October 23, 2020

An Update on the Regulation of Tracking for Ad Targeting and Analysis Around the World

Brandy Walsh
Acxiom

Reed Freeman
Venable

Chelsea Reckell
Venable

Privacy+ Security Forum

Speaker

Brandy Walsh

Privacy Attorney, Acxiom

Brandy Walsh is the Privacy Attorney at Acxiom. She is responsible for assisting the Chief Data Ethics Officer in privacy-related legislative interpretation; privacy impact assessments; and data sourcing resolution.

Bio at:
https://www.acxiom.com/people/brandy-walsh/

Speaker

Reed Freeman

Partner, Venable

Bio at:
https://www.venable.com/professionals/f/d-reed-freeman-jr

Speaker

Chelsea Reckell

Associate, Venable

Bio at:
https://www.venable.com/professionals/r/chelsea-b-reckell

Online Behavioral Advertising in the USA – Legal Framework

Online Behavioral Advertising in the USA

No National Privacy Law in the USA

- **Instead, USA has a sectoral approach by industry**
  - HIPAA, GLBA, FCRA, VPPA, COPPA
  - No specific statute governing digital advertising

- **FTC and self-regulatory groups have filled the void**
  - FTC: Report on Online Behavioral Advertising (2009); Privacy Report (2012); Blog: Keeping Up with the Online Advertising Industry (2016)
    - Device IDs, IP address, cookies considered personal data if reasonably linked to a person or device
  - NAI Code of Conduct (2020); ANA Code of Conduct; DAA Principles
    - Focus: notice, transparency, and choice

Online Behavioral Advertising in the USA

Comprehensive federal privacy law in 2021?

- Potentially: dozens of bills introduced in Congress over the past several years.
- Privacy for America Initiative

A few of note:

- **SAFE DATA Act** (Sen. Wicker (R-MS)) (Sept. 2020) (S. 4626 - Introduced and referred to Senate Commerce, first Introduced Nov. 2019 as a discussion draft)
  - Comprehensive privacy bill with additional authority to the FTC;
  - Consumer rights with respect to their data, including data portability;
  - No private right of action;
  - Would preempt state privacy, data security, and state data breach notification laws.
- **Consumer Data Privacy and Security Act of 2020** (Sen. Jerry Moran (R-KS)) (March 2020) (S. 3456 – Introduced and referred to Senate Commerce)
  - Comprehensive privacy bill with additional authority to the FTC;
  - Consumer rights with respect to their data, including data portability;
  - No private right of action;
  - Would preempt state privacy, data security, and state data breach notification laws.
- **Consumer Online Privacy Rights Act** (COPRA) (Sen. Cantwell (D-WA)) (Nov. 2019) (S. 2968 – Introduced and referred to Senate Commerce)
  - Comprehensive privacy law with additional authority to the FTC;
  - Consumer rights with respect to their data, including data portability;
  - Private right of action;
  - Would preempt state laws ONLY if they directly conflict with the provisions of the Act.
- **Data Protection Act** (Sen. Gillibrand (D-NY)) (Feb. 2020) (S.3300 – Introduced and referred to Senate Commerce)
  - Establishes a federal Data Protection Authority to enforce federal privacy law and take action to prevent entities from engaging in unfair or deceptive practices;
  - Provides for civil monetary penalties.

Online Behavioral Advertising in the USA

- High-profile matters have increased privacy awareness.
- FTC stepping up in the absence of federal privacy legislation.
- U.S. states are growing impatient, and are no longer waiting for a national privacy law from Congress.

TechCrunch

FTC fines kids' app developer HyperBeard $150K for use of third-party ad trackers

Sarah Perez @sarahintampa / 6:34 pm EDT • June 4, 2020

Comment

Online Behavioral Advertising in the USA

California Consumer Protection Act (CCPA)

Passed by the California State Legislature and signed into law on June 28, 2018

- Passed by the Legislature after only one week of debate.
- Effective January 1, 2020, enforcement began July 1, 2020.
- The California Attorney General issued the latest version of regulations in August 2020, but new modifications and a comment period were proposed on October 12, 2020. It's unclear where AdTech provisions will net out.

- **Scope**: Any for-profit business that collects or controls California consumers' personal information and (1) has an annual gross revenue over $25 million, (2) annually collects personal information from 50,000 or more Californian consumers, households, or devices, or (3) derives 50% of annual revenues from selling California consumers' personal data.

- **Enforcement**: California Attorney General – Civil
  - $7,500 for each intentional violation; $2,500 for each unintentional violation

Online Behavioral Advertising in the USA

CCPA is not a comprehensive privacy and data protection framework – it is not GDPR – but it provides a suite of consumer privacy rights. These include:

1. **Notice**: Requirement to include specific information in privacy policies (including a few CCPA-specific disclosures)
2. **Access and portability**: Right to **access** personal information (collected in the last 12 months) and **receive** such information in a readily usable and portable format, if provided electronically (commonly referred to as "portability")
3. **Deletion**: The right to request deletion of personal information (subject to exceptions)
4. **Opt out**: The right to opt out of selling personal information to third parties; if a minor (>16), the right to opt in to sell personal information on minors
5. **Non-discrimination**: The right to equal services and prices if consumers exercise their CCPA rights

Online Behavioral Advertising in the USA

CCPA's broad definition of Personal Information – Ad Tech IDs included

- "**Personal information**" is defined as "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."
- **Relevant for digital advertising**:
  - "**Unique identifier**" or "**Unique personal identifier**" = a persistent identifier used to recognize a consumer, family, or device that is linked to a consumer or family, over time and across different services
  - "**Probabilistic identifier**" = the identification of a consumer or a device to a degree of certainty more probable than not based on any categories of data enumerated in the definition of personal information.
- **Also:** Purchase history, interactions with website or apps, IP address, and **inferences drawn therefrom to create a profile on a consumer**

Online Behavioral Advertising in the USA

CCPA distinguishes between businesses that collect personal information and businesses that sell personal information

- **Businesses that collect personal information**
  - Collect means "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means either passively, actively, or by observing the consumer's behavior."
  - Applies to the Ad Tech's intake of online and offline data.

- **Businesses that sell personal information**
  - Sell 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."
  - Applies to the Ad Tech's delivery of online and offline data.

Online Behavioral Advertising in the USA

Privacy+ Security Forum

CCPA compliance requires operational, legal, and compliance tasks

Operational: Develop processes to:

- Generate reports in a portable electronic format
- Delete personal information (online and offline)
- Respond to access and deletion requests from customers

Legal:

- Update agreements, privacy policy, and website links
- Conduct due diligence on inbound and outbound partners

Compliance:

- Train employees handling consumer rights requests
- Set up toll-free number
- Confirm that existing opt-out capabilities conform to the requirements

Online Behavioral Advertising in the USA

California Privacy Rights Act (CPRA)

Californians will be voting on the CPRA on November 3, 2020. The CPRA materially amends the CCPA.

- The CPRA ballot initiative was proposed by the group that initiated the CCPA, the Californians for Consumer Privacy, founded by real estate developer Alastair Mactaggart.

- If passed, the CPRA would go into effect January 1, 2023, but there would be a "look-back" period beginning on January 1, 2022 for access rights.

- **Scope**: The CPRA would change the CCPA threshold from 50,000 to 100,000 or more consumers or households; it would remove devices from the threshold. It also adds "contractor" as a new entity and changes the definition of "third party."

Online Behavioral Advertising in the USA

Competing Laws: CCPA vs. CPRA

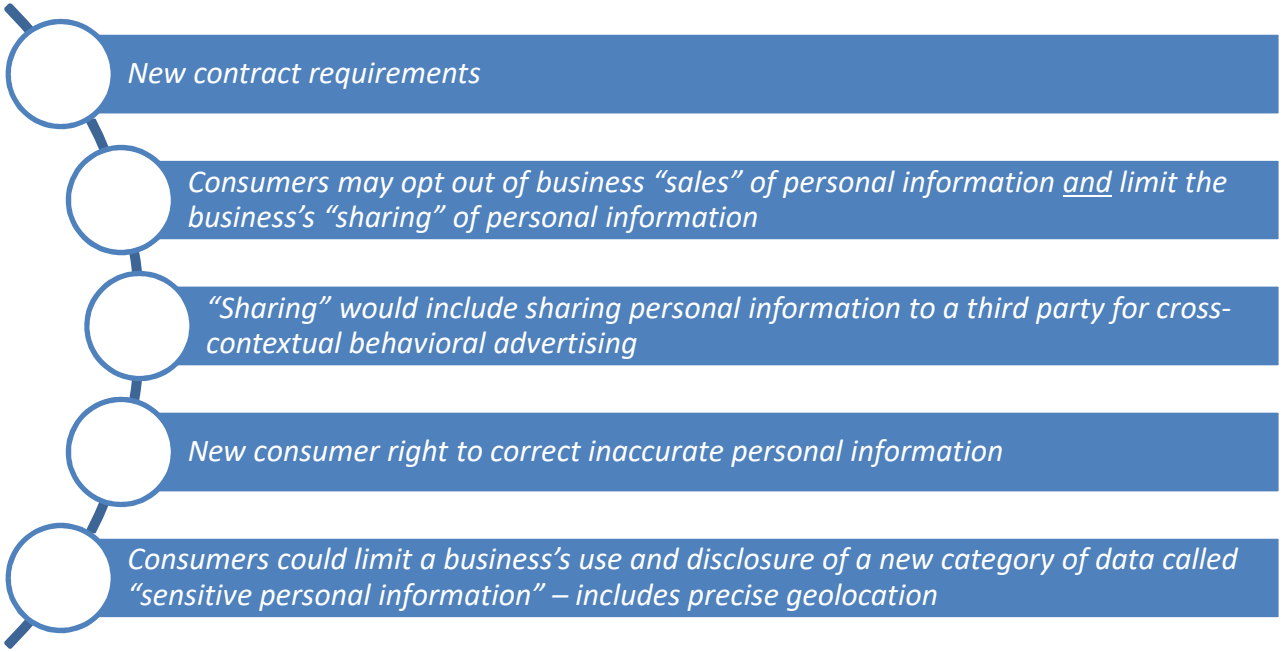
- The CPRA doesn't repeal the CCPA, resulting in possible conflict with competing or unclear provisions. Businesses may have to balance compliance across regimes.

- Possible conflicting regulations with additional regulations to come from a newly created agency, the California Privacy Protection Agency.

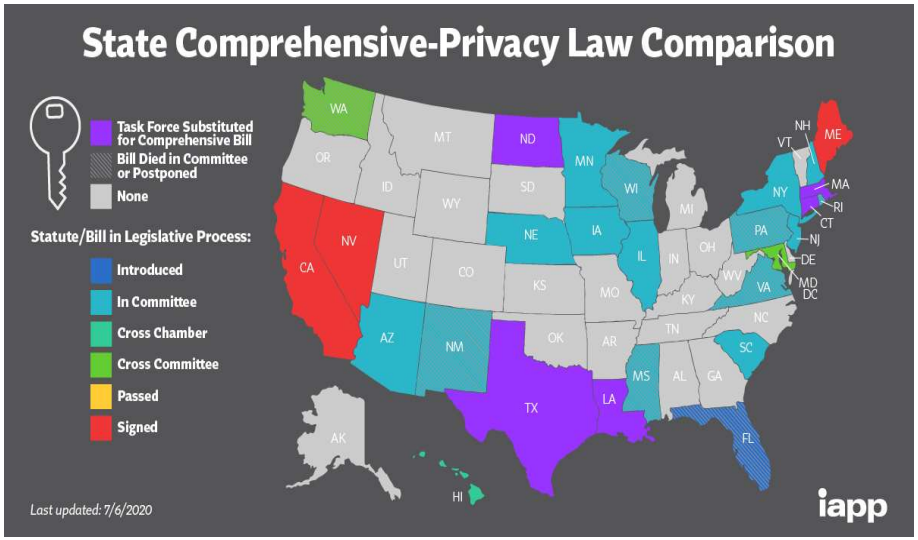
- Implications for AdTech to be determined. Issues already arising; for example, differing interpretations around browser opt-outs.

Online Behavioral Advertising in the USA

CPRA vs. CCPA. Some of the material amendments include:



Online Behavioral Advertising in the USA



CCPA/CPRA is just the beginning, absent federal preemption.

- Many other U.S. states considered similar privacy bills last year, and we expect that trend to be at least as broad in 2021 and beyond.
- Nevada and Maine already have privacy bills, but they are much more limited in scope than the CCPA (Maine: broadband providers; Nevada: certain website operators)

Online Behavioral Advertising in the USA

Privacy+ Security Forum

Ecosystem Changes: Global Privacy Controls

- Recently, a group of NGOs, publishers, and browsers released the beta version of a browser extension that functions as a global control.

- The control will enable consumers to cast a single opt-out signal across the entire Internet instead of making specific, business-by-business selections regarding who can and cannot engage in transfers of personal information.

Online Behavioral Advertising in the USA

Ecosystem Changes: Google Announcement

- In January of 2020, Google announced it intends to stop supporting all third-party cookies in its Chrome browser by 2022.
- By their nature, third-party cookies allow entities to collect data across the Internet on any website where an entity has placed such a cookie.
- Third-party cookies are commonly used to **serve customized advertising content**, measure the effectiveness of such advertising, attribute payments, measure audiences, and in other use cases.

Online Behavioral Advertising in the USA

Ecosystem Changes: Apple Announcement

Apple recently announced technological and policy changes that will restrict how app developers and their partners access and use the IDFA provided by the iOS platform. The changes are intended to go into effect next year.

- The IDFA enables advertisers to link data and customize and measure advertising across iOS apps on a single device.
- Apple will require app developers, on an app-by-app basis, **to obtain affirmative (opt-in) consent** from the iOS device user for "tracking" in order to access the device's IDFA.
- To obtain consent, the developer must include a prompt in its app stating that "[App Name] would like permission to track you across apps and websites owned by other companies." Users will then select either "Allow Tracking" or "Ask App Not to Track."

Online Behavioral Advertising in Europe

Online Behavioral Advertising in Europe

Privacy+ Security Forum

Relevant Landscape:

- **e-Privacy Directive (including member country variations)**
- **General Data Protection Regulation (GDPR)**
- **e-Privacy Regulation**

e-Privacy Directive

Privacy+ Security Forum

Online Behavioral Advertising in Europe

e-Privacy Directive

- Initially adopted in 2002; amended in 2009
- Commonly referred to as the “Cookie Law”
    - Responsible for the cookie banners you see on almost every site
- Because it is a directive, it is not binding on EU member states until they adopt it into law
    - Has resulted in many different variations
    - Fines under the law also vary based on jurisdiction
- Works in conjunction with the GDPR
- Criticized for being outdated→ supposed to be replaced by the e-Privacy Regulation

Online Behavioral Advertising in Europe

e-Privacy Directive

- General rule is that users must provide informed consent prior to having their cookies stored or before the user is tracked
- Consent must be informed and active
    - Different jurisdictions have interpreted this requirement differently (implicit vs. explicit consent)
- Exception for technical storage and cookies that are strictly necessary in order for a service to be provided
- Also requires a cookie policy

DPA Cookie Guidance

Privacy+ Security Forum

Targeted Advertising in Europe

A number of EU countries have issued guidance on the use of cookies through their DPAs and other government agencies:

Ireland (April 2020)	Belgium (April 2020)	Cyprus (July 2019)	United Kingdom (July 2019)	Germany (March 2019)
Spain (July 2020)	France (October 2020)	Czech Republic (May 2018)	Denmark (February 2020)	Finland (May 2020)
Greece (February 2020)	Hungary (July 2018)	Italy (October 2019)	Latvia (June 2018)	Lithuania (2018)
Netherlands (December 2019)	Slovenia (July 2019)			

Online Behavioral Advertising in Europe

DPA Cookie Guidance: Similarities

- To the extent that consent is required, it must be informed, specific, freely given, and unambiguous
    - Continuing to browse a website is likely *insufficient* for valid consent in most jurisdictions—particularly following the recent release of relevant GDPR guidance on cookies
- Requirements are not limited to cookies; they apply to any technology which can store and access device information (pixels, tags, etc.)
- Consent should be granular and businesses should name first and third parties who are relying on consent

Online Behavioral Advertising in Europe

DPA Cookie Guidance: Key Differences

- The UK and Ireland require consent for analytic cookies, while other jurisdictions exempt analytic cookies from the consent requirement.
- The UK suggests that legitimate interest is likely an inappropriate lawful basis for processing cookies in most circumstances, while France, Belgium, and Germany are more open to lawful bases other than consent.
- Cookie lifespan requirements vary, with some jurisdictions (France and Spain) having specific time requirements, while others (UK and Germany) implement proportionality and balance of interest tests.

General Data Protection Regulation (GDPR)

Online Behavioral Advertising in Europe

General Data Protection Regulation

- Went into effect May 2018

- Regulates "personal data," which includes online identifiers and identification numbers. GDPR, art. 4(1). Could include cookies, mobile identifiers, IP addresses, etc.

- Fines under the GDPR can be as high as 20 million Euros or 4 percent of annual worldwide turnover

Online Behavioral Advertising in Europe

General Data Protection Regulation

- Creates individual rights for EU residents

Online Behavioral Advertising in Europe

General Data Protection Regulation

- Cookies are regulated by both the GDPR and the e-Privacy Directive

- The GDPR requires one of six legal bases for processing personal data:
  - Consent;
  - Performance of a contract;
  - Legitimate interest;
  - Vital interest;
  - Legal requirement; or
  - Public interest

Online Behavioral Advertising in Europe

General Data Protection Regulation

- If processing cookies on the basis of consent, consent must be freely given, specific, informed, and unambiguous to be valid

- Various European supervisory authorities have provided guidance related to consent

- In May 2020, the European Data Protection Board (EDPB) adopted an updated set of guidelines on consent under the GDPR. Per the guidelines:
  - Cookie walls are not a valid means of obtaining consent, as data subjects are not presented with a genuine choice

  - Scrolling or swiping through a web page is ambiguous and cannot form the basis of valid consent

Online Behavioral Advertising in Europe

Privacy Shield Invalidated

- The GDPR provides that the transfer of personal data to a country outside of the EU may take place only if the country in question ensures an adequate level of data protection – many U.S. companies accomplished this through Privacy Shield certification.

- In July 2020, the Court of Justice of the European Union (CJEU) determined that the EU-U.S. Privacy Shield was no longer valid as a lawful personal data transfer mechanism in the case of *Data Protection Commissioner vs. Facebook Ireland Limited and Maximilian Schrems* (Schrems II).

- Companies now have to make sure they have Standard Contractual Clauses in place and additional safeguards for transfers of personal data from Europe to the United States. The EDPB has promised to issue something soon on what those should look like.

e-Privacy Regulation

Privacy+ Security Forum

Online Behavioral Advertising in Europe

e-Privacy Regulation

- Would replace e-Privacy Directive in terms of regulating electronic communications activity in EU member states
  - Because it is a regulation and not a directive, it would be binding on EU members immediately

- Would supplement the GDPR, though it will likely override the GDPR with respect to regulating electronic communications

- Initial draft was proposed by the EU Commission in January of 2017

- EU Council proposed a revised version in February of 2020

- Will need to pass European Parliament, European Council, and the European Commission to go into effect

Online Behavioral Advertising in Europe

e-Privacy Regulation

- Latest version of e-Privacy Regulation proposed by the European Council would allow electronic communication networks or service providers to process electronic communications metadata pursuant to their legitimate interests (as opposed to consent) if they implement certain safeguards
    - The June 2020 progress report released by the Presidency of the Council of the European Union highlighted that this change was met with mixed reactions from EU member states
- The latest version of the e-Privacy Regulation would also allow an end-user to grant consent to process cookies through browser settings
- Currently, deliberations on the draft have been postponed due to COVID-19

Online Behavioral Advertising in Asia

Privacy+ Security Forum

Asia

- The world's digital capital
- Asia-Pacific Economic Cooperation (APEC) and the move to regional harmonization
  - **2004 APEC Privacy Framework, updated in 2015**—Principles and guidelines intended to establish privacy protections to facilitate cross-border information transfers
  - **2011 APEC Cross Border Privacy Rules**—Directive to implement the APEC Cross Border Privacy Rules System
- Impact of GDPR and status of international data transfers

Asia

South Korea

- Personal Information Privacy Act (PIPA)
  - Amended in January 2020
- The Network Act

Japan

- The Act on the Protection of Personal Information 2017
  - Amended in June 2020; effective in 2022
- Japan Fair Trade Commission (JFTC) Guidelines
  - JFTC has publicly stated it is exploring cookie regulations

China

- Cyber Security Law 2017
- Draft Data Security Law
  - Released in July 2020
- Interim Measures for the Administration of Internet Advertising

Hong Kong

- Personal Data Ordinance
  - Currently under review by the Hong Kong government
- Unsolicited Electronic Messages Ordinance
- Guidance from Hong Kong Privacy Commissioner

Asia

India

- Personal Data Protection Bill 2020
- Proposed Non-Personal Data Framework
  - In July 2020, a Committee of Experts designed by the Ministry of Electronics and Information Technology issued a report seeking feedback on a proposed framework and proposed law
- Data localization

Thailand

- Personal Data Protection Act (PDPA) 2020
  - The implementation has been delayed until May 31, 2020, but specified requirements—such as security obligations—apply to certain data controllers currently

Singapore

- Personal Data Protection Act (PDPA)
  - Amendments were proposed in October 2020

Asia

	South Korea	China	Japan	Hong Kong	India	Singapore	Thailand
EU Adequacy?	Ongoing talks	✗	✓	✗	✗	✗	✗
Prior Consent?	✓	✗	✗*	✓**	✗	✓	✓
Localization?	✗	✓	✗	✗	✓	✗	✗
Significant changes?	2020	2020	2020	Possibly forthcoming	2020	Possibly forthcoming	2020

*Subject to change after the amendments to the Act on the Protection of Personal Information go into effect in 2022.
**To the extent that information collected is "personal data."

Targeted Advertising in South America

Privacy+ Security Forum

South America

- Legislative similarities country to country, but no common framework
- Constitutional principle of “habeas data”—”have the data”
  - E.g., Argentina, Brazil, Peru, Paraguay
- Often require express consent for data transfers
- Unlike in the EU, South American countries typically have frameworks that *can* apply to cookies and tracking technologies but do not have specific guidance or laws regarding such

South America

Argentina

- Personal Data Protection Act 2000
  - Influenced by the EU Data Protection Directive
- Regulations by AAIP

Brazil

- General Data Protection Law (LGPD)
  - GDPR-style law
  - Effective as of September 2020
  - Sanctions are delayed until August 2021
- Marco Civil

Chile

- Chilean Data Protection Act
  - First in region to adopt a data protection law—amended in 2018

Peru

- Personal Data Protection Law 2011 and its 2013 Regulation
  - Establishes requirements for information to be disclosed when obtaining consent

South America

	Argentina	Brazil	Chile	Peru
EU Adequacy?	✔	✕	✕	✕
Prior Consent?	✔	✔	✔	✔
Significant changes?	Possibly forthcoming	2020	Possibly forthcoming	N/A

Takeaway: Global Compliance Strategy

1. Data map: Know what information you are collecting, whom you are transferring it to, and for what purposes.

2. Identify the rules and regulations that potentially apply to you.

3. Develop a mechanism to obtain proper legal basis for use of cookies, pixels, and other tracking technologies.

4. Comply with jurisdictional requirements regarding electronic communications storage and cross-border transfer and confer with counsel regarding the changing landscape in light of *Schrems II.*

5. Implement reasonable security procedures.

6. Keep up with the evolving business and regulatory landscape.

Questions + Contact

Brandy Walsh
Privacy Attorney,
Acxiom
Brandy.Walsh@acxiom.com

Reed Freeman
Partner,
Venable
rfreeman@Venable.com

Chelsea Reckell
Associate,
Venable
creckell@Venable.com