California Consumer Privacy Act

CCPA: Questions we'll address

1. What is the California Consumer Privacy Act?
2. What are the implications for international businesses?
3. What is IAB doing to shape the outcome of the law?
4. How does CCPA relate to broader U.S. privacy developments?
5. How can businesses learn more and get further involved?

How did we get here?

Early 2018: Alastair Mactaggart spearheads efforts to include a new privacy law on the November 2018 California ballot

June 2018: Alastair Mactaggart receives enough signatures to earn place on ballot, prompting the California Legislature to negotiate a substitute bill, the CCPA, in exchange for dropping the ballot initiative

June 28, 2018: Governor Brown signs the law one week after it was introduced in the legislature

What is the timeline for the law?

Signed into law by Governor Brown on June 28, 2018

Goes into effect on January 1, 2020

Enforcement begins on July 1, 2020 or six months after regulations are adopted by the State Attorney General

Who is covered?

A business, meaning a legal entity organized or operated for the profit or financial benefit of its owners, that:

1. collects consumers' personal information
2. determines the purposes and means of the processing of consumers' personal information, and
3. Does business in California or with California residents

AND

Buys, sells, or shares personal information on 50k consumers/ households/ devices

OR

Gross revenue is greater than $25 million

OR

Derives 50% of annual revenue from the sale of Personal Information

What are the penalties for non-compliance?

Private Right of Action: The CCPA establishes a narrow private right of action for certain data breaches involving a sub-set of personal information. However, the CPPA grants companies a 30-day period to cure violations, if possible. Consumers may seek the greater of actual damages or statutory damages up to $750 per consumer per incident. Courts may also impose injunctive or declaratory relief.

Attorney General Enforcement: AG enforcement actions are subject to civil penalties of not more than $2,500 for each violation or $7,500 for each intentional violation.

How is “Personal Information” defined?

CCPA: “[I]nformation that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”

Proposed Amendment: “[I]nformation 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.”

What are some examples of “personal information”?

- Unique personal identifier, online identifier, IP address
- Browsing history, search history, information about a consumer’s interaction with a website
- Inferences used to build a profile or identify a consumer’s interests
- Bid request data, clickstream data, device graph data
- Real name, alias, postal address, email address, account name, social security number, driver’s license number, passport number, etc.

What consumer rights does CCPA grant?

- Right to know that personal information is collected, sold, or disclosed for business purposes
- Right to access personal information
- Right to delete personal information
- Right to opt-in to the sale of children's personal information
- Right to equal service and price (non-discrimination)
- Right to opt-out of the sale of personal information

What is the “right to opt-out of the sale of personal information”?

A business is required to create a separate “Do Not Sell My Personal Information” webpage with a clear and conspicuous link from their homepage that directs California consumers, or a person authorized by the consumer, to opt out of the sale of the consumer’s personal information.

Definition of Sale: “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 to another business or a third party for monetary or other valuable consideration.”

What is the “right to opt-out of the sale of personal information”?

- Gives consumers or their authorized agent the ability to direct businesses to stop selling their personal information to third parties.

- Unlike the access and deletion obligations, the do not sell obligation does not include a verification obligation, so a user sharing an identifier would seem to be enough to qualify

- Exceptions apply if the consumer subsequently provides express authorization for the sale of the consumer’s personal information, or if the personal information is solely used for complying with the opt-out request.

CCPA Scenario: Do Not Sell My Data

- A California consumer goes to their favorite publisher's home page. *Regardless of whether the consumer is a subscriber to that publisher or not*, CCPA requires a "Do Not Sell My Personal Information" link on the page that the consumer can click to stop a business from "selling" her "personal information"
- The definition of "sale" 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."
- The publisher's disclosure of data to almost all ad platforms and partners will likely be considered a "sale" subject to the "Do Not Sell My Personal Information" link. This means, if clicked, the publisher must halt almost all targeted advertising to that consumer.
- The publisher may also be prevented from pursuing such standard magazine industry practices as using subscriber lists to make advertiser-related offers to consumers, or to market other subscriptions.
- There are limited exceptions to the definition of a "sale," such as when a consumer consents to the business disclosing to a third party *provided that third party does not further "sell" that information*.

What are important considerations for publishers?

- How does a publisher authenticate an opt-out request? How does the publisher provide a pass-through request mechanism for others?

- If allowing third party IBA collection is a sale, how does the publisher stop that collection upon a do not sell request? Does it even have to under 1798.135(a)(4)?

- How does a publisher provide “explicit notice” of further sale and opt-out on behalf of a third party under 1798.115(d)?

What are important considerations for intermediaries?

Is an intermediary a "business?

- To be a "Business," a company needs to determine the "purpose and means" of processing of consumers' Personal Information. This is analogous to a data controller under the GDPR. But unlike the GDPR and the EU Directive, there is no supplementary CCPA guidance on what "purpose and means" is.

Is an intermediary a "Service Provider?"

- If the intermediary has deemed itself a processor under the GDPR, the closest related concept under the CCPA is a "Service Provider." However the definition is unclear. A Service Provider "processes personal information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract" provided that the contract prohibits the entity from using the data for anything other than performing specified services for the business.

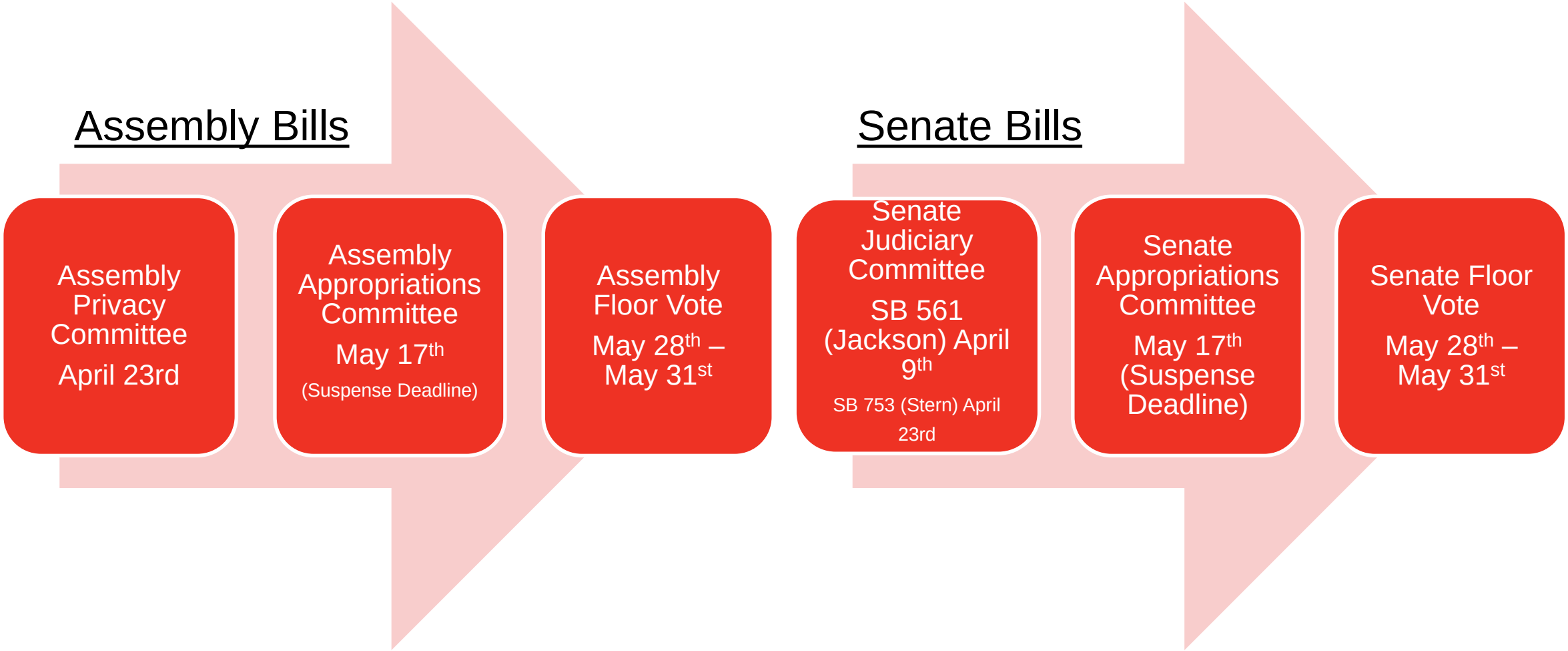
What are important considerations for intermediaries?

Is an intermediary a "Third Party?"

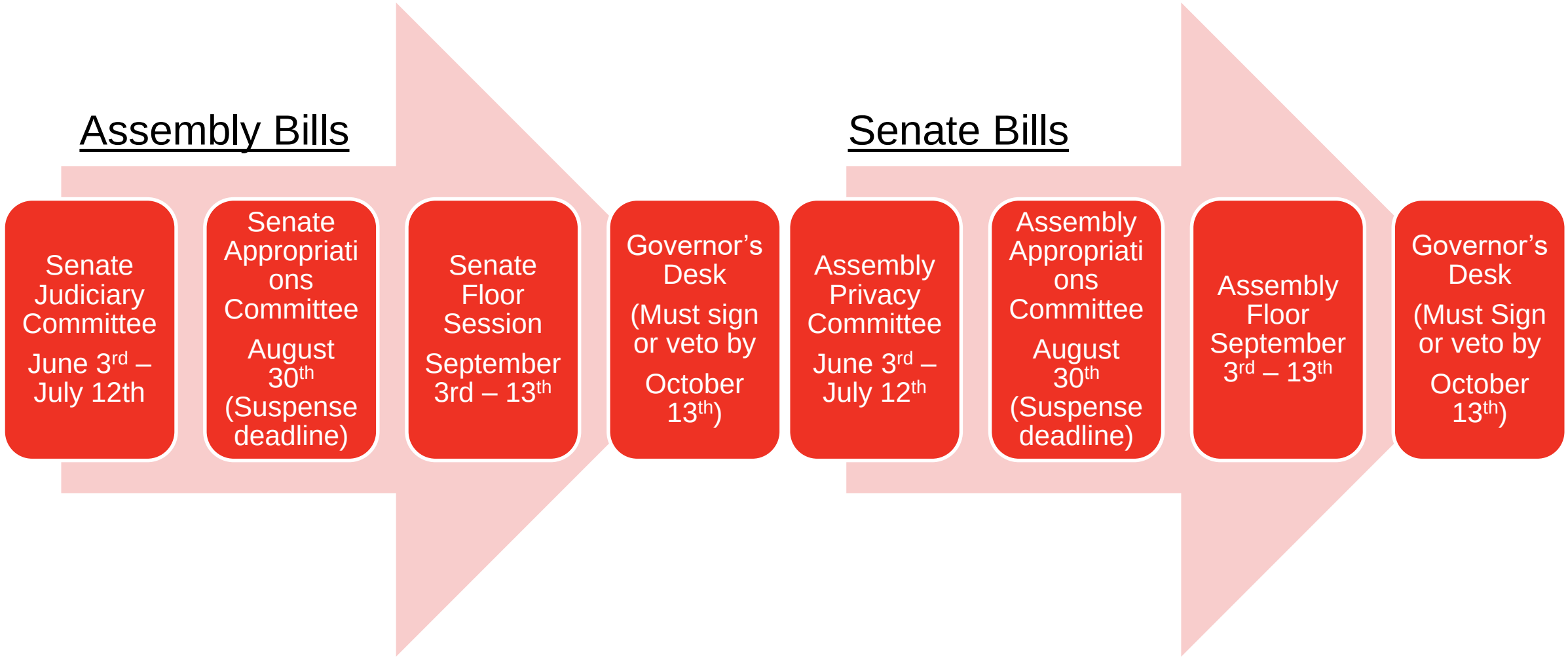
- If the intermediary is not a "Business" or a "Service Provider," then it is a Third Party. A third party cannot sell Personal Information it has been sold from a Business unless the Business has published an opt-out notice and the consumer has the opportunity to opt out (see 1798.115(d)). But what if the Third Party received the data from a Service Provider? There is no obligation for the Service Provider to enter into a contract with the Third Party to ensure the Third Party does not sell the data**.**

CCPA Legislative Amendment Update

Bill Process through May 31st



Bill Process June 1st – October 13th



IAB Policy Response to CCPA

IAB is advocating for changes that:

- Amend the definition of “Deidentified” in the CCPA to apply to information that “…does not reasonably identify, or link, directly or indirectly, to a particular consumer…” The bill also narrows the definition of “Personal Information” by striking “is capable of being associated with” and “household” from the definition. [Amendment AB 873 (Irwin)]
- Amend CCPA to allow businesses to make available to consumers a toll-free telephone number or an email address for submitting requests for information required to be disclosed, rather than both. [AB 1146 (Berman)]
- Ensure businesses need not reidentify or otherwise link information that is not maintained in a manner that would be considered personally identifiable

IAB is advocating against changes that:

- Remove the Attorney General’s obligation to provide compliance “opinions” to businesses and third parties
- Eliminate the 30-day window to “cure” any alleged malfeasance if plaintiffs are suing for monetary damages
- Expand the private right of action to any violation of a consumer’s CCPA rights. Currently limited to suits where consumers’ nonencrypted or nonredacted personal information has been subject to a data breach [SB 561 (Jackson)]
- Require companies to disclose the monetary value of users’ data

CCPA Frequently Asked Questions

What will the impact be for businesses outside of the U.S.?

CCPA does not require businesses to have a physical presence in California in order to be covered by the state's new privacy law, which goes into effect in 2020. It merely requires that they are doing business in the state and meet one of the three threshold requirements ($25 million in annual revenue; data collection on 50,000; or 50% of revenue from data sales).

Extraterritoriality is not a new concept in privacy. The European Union (EU) General Data Protection Regulation (GDPR) applies broadly beyond the territory of Europe pursuant to Article 3 of the GDPR. One of the first GDPR fines issued by the United Kingdom Information Commissioner's Office (ICO) was against a Canadian company. However, the extraterritorial breadth of the law may ultimately create enforcement challenges for regulators and the extent of enforcement beyond their borders is unclear. Perhaps recognizing this challenge, the European Data Protection Board signaled about a month ago that they would issue guidance on GDPR's extraterritorial application. Many are currently waiting for the final guidance to be posted online to determine whether they need to alter their approach.

What are the upcoming key milestones?

Summer/Fall 2019: The California State Legislature will consider amendments to the law, including amendments that would benefit the digital advertising industry in its compliance efforts.

Fall 2019: The California Attorney General has been given authority to issue regulations governing the new California privacy law following public consultation. These regulations will ultimately impact how the law is enforced, including how the law is enforced on businesses located outside of California and without a physical presence there. IAB has submitted detailed comments to the AG, asking for clarification on a number of aspects of the law.

What about the concept of business purpose?

Exception to sale: A business does not sell personal information if business uses or shares with a service provider personal information of a consumer that is necessary to perform a "business purpose"

"Business Purpose" means the use of personal information *for the business' or a service provider's operational purposes*, or other notified purposes, provided that the use of the personal information shall be reasonably necessary and proportionate to achieve the operational purpose *that is compatible with the context in which the personal information was collected*. Business purposes are:

- Auditing a current interaction and concurrent transactions, e.g., counting and verifying *ad impressions*;
- *Contextual customization of ads* shown as part of the same interaction *(if no profiles or reference to user outside of the current interaction)*;
- Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.
- Providing *advertising, marketing, analytics or similar services* on behalf of the business or service provider
- To improve, upgrade or enhance a business' device or service
- Fraud prevention, security, debugging, etc.

How can our company get involved?

IAB CCPA Tools Taskforce

- The IAB Legal Affairs Privacy Subcommittee is assessing what level of industry cooperation may be required to cause compliance with provisions of CCPA in programmatic transactions
- The industry needs to develop a technology tool (with the IAB Tech Lab) to send opt-out signals and pass notice signals to third parties.

IAB Public Policy Council

- Comprised of nearly 300 people from 150 leading publisher and ad technology companies, the Public Policy Council leads the advocacy efforts of IAB members as they engage all levels of government on key policy issues in order to ensure continued growth of the industry.

IAB Tech Lab

- Similar to the *IAB Tech Lab GDPR Technical Working Group*, IAB Tech Lab is assisting IAB in engaging technical leaders in contributing to CCPA technical solutions.

Where can I find additional resources and information?

- IAB CCPA Portal: https://www.iab.com/ccpa/
- IAB Comments to California Attorney General: https://www.iab.com/news/ccpa-comments-ca-ag/
- IAB CCPA Roadmap: https://www.iab.com/insights/ccpa-roadmap/

Federal Privacy Legislation

5 things to know about privacy discussions in Congress

1. The “creepiness” factor has grabbed the attention of House and Senate members, but issue conflation and demagoguery are rampant. In response, members have introduced a variety of legislation, but none are expected to gain traction
2. All eyes are on four specific Senate offices, that are working together to circulate a “discussion draft” this spring. That bill will be seen as the main congressional product on privacy, and will provoke sustained industry advocacy through 2020
3. A Federal bill is likely to include enhanced rulemaking authority for the FTC and required rights and mechanisms that companies must implement. Duties of “care” and “loyalty” with respect to the handling of consumer data are expected to be included
4. The “New Paradigm,” which IAB has helped draft with a cross-industry coalition, will be a main driver for congressional consideration
5. Republican Members of Congress have stated that Federal preemption must be included for any bill to pass the House and Senate, while Democrats insist that CCPA-like language must be the “floor” for any piece of draft legislation

Privacy for America

Mission

Privacy for America will work with Congress to support enactment of comprehensive federal consumer data privacy and security legislation. We have outlined a bold new paradigm for a national law that would make personal data less vulnerable to breach or misuse and set forth clear, enforceable and nationwide consumer privacy protections for the first time.

Steering Committee Members

- American Association of Advertising Agencies (4A's)
- Association of National Advertisers (ANA)
- Digital Advertising Alliance
- Interactive Advertising Bureau (IAB)
- Network Advertising Initiative (NAI)

Privacy for America

1. Protect Consumers Nationwide. The new law will provide, for the very first time, broad-based privacy rules for the entire U.S. marketplace. To date, privacy in the U.S. has been addressed through a patchwork of state and federal laws and industry self-regulation that leave gaps in consumer protection.

2. Establish New Prohibitions on Certain Data Practices. Rather than asking consumers to read the "fine print" in order to protect themselves, the new law would ban outright a wide range of harmful and unexpected data practices, including:

- ✓ ***Eligibility*** – Using a person's data to turn them down or set unfavorable terms for a job, credit, insurance, healthcare, education, or housing, unless specifically permitted under existing federal and state laws governing such benefits.
- ✓ ***Discrimination*** – Using personal characteristics such as race, color, or religion to discriminate against a consumer in setting prices or determining eligibility for products and services.
- ✓ ***Assisting and facilitating fraud*** – Sharing consumer data with another company with reason to know that it will be used to defraud a consumer.
- ✓ ***Sensitive data*** – Collecting or using sensitive data – including medical, financial, biometric, and precise geolocation data, as well as email communications and private recordings – without the permission of the consumer to whom the data relates, with limited exceptions.
- ✓ ***Vendor and third party oversight*** – Sharing consumer data with vendors or third parties without entering into enforceable contracts ensuring their lawful use of the data.

3. Create a New Data Protection Bureau to Strengthen Privacy Oversight and Enforcement. The new law would significantly strengthen privacy oversight and enforcement by creating a new Data Protection Bureau at the Federal Trade Commission (FTC), in order to enhance the FTC's longstanding expertise in overseeing privacy issues. In addition, the FTC will be provided with additional privacy staff and resources and privacy jurisdiction over common carriers and nonprofits.

Privacy for America

4. Grant Enhanced Rulemaking Authority to the FTC. Recognizing that new data practices will arise over time, the new law would set forth specific criteria for the FTC to identify and prohibit additional data practices through rulemaking.

5. Ensure Responsible Advertising Practices. Many consumers welcome information about products and services they enjoy, but some are concerned about the scope of data collected and the risk that such data could be misused. The new law would impose significant restrictions on data use for advertising – including banning certain types of data from being collected and used for advertising, limiting the purposes for which advertising data may be used, and allowing consumers to identify their preferences regarding what advertising they do or do not wish to receive.

6. Require Strong Data Security Protections. Currently, despite the massive data breaches that have occurred over the last decade, data security laws in this country still apply to only a few sectors of the economy. The new law would impose, for the very first time, robust security requirements, including the adoption of required security mechanisms, on virtually every company in this nation. Our goal is to make universal the adoption of automatic mechanisms that will have the impact that seat belts and air bags had on auto safety.

7. Authorize Strict Penalties for Violations. Currently, the FTC's authority to obtain penalties for privacy and data security violations is too limited. The new law would authorize both the FTC and State Attorneys General to seek in some cases new penalties against companies that violate it.

Alex Propes
Sr. Director, Public Policy & International
alex@iab.com