ENJOY SAFER TECHNOLOGY®

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.

AGENDA

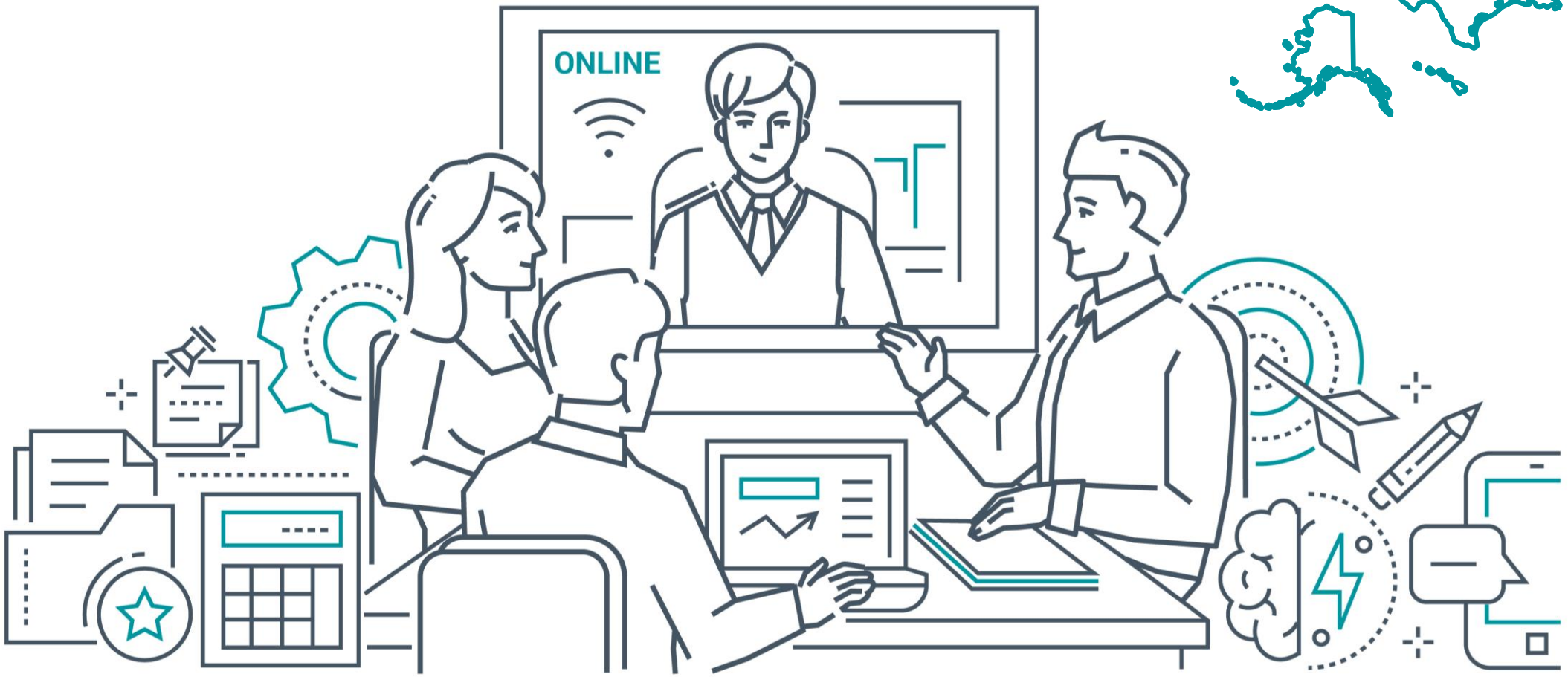
THE FUTURE

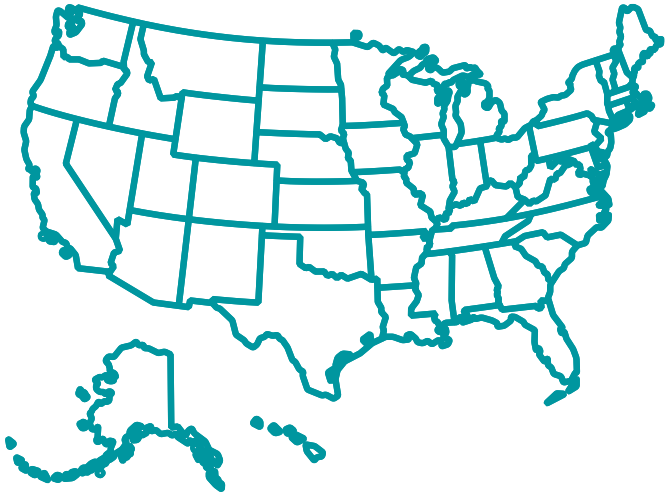
THE LAW

THE OPPORTUNITY

THE FUTURE


2020

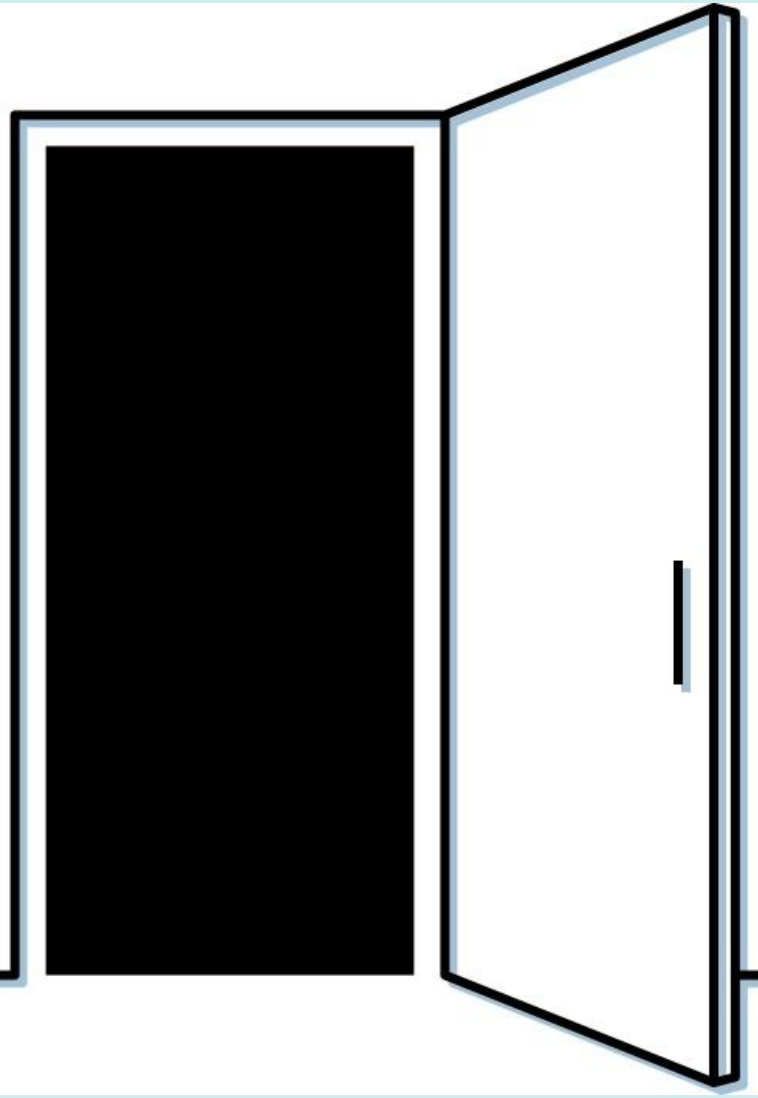

ONLINE

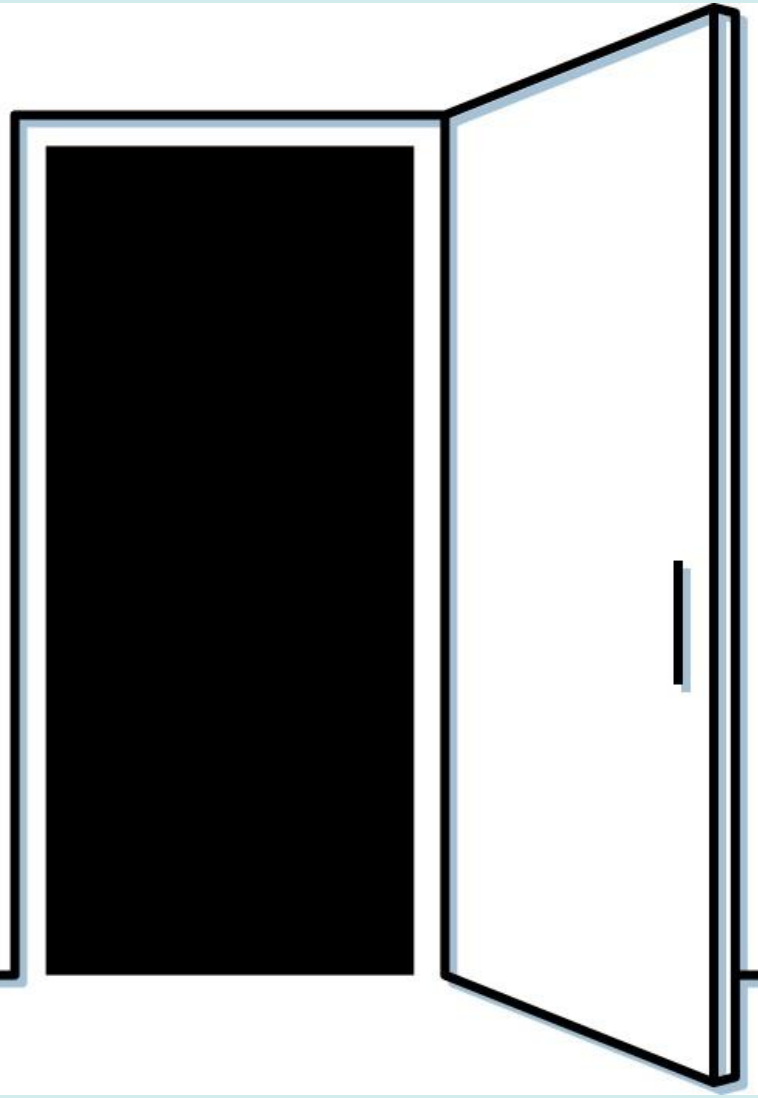



HACKED!

CALIFORNIA CONSUMER PRIVACY ACT

2020





REASONABLE SECURITY


OPPORTUNITY

THE LAW

What is the California Consumer Privacy Act?

Ownership

Control

Security

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

Who does it apply to?

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

Who does it apply to?

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

Who does it apply to?

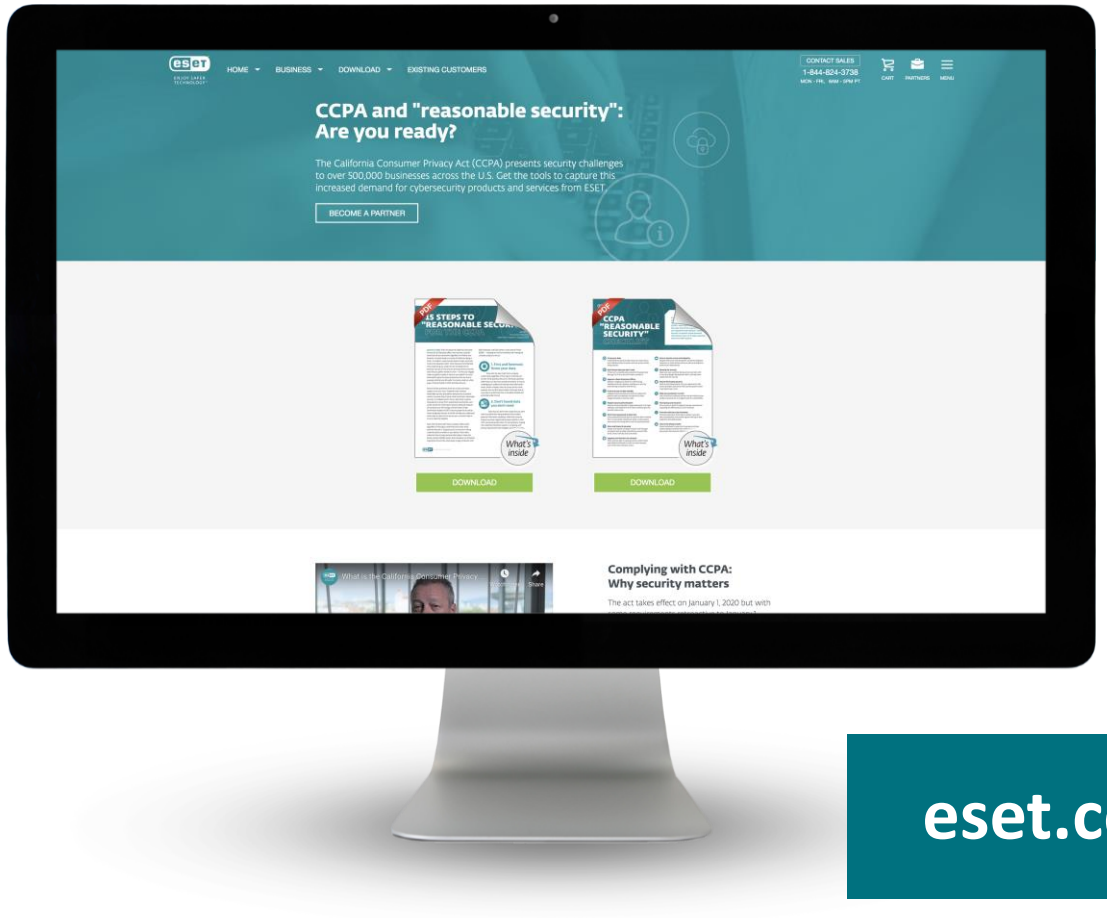
Derives **50% or more annual revenues** from selling consumers' personal information; or

Who does it apply to?

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

Who does it apply to?

CCPA Readiness Quiz



eset.com/us/ccpa-partner

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”

15 STEPS TO “REASONABLE SECURITY” FOR THE CCPA

AUTHORS: Tony Anscombe and other ESET experts // August 2019

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 200 employees, with 250 names in each phone? That’s 50,000 — meeting one of the thresholds and making the company subject to the act.

1. First and foremost: Know your data

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.

2. Don’t hoard data you don’t need

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 ENJOY SAFER TECHNOLOGY™

1

5. Require secure passwords and authentication

You should already have a password policy in force which requires upper and lower case, numbers, special characters and the like, with the requirements to change the passwords frequently and to stop previous passwords from being used again. Protect against brute force attacks — repeated attempt to input passwords — by limiting the number of retries. In addition to user name/password, consider implementing strong authentication. Using a physically separated device, such as a phone, for a second authentication factor is a best practice whenever you’re faced with regulatory compliance. Test all access methods, ensure security patches are installed on all software involved, and put monitoring in place to ensure there is no unauthorized access.

6. Don’t store passwords in plain text

In addition to requiring strong passwords, pay attention to how you store them. It’s your responsibility to store 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 greater damages. For security reasons, store passwords in hashed form, or even better, hashed and salted. Hashed or hashed-and-salted passwords are useless

eset.com/us/ccpa-partner

When does it go into effect?

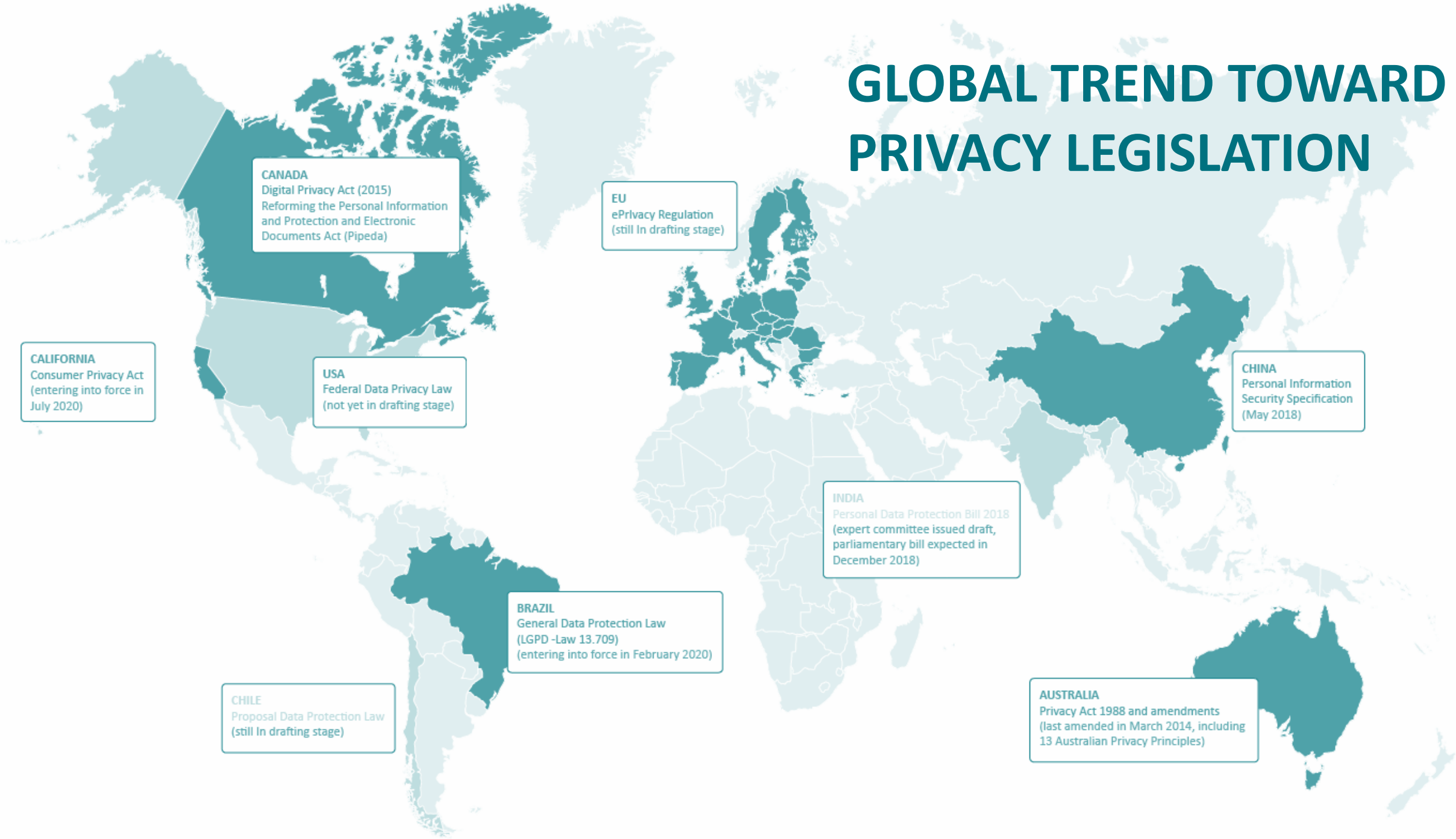
Companies must comply
by **January 1, 2020**

When does it go into effect?

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

THE OPPORTUNITY

GLOBAL TREND TOWARD PRIVACY LEGISLATION

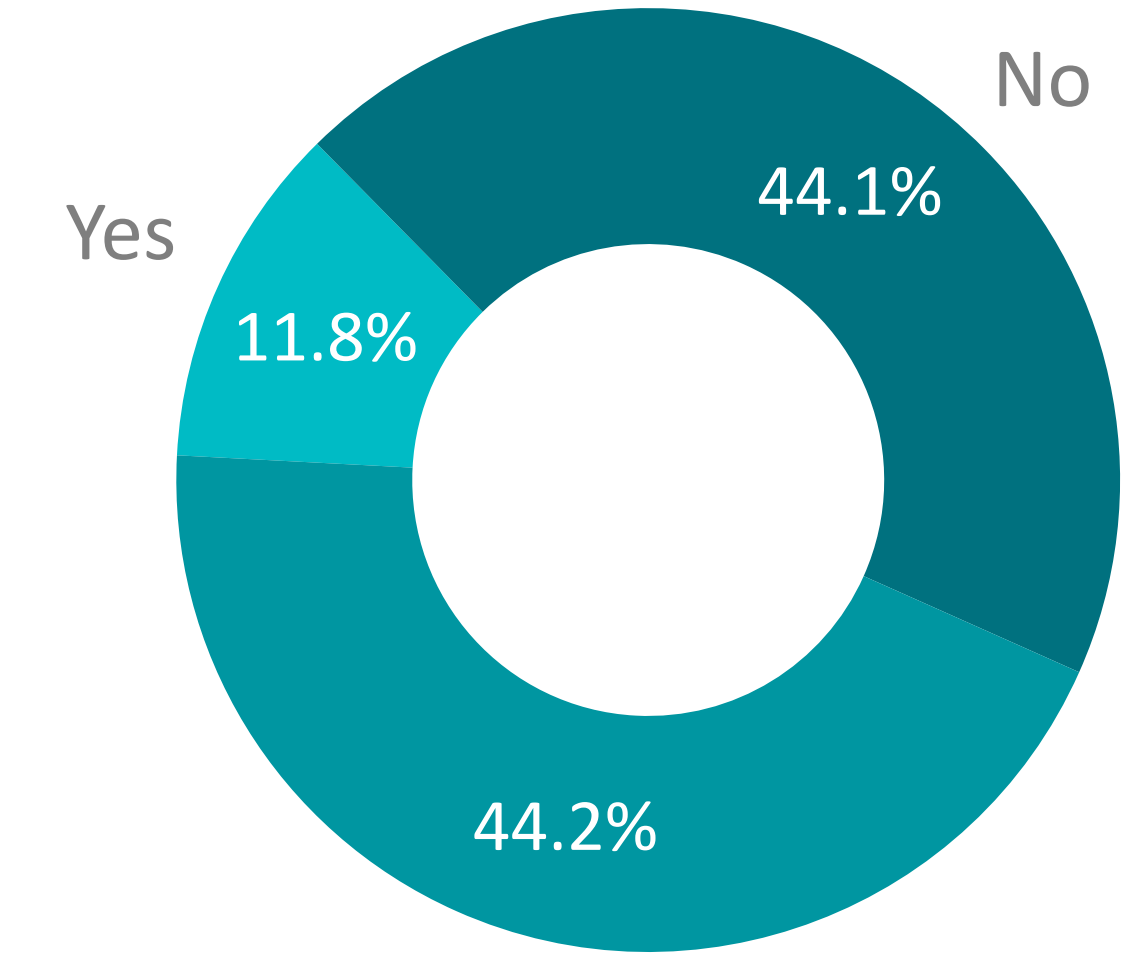


As California goes…

- **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

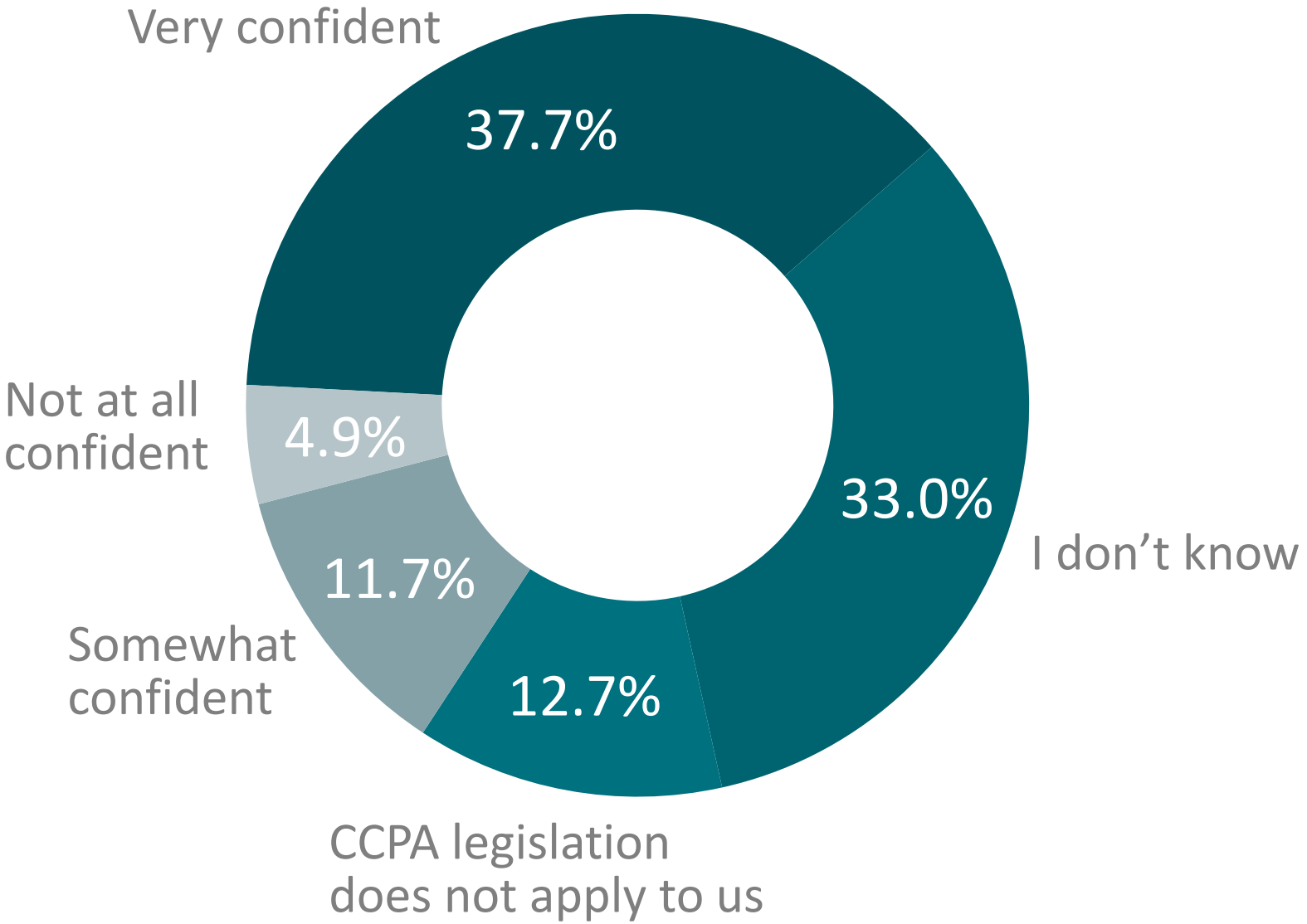
Do you know if the California Consumer Privacy Act (CCPA), effective January 1, 2020, applies to your business?



751 respondents

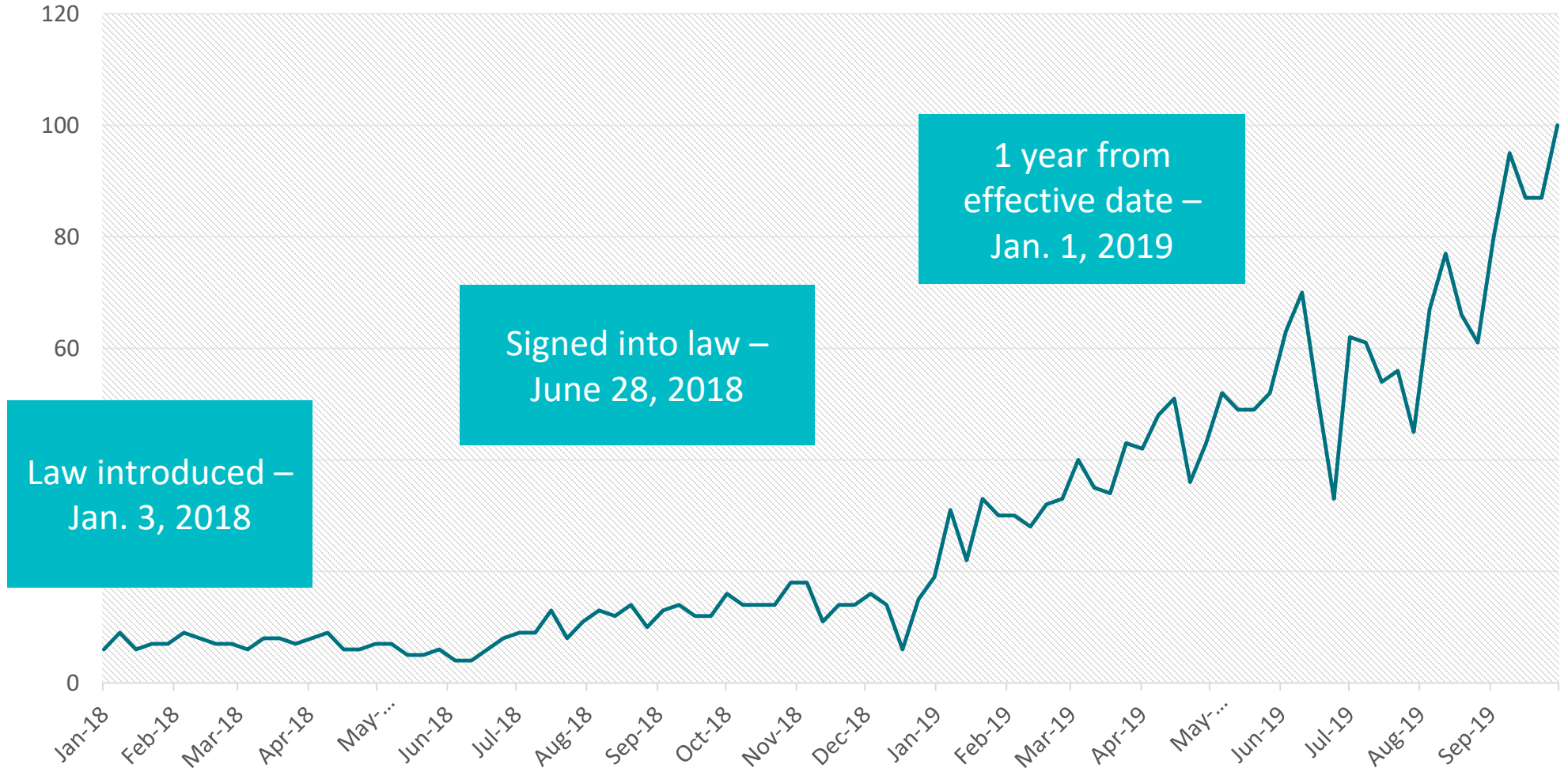
CCPA SURVEY

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



510 respondents

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

Stop by ESET booth #416

LEARN MORE

eset.com/us/ccpa-partner

ENJOY SAFER TECHNOLOGY®