Beyond CCPA

The Need for Federal Data Privacy Regulation

LiveRamp

June 6, 2019

The ethical use of data can unlock infinite value and power tremendous benefits for people. Fundamental to this is demonstrating accountability for how data is used, its impact, and its consequences. A critical utility function of the ad-driven ecosystem is connecting data. An ad-driven ecosystem enables access to free content and services, fuels an open, competitive and vibrant internet, and encourages innovation and economic growth. It is said that advertising is the greatest cross-subsidization ever of free speech – which is precious and foundational to a free society.

Often, however, data-driven advertising is conflated with harm. Instances of data misuse, negligent acts, and intentional bad acts and bad actors contribute to a trust deficit in the digital ecosystem. Importantly, the California Consumer Privacy Act (CCPA) is aimed at this target and reflects very real and valid concerns about the responsible use and protection of personal data. As an industry, we need to pay attention – and the new CCPA law will force this attention.

While there are still many unknowns with this new act, there are two certainties. First, data collectors and data users must take responsibility for protecting data and should have accountability for its use and impact. Second, while there is much to like about CCPA, there is also substantial room for improvement as the legislation is fine-tuned.

CCPA's Very Real Challenges

Although CCPA aims to address valid concerns and some obvious misconduct by a few bad actors, questions remain. Will it solve for these concerns and eliminate misconduct? Or will it offer the appearance of protection, but instead result in a series of unintended consequences? Left unimproved, there are real concerns that CCPA could hamper innovation and tilt the playing field in favor of large digital platforms at the expense of entrepreneurs and small- and medium-sized businesses.

There are a variety of emerging issues and pending amendments to CCPA, many of which were sent to the California Senate by the May 31 "crossover" date. These include:

1. Compliance Window

Companies lack the clarity and runway needed to be prepared for the CCPA effective date of January 1, 2020. Business should be granted a fair opportunity to comply. With the legislative refinement discussion still underway, and the Attorney General (AG) implementing regulations slated for release sometime this fall, **affected companies will have roughly two-and-a-half months (75 days or less) to get system changes in place to comply.** This is a vexing problem, even for ethical companies with plenty of resources that intend to operate best-in-practice data governance programs.

Industry Perspective: The business community should **suggest** a 24-month implementation period in order to ensure orderly and cost-effective compliance and **avoid** unnecessary and exorbitant disruption of the data and marketing industry.

2. Private Right of Action Threat

The business community remains concerned about the "private right of action" (PRA) course that some legislators are advocating. The threat of potentially frivolous lawsuits may not spur faster compliance so much as it may simply create greater operating and legal risk while good faith compliance efforts are underway.

Industry Perspective: Industry should be committed to compliance with key CCPA provisions and encourage legislators to avoid layering in additional legal uncertainty and complexity at this time.

3. AB 873 (Irwin)

(Amended 5.2.19) The CCPA defines "personal information" (PI) and "deidentified" (deID) information in an unworkable manner. As written, PI includes everything, even bitstream data. And, as written, the deID exclusion doesn't actually exclude. We need AB 873 (Irwin) to progress through the Senate chamber, go to the Governor's desk, and be signed into law. If any further amendments are made, they should be to strengthen the practicality of PI and brighten the exclusion for deID data.

Industry Perspective: Businesses should consider advocating for this effort, because it clarifies what might otherwise be ambiguous language in the legislation.

4. AB 25 (Chau)

(Amended 4.12.19) This bill would amend the definition of "consumer" to exclude a person's information in the role of employee, job applicant, business contact, agent of the business, and contractor information.

Industry Perspective: Businesses should support this clarification, as it ensures that small businesses and virtually every employer doesn't incur significant and unintended compliance costs. The exclusion of business contact and agent data is also important.

5. AB 1416 (Cooley)

(Amended 5.6.19) This bill addresses the "collection" and "disclosure" of consumer personal information by creating an exception to the CCPA (1) for a business that provides a consumer's personal information to a government agency solely for the purposes of carrying out a government program, and (2) for a business that sells the personal information of a consumer who has opted out of the sale of their personal information to another person for the sole purpose of detecting security incidents and protecting against malicious, deceptive, fraudulent, or illegal activity.

Industry Perspective: Businesses should consider supporting this effort, for the greater good of society and the prevention of fraud and other malfeasance.

6. AB 874 (Irwin)

(Amended 3.25.19) This bill fixes the definition of "personal information" to exclude public record data, which is already robustly regulated by state law.

Industry Perspective: This should be supported, since it is already regulated under existing state law.

7. AB 846 (Burke)

(Amended 5.20.19) As written, the CCPA precludes loyalty card and rewards programs. This bill fixes the CCPA nondiscrimination section to clearly allow loyalty and rewards programs.

Industry Perspective: This should be supported to protect consumer choice and their ability to collect loyalty rewards.

There are additional CCPA-related bills to keep an eye on, as they will likely gather more universal support:

1. AB 1564 (Berman)

(Amended 4.30.19) This bill would require the business to make available to consumers a toll-free telephone number or an email address for submitting requests for information required to be disclosed. This bill is one of the smaller items on our wish list.

Industry Perspective: This should be supported, as it provides clarity and standardization while also allowing businesses to provision information disclosure in whatever method is consistent with their business practices.

2. AB 1146 (Berman)

(Amended 4.30.19) This bill would exempt from the CCPA vehicle information shared between a new motor vehicle dealer and specified parties. This includes the vehicle's manufacturer or if the information is shared pursuant to, or in anticipation of, a vehicle repair relating to warranty work or a recall, as specified.

Industry Perspective: This should be supported in the interest of societal good and consumer protection.

3. AB 981 (Daly)

(Amended 4.30.19) Insurance Information and Privacy Protection Act. This bill has been significantly amended. Now, it would eliminate a consumer's right to request that a business delete or not sell the consumer's personal information under the CCPA if it is necessary to retain or share the consumer's personal information to complete an insurance transaction requested by the consumer.

Industry Perspective: This should be supported in the interest of societal good.

There are other data-related bills in play that we should pay attention to:

1. AB 1395 (Cunningham)

(Amended 5.22.19) This bill would prohibit a smart speaker device, as defined, or a specified manufacturer of the device, from saving or storing recordings of verbal commands or requests given to the devices, or verbal conversations heard by the device, regardless of whether the device was triggered using a key term or phrase. Working on language with author.

Industry Perspective: This bill is troublesome. It appears to prescribe how innovation should work, and is counter to consumer choice.

2. AB 1130 (Levine)

(Amended 5.16.19) Data Breach. This bill would require businesses to notify consumers of compromised government-issued IDs and biometric information as broadly defined under CCPA and subject breach of that data to the private right of action contained in CCPA. AG's office has agreed to narrow the definition of biometric data, but does not agree to removing CCPA liability for biometric data (based on feedback from the AG).

Industry Perspective: We oppose this bill, unless amended to keep liability under CCPA.

3. AB 1202 (Chau)

(Amended 5.16.19) Privacy: data brokers. This bill would require "data brokers" – very broadly defined using the CCPA definitions of "personal information" and "sell" – to register with the Attorney General. The bill would require the Attorney General to

put the information online. Working on language with author.

Industry Perspective: We oppose unless amended (ANA and other advertising groups also oppose).

4. AB 1316 (Gallagher)

(Amended 4.29.19) Internet: social media or search engine service: censorship. This bill would prohibit a person who operates a social media internet website located in California, as defined, from removing or manipulating content from that site on the basis of the political affiliation or political viewpoint of that content.

Industry Perspective: Watch: potential First Amendment concerns.

5. AB 1138 (Gallagher)

(Amended 5.13.19) Social media: The Parent's Accountability and Child Protection Act. This bill prohibits a social media website or application from allowing a person under 16 years of age to create an account with the website or application unless the website or application obtains the consent of the person's parent or guardian prior to creation of the account, and would require the Department of Justice to establish guidelines relating to the specific means by which a social media website or application shall obtain that consent. Child advocacy groups like Trevor Project and NYCL are leading with opposition of limits on what teens can do online.

Industry Perspective: We oppose this bill because it creates a different standard than the Federal COPPA law and may eliminate common communication methods.

6. AB 1665 (Chau)

(Amended 5.8.19) The Parent's Accountability and Child Protection Act. This bill would prohibit a person or business that conducts business in California that also operates an internet website or application that seeks to use a minor's name, picture, or any information about the minor on a social media, internet website, or application, as specified, from doing so without obtaining prior parental consent.

Industry Perspective: Watch. The practical effect of this bill is uncertain.

7. AB 161 (Ting)

(Amended 5.17.19) Solid waste: paper waste: electronic proofs of purchase. This bill would require, on and after January 1, 2022, a proof of purchase for the retail

sale of food, alcohol, or other tangible personal property, or for the provision of services provided to a consumer by a business to be provided only in electronic form, unless the consumer requests that the proof of purchase be provided in paper form.

Industry Perspective: We oppose this bill because it introduces unnecessary processes and complexity on affected businesses.

8. AB 1281 (Chau)

(Amended 4.12.19) Privacy: facial recognition technology: disclosure. This bill would require a business in California that uses facial recognition technology to disclose that usage in a physical sign that is clear and conspicuous at the entrance of every location that uses facial recognition technology, as defined. The bill would consider a violation of these provisions to be unfair competition within the meaning of the Unfair Competition Law, and would authorize these provisions to be enforced consistent with that law. Language in negotiation with Chau's office.

Industry Perspective: Currently neutral position based on recent amends.

Two-Year Bills of Note

1. SB 753 (Stern)

(Amended 4.4.19) California Consumer Privacy Act definition of sale: advertisement service exception. This bill would provide that a business does not sell personal information if the business, pursuant to a written contract, shares, discloses, or otherwise communicates to another business or third party a unique identifier only to the extent necessary to serve or audit a specific advertisement to the consumer. The bill would require the contract to prohibit the other business or third party from sharing, selling, or otherwise communicating the information except as necessary to serve or audit advertisement from the business. Failed in Senate Judiciary and is now a two-year bill.

Industry Perspective: We support this bill, as it would exclude from the definition of "sale" the use of unique identifiers essential to functionally serving ads.

2. AB 288 (Cunningham)

(Amended 3.19.19) Consumer privacy: social media companies. This bill creates an onerous private right of action with a right to excessive punitive damages

for purely economic losses at a low evidentiary standard, along with attorney's fees, for a new consumer right to delete data that conflicts with the consumer right to delete recently provided by the CCPA.

Industry Perspective: We oppose this bill because it conflicts with obligations under CCPA, creating an impossible compliance situation for businesses.

3. AB 904 (Chau)

(Amended 3.28.19) Search warrants: tracking devices. This bill would specify that a tracking device includes any software that permits the tracking of the movement of a person or object.

Industry Perspective: Watch. The definitions contained in the current version of the bill have potential implications to commercial software and intersection with other California law and related definitions.

4. AB 950 (Levine)

(Introduced 2.20.19) Consumer privacy protection. This bill would require a business that conducts business in California, and that collects a California resident's consumer data, to disclose to the consumer the monetary value to the business of their consumer data by posting the average monetary value to the business of a consumer's data, including in its privacy policy posted on its internet website, and including in its privacy policy disclosure of any use of a consumer's data that is not directly or exclusively related to the service that the consumer has contracted the business to provide, as specified. Also requires disclosure to the consumer the average price it paid for a consumer's data and actual price it was paid for a consumer's data upon receipt of a verifiable request for that information from the consumer. Would also establish the Consumer Data Privacy Commission comprised of members of academia, civil society, and industry to provide guidance to the legislature regarding appropriate metrics and methodology for determining the value of consumer data. The bill would require the commission to report its findings to the legislature on or before January 1, 2021. Levine's office confirmed in writing their intention for this to be a two-year bill.

Industry Perspective: We oppose this bill, as it introduces unworkable obligations in a data-driven digital ecosystem.

5. AB 1760 (Wicks)

(Amended 4.12.19) California Consumer Privacy Act of 2018. A substantial bill that redefines many elements of CCPA, including the name. Includes a PRA as well as city attorney enforcement, requires naming third parties with whom a company shares or sells data, defines "sharing of data" and replaces "sell" in the CCPA with "share," and much more. **Need all hands on deck to ensure this bill does not progress.**

Industry Perspective: We oppose this bill because it rewrites much of the CCPA in a troublesome manner and incentivises frivolous lawsuits.

CCPA has the potential to create unintended consequences and real challenges for competition and innovation. Large techopolies have near-unlimited resources to comply with the law and weather the storm of typical class-action attacks. Smaller companies and market entrants, who are also innovating for the future, do not. The result is a CCPA barrier-to-entry moat for the outsized tech giants. The unprecedented definitions of "personal information" and "sell" might just enable terrorists to opt out of the very data systems designed to identify them. And this is just one of the many, and still developing, lists of surprising and unfortunate effects of the law.

What About a National Standard?

Some of our laws have been made at the state level, with each state's own notion of what is good or not for that state. When issues are deemed too impactful for disparate state-by-state-by-state standards, laws are made at the federal level. Data regulation is one of those.

Federal laws underpin our "fairness and justice for all," and national standards support our united future, economy, and competitive position in the world. We must strive for a workable, meaningful, future-prepared law of the land that protects fairness, fuels our renowned American innovation, and ensures the United States remains competitive into the data-driven, digital future of the world.

However, the CCPA is coming. We may not get the practical, workability fixes so that the law is clear enough for companies to actually comply or remove "unintended consequences." We may have to guess our way towards compliance. For those of us who operate across the United States or hope to, we will be navigating the complexities and differences of other states' emerging "CCPA look-similars." As a result, data-processing systems will need to be rebuilt to process differently on a state-by-state basis.

The promise of this fourth Industrial Revolution—what's also been called the Machine Age and the Digital Era—is that data and computing can solve many of our most pressing human challenges. From health and well-being revolutions to equal opportunity, the thoughtful, effective, and ethical use of data will fuel an amazing future.

For now, CCPA fixes are needed in the near term. Ultimately, we need one standard for all—one that is balanced, practical, and addresses the realities of our digital future. We need to protect competition and innovation and preserve trust in our ecosystem through transparent, accountable, and demonstrable data practices.

LiveRamp believes proper use of data benefits both businesses and individuals and provides the much-needed context for delivering better, more relevant customer experiences. **Read more** about LiveRamp's Data for Good.