Third Party

- ✓ Business disclosing PI to Third Party will not be liable under CCPA if Third Party uses it in violation of the restrictions set forth CCPA **provided that**, at the time of disclosing the PI, the business *does not have actual knowledge, or reason to believe*, the Third Party intends to commit such a violation.

Third Parties – Proposed Regulations



Defines “Categories of third parties” to mean:

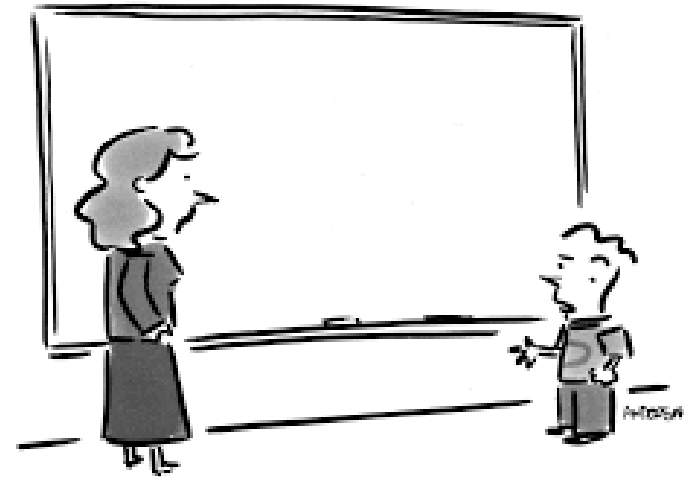
types of entities that do not collect personal information directly from consumers, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers.



Personal Information

Section 1798.140 (o)

Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.



"Before I write my name on the board, I'll need to know how you're planning to use that data."

125+ Types of Personal Information

Identifiers & Characteristicsⁱ

- real name
- signature
- user alias / account name
- unique pseudonym
- customer number
- postal address
- email address
- social security number
- driver's license number or state identification card number
- passport number
- telephone number
- insurance policy number
- military or veteran status
- national origin
- race
- age (over 40)
- color
- religious creed
- sex/gender
- gender identity
- gender expression
- sexual orientation
- marital status

Education Informationⁱⁱ

- education
- student's report card & transcript
- student's disciplinary record
- student's dates of attendance
- student's honors and awards
- student's participation in officially recognized activities/sports

Electronic Dataⁱⁱⁱ

- Internet Protocol (IP) address
- device identifier
- cookies
- beacons
- pixel tags
- mobile ad identifiers
- physical characteristics or description
- browsing history
- search history
- consumer's click stream
- geolocation data (latitude and longitude coordinates; postal/zip code)
- contents, sender, recipients, format, or location of the sender or recipients at any point during electronic communication
- time or date electronic communication was created, sent, or received
- any information pertaining to any individual or device participating in electronic communication
- information stored on or generated through operation of electronic device (including current and prior locations of electronic device)

Commercial Information^{iv}

- products or services purchased, obtained, or considered
- other purchasing or consuming histories or tendencies
- records of personal property

Employment Information^v

- employment status
- employment history
- request for family care leave
- request for leave for an employee's own serious health condition
- request for pregnancy disability leave
- employee's job application file
- employee's personal file
- employee's payroll/benefits information
- employee's leave/medical file
- resume
- employment contract
- independent contractor agreement
- performance review
- disciplinary record

Biometric & Physical Information^{vi}

- imagery of the iris & retina
- imagery of the face
- any other physiological characteristics
- fingerprint, hand, palm, vein patterns
- voice recordings
- keystroke patterns or rhythms
- audio recordings
- visual information
- thermal information
- olfactory information

Financial Information^{vii}

- bank account number
- credit card number
- debit card number
- any other financial information

Health Information^{viii}

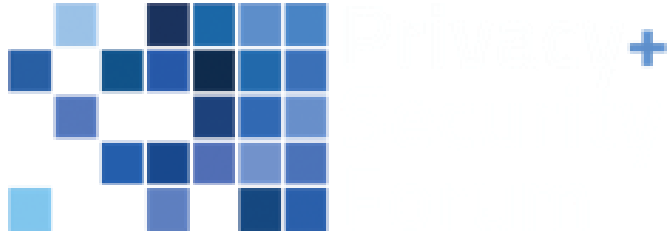
- any medical information
- medical condition (genetic characteristics, cancer or a record or history of cancer)
- health insurance information
- sex/gender (includes pregnancy, childbirth, breastfeeding and/ or related medical conditions)
- ancestry
- disability (mental and physical including HIV/AIDS, cancer, and genetic characteristics)
- genetic information / individual's deoxyribonucleic acid (DNA)
- gait patterns or rhythms
- sleep, health, or exercise data
- retaliation for reporting patient abuse in tax-supported institutions

Inferred Data^{ix}

- Inferences drawn from any individual data element or combination of Personal Information
- Any derivation of Personal Information
- Any profile or segment attributed to an individual
- Consumer identification more likely than not
- Any predicted characteristics or trait

Selling...

A Very Broad Definition



1798.140 (t) (1)

“Sell,” “selling,” “sale,” or “sold,” means selling, *renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally*, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party *for monetary or other valuable consideration*.

Valuable Consideration

- Assuming term is interpreted consistent with existing contract law, “valuable consideration” would encompass any exchange of personal information where the transferring entity receives **any benefit** to which it is not legally entitled.
- Unlike Nevada’s new law (SB 220), CCPA covers many more activities than simply selling data to another company for money.





Adtech.....

Personal Information Flowing Everywhere....

Behavioral Advertising



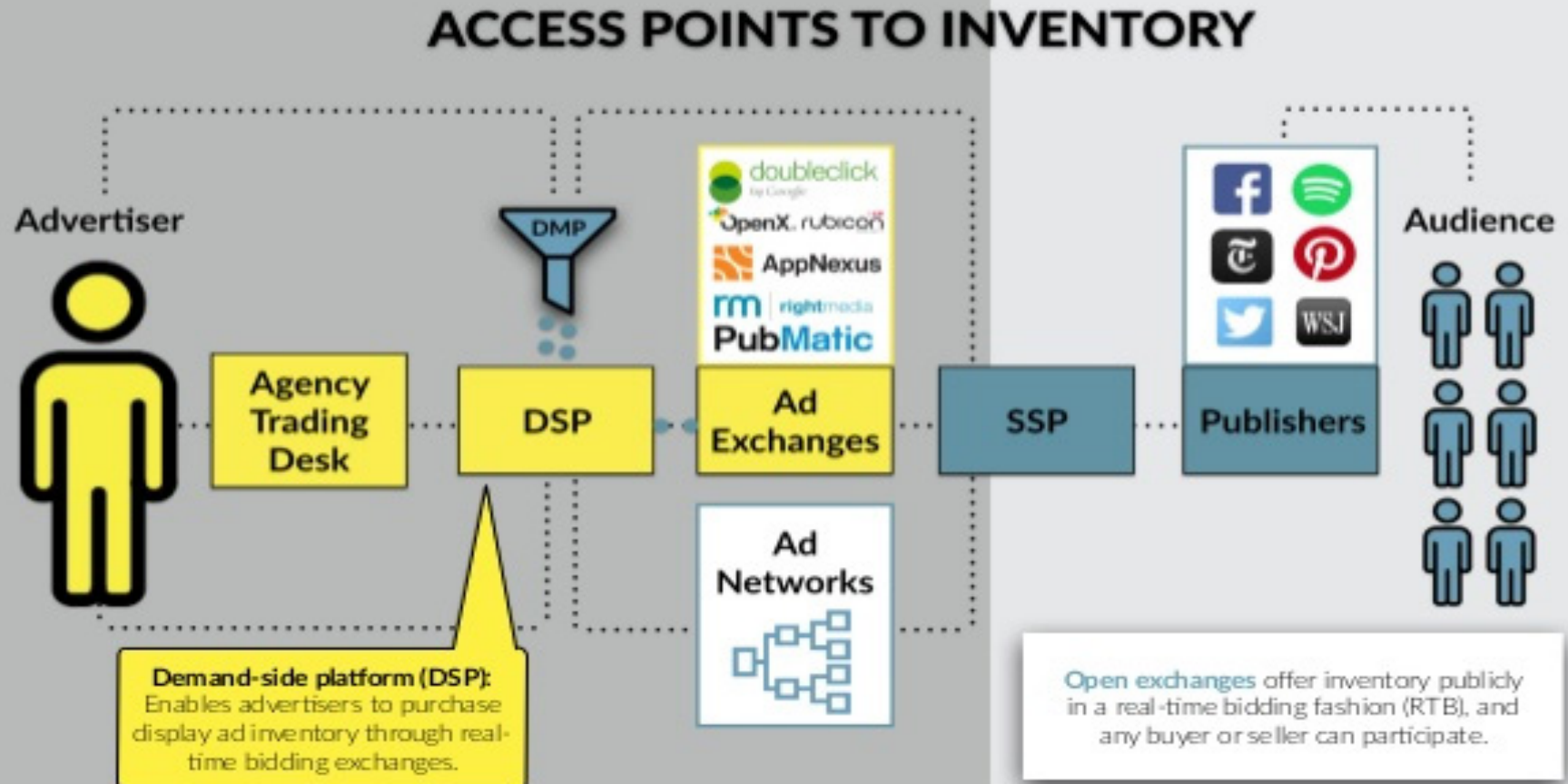
Adtech Alphabet Soup – It's Complicated

September 2012



How the Process Works

Source: <https://tinyurl.com/y3a3sjxz>



Exceptions to Selling

Understanding When a Sale Is Not a Sale....



Exceptions to Selling

- ✓ Consumer consents to sale, and third party does not sell PI, unless disclosure would be consistent with CCPA.
- ✓ PI shared with third party to advise that consumer is opting-out of a sale.
- ✓ PI shared with service provider that is necessary to perform a business purpose.
- ✓ PI transferred to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business.



Exceptions to Selling - Consent



Privacy +

2) (A) For purposes of this title, a business does not sell personal information when a consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the **third party does not also sell the personal information**, unless that disclosure would be consistent with the provisions of this title.

- An intentional interaction occurs when the **consumer intends to interact** with the third party, via one or more **deliberate interactions**.
- Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.



Exceptions to Selling - Consent

| GDPR | CCPA |
|--|---|
| <p>Consent of the data subject means any <i>freely given, specific, informed and unambiguous</i> indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.</p> | <p>Consent not defined; however deliberate act appears to be required.</p> <p>Lack of consent definition may leave open the possibility of a broad consent mechanism which includes further sharing by third parties subject to compliance with other CCPA provisions such as notice.</p> |

Yes – Financial Incentives are Permitted

Paying for Data Under the CCPA

Offering Financial Incentives

- A business can offer a financial incentive to a consumer in exchange for allowing the business to sell the consumer's data as long as any price difference is reasonably related to the value of the consumer's data.
- If business offers financial incentive it must provide consumers with an explanation of why the financial incentive is permitted under the CCPA, a good-faith estimate of the value of the consumer's data in relation to the financial incentive, and a description of the method used to calculate the value.
- A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.125(b)(3) which clearly describes the material terms of the financial incentive program, and that consent may be revoked by the consumer at any time.



Calculating the Value of Consumer Data

Pursuant to the proposed Regulations, a business offering financial incentives must use (and document) a reasonable and good-faith method for calculating the value of their consumer data. The business must use one or more of the following methods:

- ✓ The *marginal* value of the sale, collection, or deletion of an average consumer's data
- ✓ The *average* value of the sale, collection, or deletion of an average consumer's data
- ✓ Revenue or profit generated by the business from separate tiers or classes of consumer data
- ✓ Revenue generated by the sale, collection, deletion or retention of consumer data
- ✓ Expenses related to the sale, collection, deletion or retention of consumer data
- ✓ Expenses related to the offer, provision, or imposition of any financial incentive or price difference
- ✓ Profit generated by the business by the sale, collection, deletion or retention of consumer data
- ✓ Any other practical or reliable method of calculation used in good faith

Opt-Out Procedure....

How It Works If You Sell



Notice of Opt Out Right

- ✓ Notice of the right to opt out of a sale should inform consumers of their right to direct a business that sells (*or may in the future sell*) their personal information to stop selling and refrain from doing so in the future.
- ✓ A business is exempt from providing a notice of the right to opt out if it does not and will not sell personal information during the time period during which the notice is not posted, and it states this in its privacy policy.
 - ✓ When a business' privacy policy states this, a consumer whose personal information is collected while that policy is not in place "shall be deemed to have validly submitted a request to opt-out."

Notice of Opt Out Right

- ✓ Not only must the opt-out notice advise of the right to opt out and provide a link to the business's privacy policy, but it must also include information about:
 - ✓ the webform by which consumers can submit their opt-out requests online;
 - ✓ where the business does not operate a website, the offline method a consumer can use to opt out;
 - ✓ instructions on any other methods a consumer can use to opt out; and
 - ✓ the proof required when a consumer uses an authorized agent to exercise their opt-out rights.



Website Format

- ✓ A business that sells personal information “shall post the notice of the right to opt-out on the Internet webpage to which the consumer is directed after clicking on the ‘Do Not Sell My Personal Information’ or ‘Do Not Sell My Info’ link on the website homepage or the download or landing page of the mobile application.”
- ✓ An opt-out button or logo “may be used in addition to posting the notice of the right to opt-out, but not in lieu of any posting of the notice.”





Business Must Notify Third Party

Pursuant to proposed Regulations, business must inform third parties of consumer's opt-out request.

A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.



Business Must Wait a Year

- Pursuant to proposed Regulations, business must wait a year before seeking to sell consumer's data again.

“For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.”



12
Months

Questions + Contact



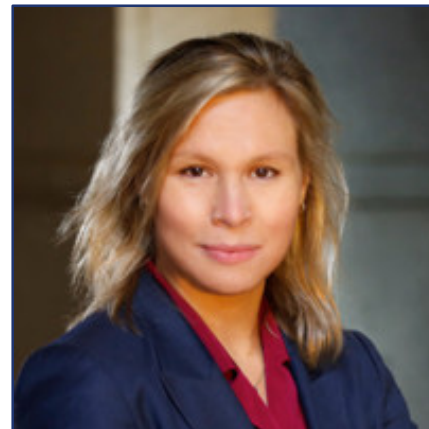
Darren Abernethy

Senior Counsel
TrustArc
415.766.6451
darren@trustarc.com



Adriana Beach

Privacy & Data Protection
Counsel, 23andMe
650.938.6300
adrianab@23andMe.com



Gretchen Ramos

Co-Chair, Greenberg Traurig's Data,
Privacy & Cyber Group
415.655.1319
ramosg@gtlaw.com