Privacy Policy: What Happened in California and What is Happening in Congress

Presenters:

Alan Thiemann, Conexxus General Counsel

Paige Anderson, NACS Government Affairs Director

CONEXXUS
solve forward

Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q & A

Housekeeping

This webinar is being recorded and will be made available in approximately 15 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck

- Survey Link – Presentation provided at end

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions
- Our webinars may be used toward PCI continuing education credits. Please contact arussell@conexxus.org for questions regarding a certificate of webinar attendance.

Email: **info@conexxus.org**

CONEXXUS
solve forward

Presenters

Conexxus Host

Allie Russell
Conexxus
arussell@conexxus.org

Speakers

Alan Thiemann, General Counsel, Conexxus

Paige Anderson, Director, Government Relations, NACS

CONEXXUS
solve forward

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards…
  - Data exchange
  - Security
  - Mobile commerce
- We provide vision
  - Identify emerging tech/trends
- We advocate for our industry
  - Technology is policy

CONEXXUS
solve forward

2019 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
January 24, 2019	Who's Watching Your Network? What you should know about Managed Detection & Response (MDR)	Mark Carl Tom Callahan	ControlScan
February 28, 2019	Protect Your Business: PCI Resources for Securing Payment Data	Elizabeth Terry	PCI Security Standards Council
March 21, 2019	Proactive Defense in Depth	Brett Stewart DeWayne Mangan Mark Palmer	Acumera
May 30, 2019	Firewalls, LANS & WANS The Basics, The Benefits and The Security!	Simon Gamble	Mako Networks
June 27, 2019	Web Payment Asipirations	Ian Jacobs	W3C
July 25, 2019	Skimming	Linda Toth Paige Anderson Caleb Burke	Conexxus NACS CITGO
August 8, 2019	Application Security 101	Denis Sheridan	Synopsys

CONEXXUS
solve forward

2019-2020 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
August 29, 2019	Don't Get Phished!! Train Your Employees To Avoid Ransomware	Geoffrey Vaughan Ed Adams	Security Innovation
September 26, 2019	Using Data Science to Proactively Manage the Connected C-Store	Ashwin Swamy Thomas Duncan	Omega ATC Omega ATC
October 24, 2019	Easy PCI—How to Make PCI & Attestation Easier	Ajith Edakandi	Hughes
November 21, 2019	Applicability of PCI DSS requirements for Merchants and MNSP's	Sam Pfanstiel	ControlScan
December 5 and 12, 2019	EMV	TBD	TBD
January, 2020	TBD	TBD	Cybera

CONEXXUS
solve forward

2020 Conexxus Annual Conference
April 26-30, 2020
Loews Ventana Canyon Resort
Tucson, AZ

Conexxus thanks our 2019 Annual Diamond Sponsors!

CONEXXUS
solve forward

CCPA -- General

- Modeled after the EU's General Data Protection Regulation (which became effective on May 28, 2018).
- In reality, there are more differences than similarities, but both require an entity that collects personal information to give individuals the right to protect their own information. GDPR is focused on obtaining "informed consent" for future data collection and use while CCPA is focused on giving notice of rights concerning what personal information has been collected and used during the past 12 months.
- CCPA is principally an "opt-out" law while the GDPR is an "opt-in" law.

CCPA Landscape

CCPA imposes obligations on a covered entity to:

- secure a consumer's personal information;
- provide notification in the event of a breach; and
- develop compliance programs to manage a sweeping package of consumer rights.

CCPA – Effective on Jan. 1, 2020

- CCPA provides broader rights to consumers and stricter compliance requirements for businesses than any other existing state or federal privacy law.
- Businesses that are subject to complying with the EU's GDPR may find complying with CCPA less of an adjustment in their data practices.
- Proactive businesses are already considering CCPA a de-facto U.S. privacy law and preparing privacy operations to address all consumer data they touch.
- CCPA requires expert judgment and team effort among data privacy officers, IT staff, and business leaders to prepare.

Consumers' Rights

A Consumer has the right to request that a business:

- Disclose the categories and specific pieces of personal information it has collected;
- Disclose the categories of sources from which the personal information is collected;
- Disclose the business or commercial purpose for collecting or selling the personal information;
- Disclose the categories of third parties with whom the business shares the personal information;
- Delete any personal information about the consumer that the business has collected from a consumer, unless it meets certain exceptions; and
- Not "sell" (broadly defined) the consumer's personal information (the "Do Not Sell" opt-out).

NOTE: Businesses typically must respond to any of these requests within 45 days of receipt, and must provide certain easily accessible, cost-free methods for exercising these rights.

Right to Request Access

A consumer has the right to request information regarding:

- the categories of personal information a business collects about him/her:
  - identifiers – e.g. real name, address, social security number
  - characteristics of protected classification under California or Federal law;
  - Commercial information – e.g. products purchased, records of personal property
  - Biometric information
  - Internet or other electronic network activity – e.g. browsing history, search history
  - Geolocation data
  - Audio, visual, and similar information
  - Profession or employment related information;
- the sources from which that personal information was collected (e.g., online order histories, online surveys, tracking pixels, cookies, web beacons);
- the categories of personal information sold to third parties;
- the categories of personal information disclosed for business purposes;
- the categories of third parties to whom personal information was sold or disclosed (e.g., tailored advertising partners, affiliates, social media websites, service providers);
- the business or commercial purposes for which personal information was collected or sold (e.g., fraud prevention, marketing, improving customer experience); and
- the “specific pieces” of personal information collected.

Who is Covered?

The CCPA applies to a for-profit business regardless of where located, which:

- Does business in California;
- Collects consumers' personal information of California consumers;
- Determines the purposes and means of the processing of consumers' personal information; and
- Meets any ONE of the following tests:
  - Has annual gross revenues in excess of $25 million;
  - Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or
  - Derives more of its annual revenues from selling consumers' personal information (more than 50 percent).

NOTE: Parent companies and subsidiaries using the same branding are covered in the definition of "business," even if they themselves do not exceed the applicable thresholds.

Exemptions

- Exceptions if you are required by law to keep personal information (e.g., I-9 employee information, EEOC demographics).
- Deidentified or aggregate consumer information (anonymization, psuedonomization).
- Conduct occurring “wholly outside of California”
- Exceptions applicable to certain personal information already subject to state or federal regulation (applying to types of information, not types of businesses):
  - 1) medical information or Protected Health Information governed by California law, HIPAA or the FDA’s “Common Rule” applicable to clinical trials;
  - (2) personal information subject to the California Financial Information Privacy Act or the federal Gramm-Leach-Bliley Act (applicable to financial institutions);
  - (3) personal information sold to or from consumer reporting agencies as covered by the Fair Credit Reporting Act; and
  - (4) personal information subject to protection under the Driver’s Privacy Protection Act.

Exemptions

- CCPA includes exceptions where application of the statutory obligations would conflict with controlling state or federal law (e.g., free speech protections of the First Amendment).
- Thus, the CCPA right to deletion will not have the same reach as the GDPR's "right to be forgotten," at least with respect to social media.
- A business also may be able to cite federal pre-emption in some instances (e.g., CCPA's prohibition on contract arbitration clauses and class action waivers) that would limit consumers' CCPA rights may be pre-empted by the Federal Arbitration Act.

Penalties

- For violations of breach notification provisions: private right of action.
- For all other violations, the AG will enforce.

Note: The AG has been trying to get the Legislature to allow private actions for all violations, claiming it doesn't have the resources to enforce the law.

Fines

- Violations of the CCPA are subject to civil penalties of $2,500 for each violation or $7,500 for each *intentional* violation after notice and a 30-day opportunity to cure have been provided.
- Enforcement will be delayed until six months after publication of the Attorney General's implementation guidelines, or July 1, 2020, whichever is sooner (using a one-year "look-back" period).

Amendments (Oct. 12)

- One-year delays for employee data (AB-25) and business-to-business customer representative personnel data (AB-1355) from much of the law's application.

- Clarification that a business does not need to retain or collect additional information than it would otherwise do in the ordinary course of business (AB-1355).

- Clarification that a business operating only online only needs to provide an email address as a designated consumer request method (AB-1564).

Amendments (Oct. 12)

- Changes to the definitions of “personal information” (AB-874 and AB-1355) to eliminate “publicly available” information (AB-874) and to define the term “verifiable consumer request” (AB-1355).

- Modified the definition of “personal information” as information that is “reasonably capable of being associated with” a particular consumer or household, instead of simply “capable of being [so] associated”.

Amendments (Oct. 12)

- Clarification that CCPA class-action lawsuits may not be brought for data breaches when “data breach personal information” is either encrypted or redacted (not both).

- Clarification that deidentified and aggregated information are exempt from the statute.

- Clarification that the reasonableness of charging a different price or rate or providing a different level or quality of goods or services is measured in relation to the value of the personal information to the collecting business -- not to the consumer.

Note: AB 846, which would have exempted loyalty programs from CCPA, was withdrawn. The sponsor indicates she will reintroduce the bill again in 2020.

Amendments (Oct. 12)

- CCPA now requires the registration of “data brokers” on a public website maintained by the AG. Essentially, the definition of “data broker” is one who “knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.”

NOTE: CCPA’s definition of “sells” includes a business that shares personal information as part of its business without a relationship with the person in question a “data broker.”

- Clarification that a consumer has a “direct relationship with traditional and e-commerce businesses, which could have formed in a variety of ways such as by visiting a business’ premises or internet website, or by affirmatively and intentionally interacting with a business’ online advertisements, may have some level of knowledge about and control over the collection of data by those businesses, including: the choice to use the business’s products or services, the ability to review and consider data collection policies, the ability to opt out of certain data collection practices, the ability to identify and contact customer representatives, and the knowledge necessary to complain to law enforcement.”

NOTE: A business has a direct relationship with a consumer who browse its website or has clearly disclosed all of the third-party tracking on its website and offered an opt-out, then it looks like even that third-party tracking is not a “data broker.”

First One-year Moratorium

- Employee data is largely excluded from the CCPA's scope until January 1, 2021. However, employee data remains subject to two CCPA provisions:
- (1)employers must provide employees with a list of the categories of personal information that they will collect and must note how it will use such data.
- (2) employee data remains subject to the private right of action related to security breaches.

NOTE: the moratorium helpfully also covers emergency contact and beneficiary data, not strictly the employee's personal information. However, the bill does not clarify whether third party HR vendors' use of such information is also excluded when the vendor receives and uses consumers' personal information solely related to their role as employees.

Second One-year Moratorium

- **Limited exception for personal information reflected in a business transaction until Jan. 1, 2021.** Although this language has been referred to as the “B2B” exemption, the scope is actually much narrower. The exemption does not cover the personal information exchanged pursuant to a transaction, but rather the personal information of the consumer(s) effectuating or otherwise involved in the transaction. There are also significant limitations to the exemption (e.g., a consumer still has the right to opt-out of sales).

CCPA Draft Regulations (Oct. 12)

- California AG releases draft of implementation regulations.
- Comments due by Dec. 6.
- Final Regulations by July 1, 2020.
- Several critical regulations for merchants (see next slide)

CCPA Draft Regulations

- What constitutes a “verifiable consumer request”
- Who qualifies as a “California resident”?
  - Option: business could elect to give CCPA rights to non-residents, which could facilitate compliance by eliminating the need to verify California residency.
- What a business must do, if anything, to tie pseudonymous data (e.g., online identifiers and browsing data) to a particular consumer seeking to exercise his/her rights.

CCPA Draft Regulations

- Loyalty program incentives should be “reasonably related” to the value of a consumer’s data to the business, calculated using one of eight methods outlined in the regulations, or risk falling foul of non-discrimination provisions.
- Companies that handle the personal information of more than 4 million consumers will be subject to additional requirements.

CCPA Draft Regulations

The law allows consumers to request that their data be deleted and to opt out of having data sold to third parties. Draft regulations propose specific requirements for compliance with the law, such as the “Do Not Sell” link.

Notice of how to Request

A business shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number, and if the business operates a website, an interactive webform accessible through the business's website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.

CCPA Draft Regulations

- Compliance with the regulations will cost businesses between $467 million and $16.5 billion between 2020 and 2030.
- Tech industry groups have noted that the same study estimated the total cost of initial compliance with the law at around $55 billion.

Steps for a Merchant

You must comply with a host of new requirements governing the collection, use, and sharing of your customers' personal information. You will need to:

1) conduct a data flow analysis to identify where all personal information resides:
2) update the disclosures in your privacy notices/policies;
3) establish processes for receiving and responding to consumer rights requests and train your personnel who will be involved in handling requests from consumers;
4) observe restrictions on data monetization practices; and
5) review and revise contracts with vendors that handle customers' personal information on their behalf.

Until Jan. 1, 2021

- **For Employee Data:** Draft a simple employee privacy notice if you have not done so already.
- **For Business Contacts:** Make sure that you do not sell personal information collected while conducting a business-to-business transaction to eliminate such information completely from the scope of CCPA rights.

Data Flow Analysis

In order to comply with the CCPA and respond to consumers' requests, you will need to:

1) conduct a thorough analysis of all of your business systems to identify where consumers' personal information exists and how it is being used;
2) make any changes to your systems functioning to reduce the collection, processing, or use of unnecessary personal information;
3) be able to establish a procedure for responding to consumer requests.

Data Inventory

- You should create a data inventory or data flow map to understand all the ways in which you may obtain personal information, the types of personal information you collect and share, the purposes for which you use it, the parties with whom you share it and why/how it is retained and secured, and your current data disposal practices.

Privacy Policy

In order to comply with the CCPA you Privacy Policy must provide:

- A description of consumers' rights under the CCPA;
- A description of the categories of personal information collected by the business in the preceding 12 months;
- The commercial and business purposes for which the personal information is collected;
- The categories of personal information sold or disclosed for a business purpose in the preceding 12 months;
- The categories of third parties with whom personal information is shared;
- A link to a "Do Not Sell My Personal Information" web-based opt-out tool;
- A description of any financial incentives for providing data or not exercising rights (e.g., if the company offers a 15% discount to individuals who provide their email address for marketing purposes, this incentive must be disclosed in the privacy policy); and
- Two or more designated methods for submitting information requests, including a toll-free number and a website address (if applicable).

Privacy Policy

Proposed regulations require (§999.308):

1) A privacy policy shall be designed and presented in a way that is easy to read and understandable to an average consumer.

2) The notice shall:

a. Use plain, straightforward language and avoid technical or legal jargon.

b. Use a format that makes the policy readable, including on smaller screens, if applicable.

c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.

d. Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the policy in an alternative format.

e. Be available in an additional format that allows a consumer to print it out as a separate document.

“Data brokers”

- You need to look carefully to find or establish that your consumers have “knowledge about and control over” sufficient to establish a “direct relationship” with you, so you are not covered by the “data broker” requirements.

Financial Incentives

If you have a loyalty program, the AG's Draft Regulations (§999.307) would require:

A business shall include the following in its notice of financial incentives:

- (1) A succinct summary of each financial incentive or price or service difference offered;
- (2) A description of the material terms of each financial incentive or price of service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference;
- (3) How the consumer can opt-in to each financial incentive or price or service difference;
- (4) Notification of the consumer's right to withdraw from each financial incentive at any time and how the consumer may exercise that right; and
- (5) An explanation of why each financial incentive or price or service difference is permitted under the CCPA, including:

  a. A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and

  b. A description of the method the business used to calculate the value of the consumer's data.

“DO NOT SELL”

- You need to work with your web-developer/app developer/software/IT team to ensure that you have a functioning button on your website or app.
- You need to work with your sales/marketing team to ensure that when a person clicks on this button that the information results in the proper outcomes.
- You need to include this information in your Privacy Policy.

State Laws

2018-19 key updates and trends

Key trends in how privacy law is shaping up around the nation:

- Every state now has a law requiring companies to publicly disclose when a data breach occurs, but there are significant differences among them.
- Many states have expanded the definition of “personally identifiable information” to include more types of data and combinations of data.
- California passed the toughest privacy and data protection law in the nation, pushing it to the top of the rankings.
- Maine is the only state to pass a law prohibiting law enforcement from tracking a person’s location using GPS or other geo-location info built into smartphones and computers. Illinois and California have both put forth such bills in the past, but they were vetoed.
- Illinois is the only state to specifically protect biometric data, but that law (BIPA) but amendments are being considered that would reduce some impacts.
- Maine introduced a new data protection act in 2019 that stipulates internet service providers cannot “use, disclose, sell, or permit access to customer personal information” without customer consent, save for certain exemptions such as complying with a court order
- Nevada passed an act on October 1, 2019 that allows customers to opt out of online data sharing

2020 State Laws

New amendments to CCPA regarding expanded enforcement are expected to be introduced by privacy advocates (and November 2020 ballot initiative).

Amendments to resolve the one-year moratoria on personal information of employees and business contacts.

CCPA-type legislation is expected to be re-introduced in states where legislation failed to pass in 2019: Washington, Texas, New York, Hawaii, Maryland, Massachusetts, Mississippi, New Mexico and Rhode Island, and others.

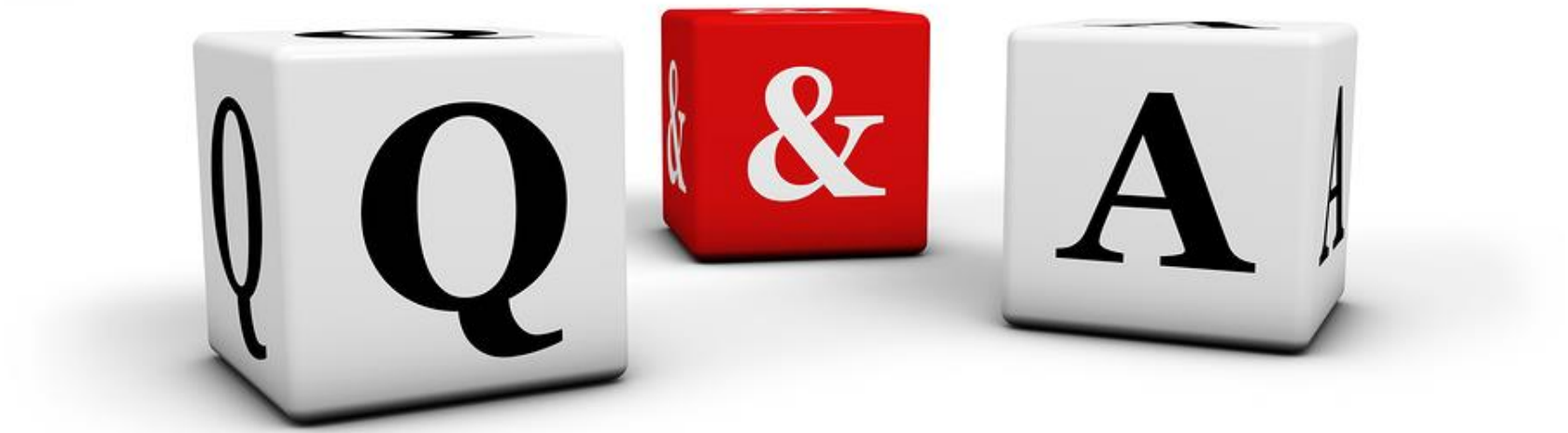
Other states' CCPA-style laws are similar in certain ways, but with key differences (e.g., focus on obtaining consent).

Federal Privacy

The prospect of having to comply with dozens of different state laws of this nature has fueled interest in a federal law to harmonize these proposals and provide businesses with clear compliance goals.

Outlook for Federal Privacy Legislation

- The Political Landscape
- The Playing Field & the Players
- House & Senate Update
- Main Street Privacy Coalition



CONEXXUS
solve forward

- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Profile: Conexxus.org
- Follow us on Twitter: @Conexxusonline

DISCLAIMER: Conexxus does not endorse any products or services that may be described or mentioned in this presentation. The views and opinions expressed in this presentation are solely those of the speakers and not of Conexxus. By hosting this webinar, Conexxus is not providing any legal advice; if you have any questions about legal issues raised or discussed, you should seek the assistance of attorneys who are competent in that area.