

CCPA: Should I be scared?



JOSHUA MARPET

- COO and co-founder of **Red Lion** with pending blockchain patent
- Accomplished speaker, executive, startup CEO, and graduate of the Mach37 Cyber -accelerator
- Member of the CEO organizations Mindshare and Missionlink
- One of the primary organizers of Security BSides Delaware
- Former board member of Hackers for Charity, BSidesLV, and CSA - DelVal
- Editor of the *SYNACK Journal of Information Security*
- Sleeps occasionally; shaves head at same rate...



JMarpet@redlion.io



@Quadling



RED LION

COMPLIANCE & SECURITY. CONNECTED

What is CCPA?

- California Consumer Privacy Act - AB-375
- “Information 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*.”
- A particular “consumer bill of rights” is addressed in CCPA, including:
 - The right to opt out - WITHOUT a change in price or quality!
 - The right to access
 - The right to delete
 - Opt-in for Children (For children under the age of 13, the opt-in must be collected from a parent or guardian.)



CCPA Action Timeline

- **AB-375** signed into law by Jerry Brown, Gov of CA, on June 28, 2018
- Amendments to the CCPA, Senate Bill 1121, passed September 23, 2018
- Jan 1, 2020- CCPA goes into effect
- California AG publish regulations between Jan. 1, 2020, and July 2, 2020
- Attorney General is precluded from bringing an enforcement action under the CCPA until the earlier of six months after the final regulations are published

CCPA Ideals

- Consumers know which personal data are being collected
- Consumers know whether their personal data are sold or disclosed, and to whom
- Say “no” to the sale of personal data
- Access their own personal data
- Equal service and price, even if they exercise their privacy rights



CCPA vs. GDPR

California Consumer Privacy Act

- For-profit businesses only
- Opt-out from *SALE* of personal data
- No special categories with extra protections
- Exemptions for medical data and personal information covered by HIPAA, GLBA, etc.

General Data Protection Regulation

- Not limited to for-profits, but specifies means of processing
- Opt-out from *PROCESSING* personal data
- Extra protections for special categories (Art. 9-10) and automated processing
- Medical data are not exempt



CCPA vs. GDPR

California Consumer Privacy Act

- Can sell personal data of children with opt-in (13-16) or parent/ guardian opt-in (<13)
- Exceptions allowed for research purposes
- Right to access personal data from the last 12 months
- Right to deletion (under specific conditions)

General Data Protection Regulation

- Can process personal data of children (<16) with parent/ guardian consent
- Exceptions allowed for research purposes
- Right to access all personal data processed
- Right to erasure/ “right to be forgotten”



CCPA vs. GDPR

California Consumer Privacy Act

- No requirements for dedicated compliance officers, risk assessments, or specific breach notifications
- \$7,500 per violation, per consumer - no max
- Private right of action can be \$100-750/ person/ incident, or actual damages if higher

General Data Protection Regulation

- Require Data Protection Officer, Data Protection Impact Assessments, and specific breach notifications
- Maximum of 4% of global annual revenues in penalties
- No guidance on floor/ ceiling for private right of action



Why do I care?

Do you:

- Sell to or collect personal information from CA residents?
- Work as a for-profit?
- Have >\$25MM annual gross revenue
- Buy/ receive/ sell/ share \geq 50k personal information records from consumers/ households/ devices

AND/ OR

- Earn \geq 50% annual revenue selling personal information?



What does CCPA mean for my business?

- Right to be informed of the categories of personal information that a business collects or otherwise receives, sells or discloses about them; the purposes for these activities; and the categories of parties to which their personal information is disclosed.
- Grants California residents the right to request more detailed information about the personal information a business holds specifically about them, and the right to obtain portable copies of their personal information from the business.
- Right to prohibit a business from selling their personal information, and to request that a business delete their personal information.
- Right to get service WITHOUT personal information collected, and no price differential



CCPA Sanctions

- Violations of the CCPA are enforceable by the California Attorney General, *of \$2,500 per violation, or up to \$7,500 per intentional violation.*
- Notably, the CCPA includes a private right of action with the potential for statutory damages, though as currently drafted this remedy is most likely intended to be limited to certain types of data security incidents.
- Companies, activists, associations and others can be authorized to exercise opt-out rights on behalf of California residents
- Companies that become victims of data theft or other data security breaches can be ordered in civil class action lawsuits to pay statutory damages between \$100 to \$750 per California resident and incident, or actual damages, whichever is greater,



CCPA - Does it affect me?

“Last year, AT&T launched the latest sexy trend in broadband -- charging users significantly more money if they want to opt out of their ISP's **snoopvertising**. It basically works like this: users ordering AT&T's U-Verse broadband service can get the service for, say, \$70 a month. But if you want to opt out of AT&T's Internet Preferences snoopvertising program (which uses deep packet inspection to study your movement around the Internet down to the second) you'll pay at least \$30 more, per month. *With its decision, AT&T effectively made user privacy a premium service.* ”

<https://www.techdirt.com/articles/20160329/08514034038/att-tries-to-claim-that-charging-users-more-privacy-is-discount.shtml>



CCPA - What you don't know

- 1. “Look Back” Provision** - Yes, the CCPA doesn't go into effect until New Year's Day 2020, but that compliance deadline comes with an obligation to deliver personal information collected, sold, shared or otherwise disclosed over the past 12 months —which means back to *Jan. 1, 2019*
- 2. Enforcement Delayed** - Again, yes, the compliance deadline is Jan. 1, 2020, but the attorney general may not bring an enforcement action until six months after publication of final regulations or July 1, 2020, whichever is sooner (Cal. Civ. Code § 1798.185(c)).
- 3. Private Cause of Action Not Based on CCPA Violation** - The plaintiffs' bar may be looking forward to filing the first private right of action under the CCPA, but a consumer's right to sue is not based on a violation of any of the CCPA's provisions. Rather, the private right of action created under Cal. Civ. Code § 1798.150 is for violations of an existing law, Cal. Civ. Code § 1798.81.5, which requires businesses to implement and maintain reasonable security procedures and practices.
- 4. “Personal and Olfactory Information” in a Consumer Suit** - The good news for businesses on the receiving end of a lawsuit—looking on the bright side here—is that any alleged failure to secure information will not be sufficient grounds for maintaining a cause of action.



CCPA - What you don't know (continued)

5. Consumer Rights Not Waivable - The CCPA creates a number of new consumer rights — among them, the right to disclosure, the right to deletion, and right to opt -out—but none of those rights may be waived or limited by contract.

6. Businesses Have Rights, Too - While the obligations imposed on businesses are substantial, the CCPA also creates a few rights for businesses, the most important of which is the right to cure. Both Cal. Civ. Code § 1798.150(b) and Cal. Civ. Code § 1798.155(b) grant businesses 30 days to cure alleged violations.

7. Deliberate Avoidance - Given the number of obligations imposed on businesses, it may be tempting for some organizations to devise workarounds to escape the law's provisions. Such workarounds, however, may be futile, for Cal. Civ. Code § 1798.190 expressly permits a court to disregard any “steps or transactions” taken with the intent to avoid the reach of the statute.



CCPA - What you don't know (continued)

8. Financial Incentive to Enforce - The CCPA creates a "Consumer Privacy Fund" to offset any costs incurred by state courts and the attorney general in relation to enforcement actions (Cal. Civ. Code § 1798.160).

9. Objections Raised - As of this presentation, the California attorney general is conducting a series of public forums as part of the mandate to adopt regulations that interpret the CCPA and establish procedures for compliance (Cal. Civ. Code § 1798.185). But a group of professors, attorneys, and other privacy professionals has reached out instead to the California Legislature, urging lawmakers in a letter drafted Jan. 17, 2019, to make "major changes" to the CCPA. The group identifies six areas of concern, including the law's inconsistencies with the GDPR and its overly broad definitions. The group suggests, among other things, that the legislature strive to harmonize the CCPA with the GDPR to "eliminate the need for two different compliance programs" or alternatively to provide a "CCPA safe harbor for GDPR-compliant businesses."



CCPA - What you don't know (continued)

10. Copycat Proposals Already in the Works - Other states are already looking to jump on the CCPA bandwagon:

- Massachusetts, for instance, [SD 341](#) looks remarkably similar to the CCPA
- Rhode Island's [SB 234](#), introduced Jan. 31, 2019, also contains a number of CCPA -like provisions
- Washington [SB 5376](#), introduced Jan. 18, 2019, also addresses consumer privacy rights, but it tracks more closely to the GDPR than the CCPA.
- New York's [A 465](#), introduced Jan. 9, 2019, would create a new "personal information protection act" establishing, among other things, a personal information bill of rights.
- <https://usprivacybill.intel.com/legislation/> -





Questions?



Joshua Marpet

@quadling

Jmarpet@redlion.io



RED LION
COMPLIANCE & SECURITY. CONNECTED



CCPA - References

- <https://usprivacybill.intel.com/legislation/>
- <https://www.techdirt.com/articles/20160329/08514034038/att-tries-to-claim-that-charging-users-more-privacy-is-discount.shtml>
- <https://blog.returnpath.com/gdpr-vs-ccpa/>



CCPA - PII Definition

(1) “Personal information” means an individual’s first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(A) Social security number.

(B) Driver’s license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

(D) Medical information.

(2) “Medical information” means any individually identifiable information, in electronic or physical form, regarding the individual’s medical history or medical treatment or diagnosis by a health care professional.

(3) “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

