

California's New Privacy Law An Opportunity for MSPs



Rachel Globus Sr. Marketing Manager, ESET

I am not a lawyer!

The information in this presentation is provided as a courtesy by ESET and does not constitute legal advice or client attorney relationship.

Seek an attorney's advice for your needs.

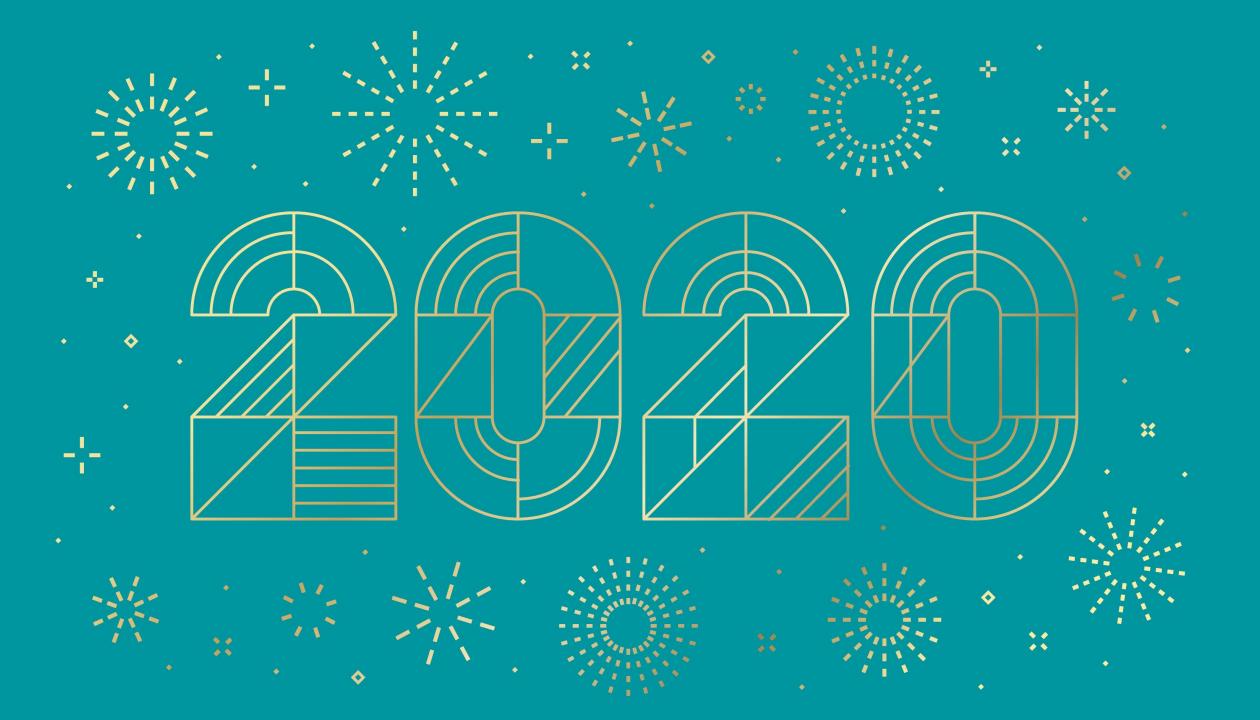








THE FUTURE





background:repeating-linear-gradient(-45deg,transparent,transparent 49%,#2b5672 40%,#2b5672 40%,transparent); background-size:6px 6px; background-repeat: repeat }.g-transparent-a: link,.g-transparent-a: visited {

1:width:1420 86,11 :position:abso ansparent;display:b :point ical-al ex-direction s:stretch} vout=fl ord ordinal oup:3:-webk.

#masterPage.mesh-layou

cont

ent}.transitioning-comp *{transition:inherit!important;-webkit-transition:inherit rerContainer{position:absolute;background-color:#fff;box-shadow:0 4px 10px 0 rgba(ight:45px;border-radius:100px;text-align:center}.selectionSharerContainer:after{ e;bottom:-10px;left:42%;border-width:10px 10px 0;border-style:solid;border-colo k;width:0}.selectionSharerContainer .selectionSharerOption{display:inline-bloc :top;padding:13px 11px 11px 13px;margin:1px;z-index:-1}.selectionSharerContai tor{margin-top:9px;margin-bottom:18px;background-color:#eaf7ff;height:26px;w ual-focus-on .focus-ring:not(.has-custom-focus):focus{box-shadow:inset 0 0 0 #3899ec!important}#masterPage.mesh-layout[data-mesh-layout=flex]{display ex;display:flex;-webkit-box-orient:vertical;-webkit-box-direction



order:2;order:2}#masterPage.mesh-layout[data-mesh-layout=flex] ata-mesh-layout=flex] #SITE_F00TER-placeholder{-webkit-box-ordinal-gr mesh-layout[data-mesh-layout=grid]{display:grid;grid-template-rows: -webkit-min-content -webkit-max-content;grid-template-rows:max-con splay:-ms-grid;-webkit-box-align:start;-webkit-align-items:start; tent ck:st tch;-webkit-justify-content:stretch;justify-content:stretch}#master [bi: FE_HEADER,#masterPage.mesh-layout[data_mesh-layout=grid] # /2}#masterPage.mesh-layout[data-mesh-layout=grid] #

obileView]{grid-area:2/1/3/2}#masterPage.mesh-layout[data-mesh-layou 74/2}#masterPage.mesh-layout[data-mesh-layout=grid] #SITE_FOOTER,#master #SITE_F00TER-placeholder{grid-area:4/1/5/2}#masterPage.mesh-layout apinlingContentigrid_area: 1/1///21#masterPage mech_layout decktons fuidth

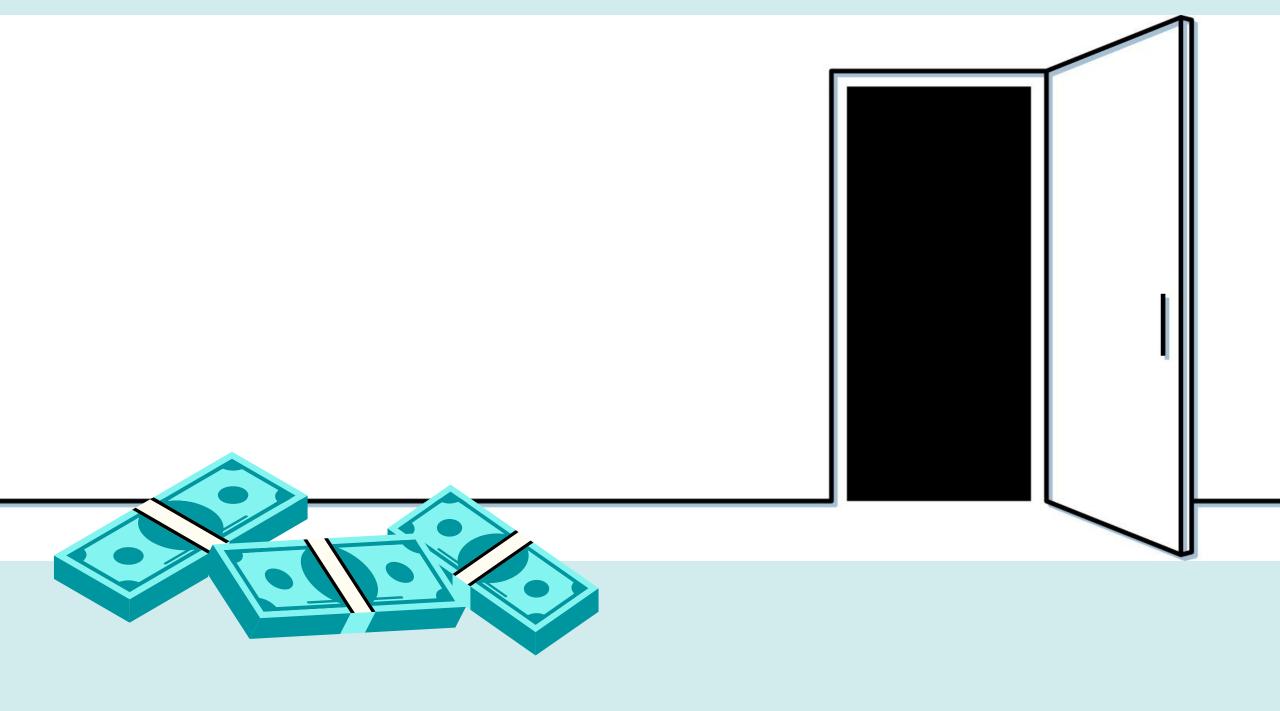
CALIFORNIA CONSUMER PRIVACY ACT

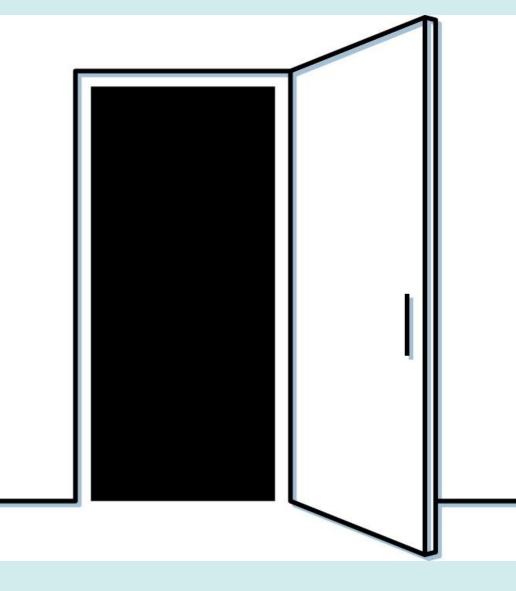












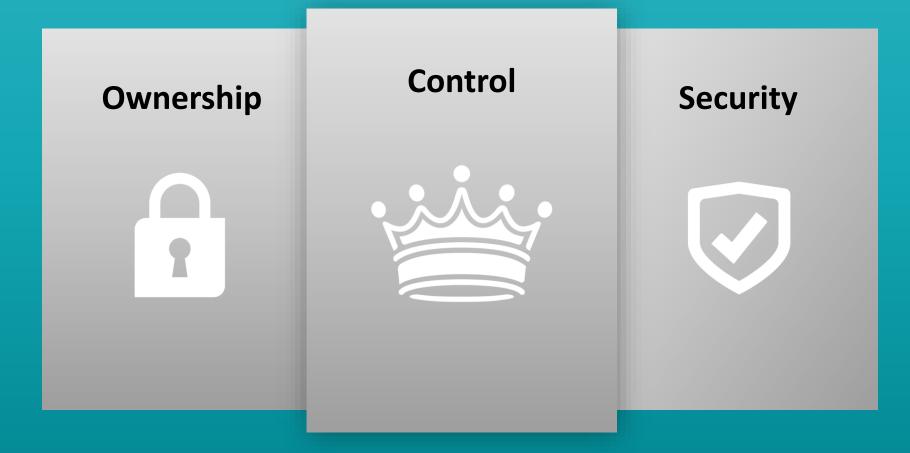
REASONABLE SECURITY

A REAL PROPERTY OF THE PARTY OF THE PARTY.

per daily and Spetitist large structures of time spectracy large methods are beinging of the special and sensitive in payment locking for a special point of the special point structure and sensitive in payment to account second-second respective structures appoint ranky. We also receive a second second-second respective to the second second and any second second bios access control accession of point daily methods any second bios access control accession and the structure appoint and the special bios access control accession and point daily method second accession accession and accession accession and any structure appoint.



What is the California Consumer Privacy Act?



What information does CCPA apply to?



Privacy aspects of CCPA created a new definition of "personal information":

 Any information that identifies, relates to, describes, or is capable of being associated with a natural person who is a California resident...

What information does CCPA apply to?



Security and breach aspects of CCPA apply to "personal information" as that phrase is defined under Civil Code 1798.81.5

For-profit business that does business in California and meets one of the following criteria...



Annual gross revenues > \$25,000,000; or



Derives 50% or more annual revenues from selling consumers' personal information; or



Annually buys, receives, sells, or shares PI of **50k+** consumers, households or devices





Who does it apply to? CCPA Readiness Quiz





How will it be enforced?



Attorney General may assess \$2,500 to \$7,500 in penalties for each violation of the CCPA's provisions generally

How will it be enforced?



Data breach victims can sue for damages from \$100 -\$750 per consumer per incident or actual damages

Arguably the greatest risk to covered businesses involves data security...

Source: Chronicle of Data Protection, Hogan Lovells US LLP

CCPA and "reasonable security"

Penalty for breaches arises from a "violation of the duty to implement and maintain reasonable security procedures and practices."





What is "reasonable security"?

15 Steps to "Reasonable Security"

other ESET experts // August 2019

15 STEPS TO "REASONABLE SECURITY" Fony Anscombe and

January 1, 2020. That's the date the California Consumer Privacy Act (CCPA) takes effect. Your business could be bound by the act's provisions regardless of whether your business is located inside or outside of California. Being a small- or medium-sized business doesn't mean you're too small to be impacted, either. That's because the thresholds that would bring you under the act are based not on business size, but on the amount and type of the consumer data that you gather, handle or store - or that you engage others to gather, handle or store on your behalf. For more information about the many provisions of the act and to evaluate whether you fall under its scrutiny, read our white paper, Practical Guide to CCPA and Data Security.

One of the key provisions of the act is that businesses subject to the law must "implement and maintain reasonable security" procedures and practices to protect. certain consumer data. Exactly what constitutes "reasonable security" isn't defined within the act. But there is plenty of guidance to draw from, published by authorities such as the Center for Information Security, National Institute of Standards and Technology and the Federal Trade Commission. Based on ESET's security expertise as well as these recognized sources, this brief will help you understand what steps to take now to secure your consumer data in time to meet the deadline.

Start with the data itself. Every company collects data regardless of how big or small they are or even what business they are in. Suppose you're a contractor storing customer phone numbers in your phone. That is data collection that includes personal information. Unless the phone contains 50,000 names, that's far below the threshold required by the act. But what about a large contractor with

50,000 - meeting one of the thresholds and making the company subject to the act

200 employees, with 250 names in each phone? That's



Start with the data itself. Every company collects data regardless of how big or small they are or even what business they are in. Moreover, personal information can be and is stored everywhere. It may be challenging to understand what personal information exists, where it resides, who has access and for what purpose. But you first need to take a thorough look at your data to understand how it should be treated and protected under the act.



Data that you don't have is data that you don't need to protect from being breached. Don't collect personal information needlessly. Hold onto it only as long as you have a legitimate business need for it. And don't use personal data when it's not necessary. Purging non-essential information assists in complying with privacy requirements and mitigates risk to the business

eset

point a Data ection Officer

to the where, what and why

o protect it, appoint a Data

PO). The DPO is primarily

should categorize the data.

licy to be created so that only

be blocked by policy, ensuring

from a remote device. Put contro need to be able to see the data or

passwords and authentication You should already have a password policy in force

5. Require secure

which requires upper and lower case, numbers, special eing your data protection strategy characters and the like, with the requirements to change CCPA. The DPO's responsibilities the passwords frequently and to stop previous passwords from being used again. Protect against brute force attacks - repeated attempt to input passwords - by mpany and employees on limiting the number of retries. In addition to user name/ nce requirements password, consider implementing strong authentication. to ensure compliance and Using a physically separated device, such as a phone, sues proactively for a second authentication factor is a best practice ved in data processing whenever you're faced with regulatory compliance. Test ance and providing advice on all access methods, ensure security patches are installed rotection efforts on all software involved, and put monitoring in place to nt of contact for the business on ensure there is no unauthorized access.



ontrol access to In addition to requiring strong passwords, pay attention sensibly to how you store them. It's your responsibility to store need to know or have access conal information contained in access to it. The DPO or person

passwords securely as part of your customers' personal data. A perpetrator who breaches your data could use the improperly stored password to masquerade as your customer to access your systems, and possibly accounts on other companies' systems if the customer uses the same password. This escalates the effect the breach of your system has on the consumer, exposing you to granted access based on their licy should go further and may greater damages. For security reasons, store passwords in hashed form, or even better, hashed and salted what devices individuals can access Hashed or hashed-and-salted nasswords are useles data that isn't directly essential or



eset.com/us/ccpa-partner

When does it go into effect?

Companies must comply by January 1, 2020



When does it go into effect?

Enforcement actions by the Attorney General begin by July 1, 2020



THE OPPORTUNITY

GLOBAL TREND TOWARD PRIVACY LEGISLATION

CHINA Personal Information Security Specification (May 2018)

(expert committee issued draft, parliamentary bill expected in December 2018)

AUSTRALIA

Privacy Act 1988 and amendments (last amended in March 2014, including 13 Australian Privacy Principles)

CALIFORNIA Consumer Privacy Act (entering into force in July 2020)

÷.

USA Federal Data Privacy Law (not yet in drafting stage)

(still In drafting stage)

BRAZIL

General Data Protection Law (LGPD -Law 13.709) (entering into force in February 2020)

EU

ePrivacy Regulation

(still In drafting stage)

CANADA

Digital Privacy Act (2015)

Documents Act (Pipeda)

Reforming the Personal Information

and Protection and Electronic

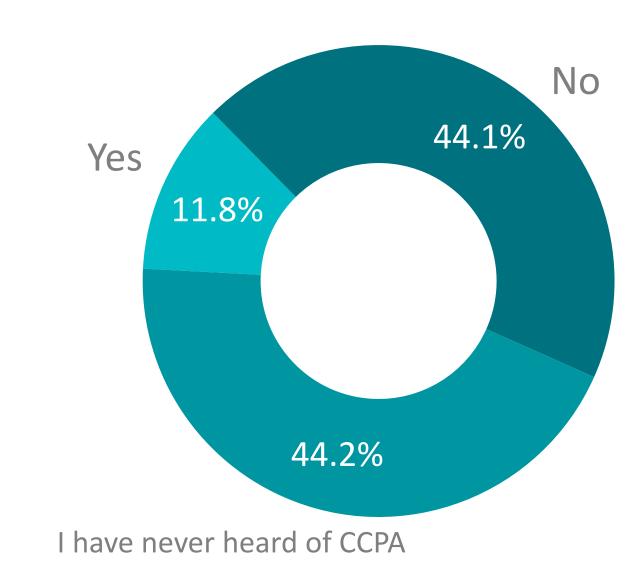
As California goes...

- 12% of all U.S. residents
- 5th largest economy globally
- First to pass a law mandating data breach notifications
- Home of Google, Facebook, Apple, HP, Oracle...



CCPA SURVEY

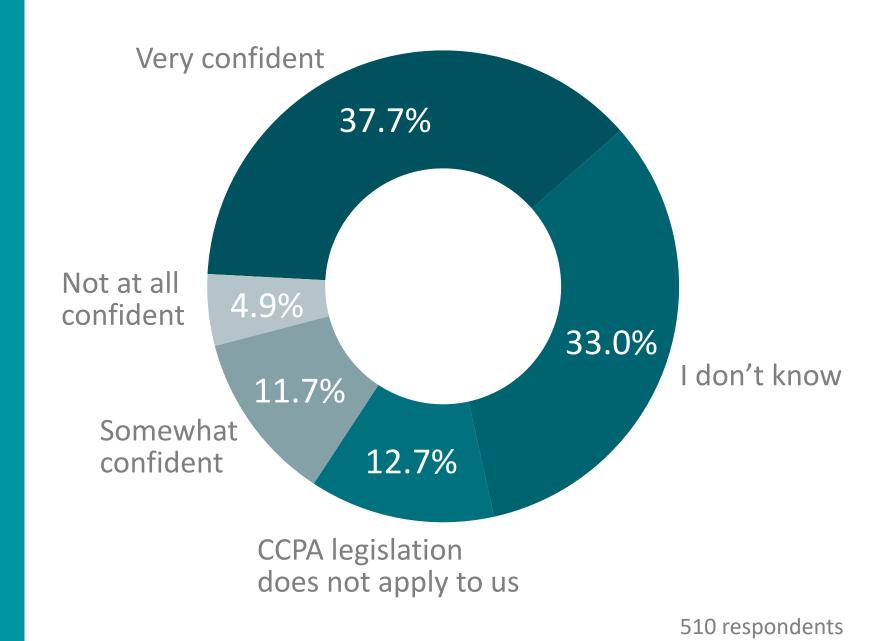
Do you know if the California Consumer Privacy Act (CCPA), effective January 1, 2020, applies to your business?



751 respondents

CCPA SURVEY

CCPA requires "reasonable security." How confident are you that your organization will be compliant as of January 1, 2020?



Interest in CCPA over time



Source: Google Trends search Oct. 15, 2019

ESET Security Solutions to Support CCPA Compliance

- Endpoint protection
- Two-factor authentication
- Encryption
- Security awareness training
- Data leak prevention
- Backup and recovery





LEARN MORE

eset.com/us/ccpa-partner

