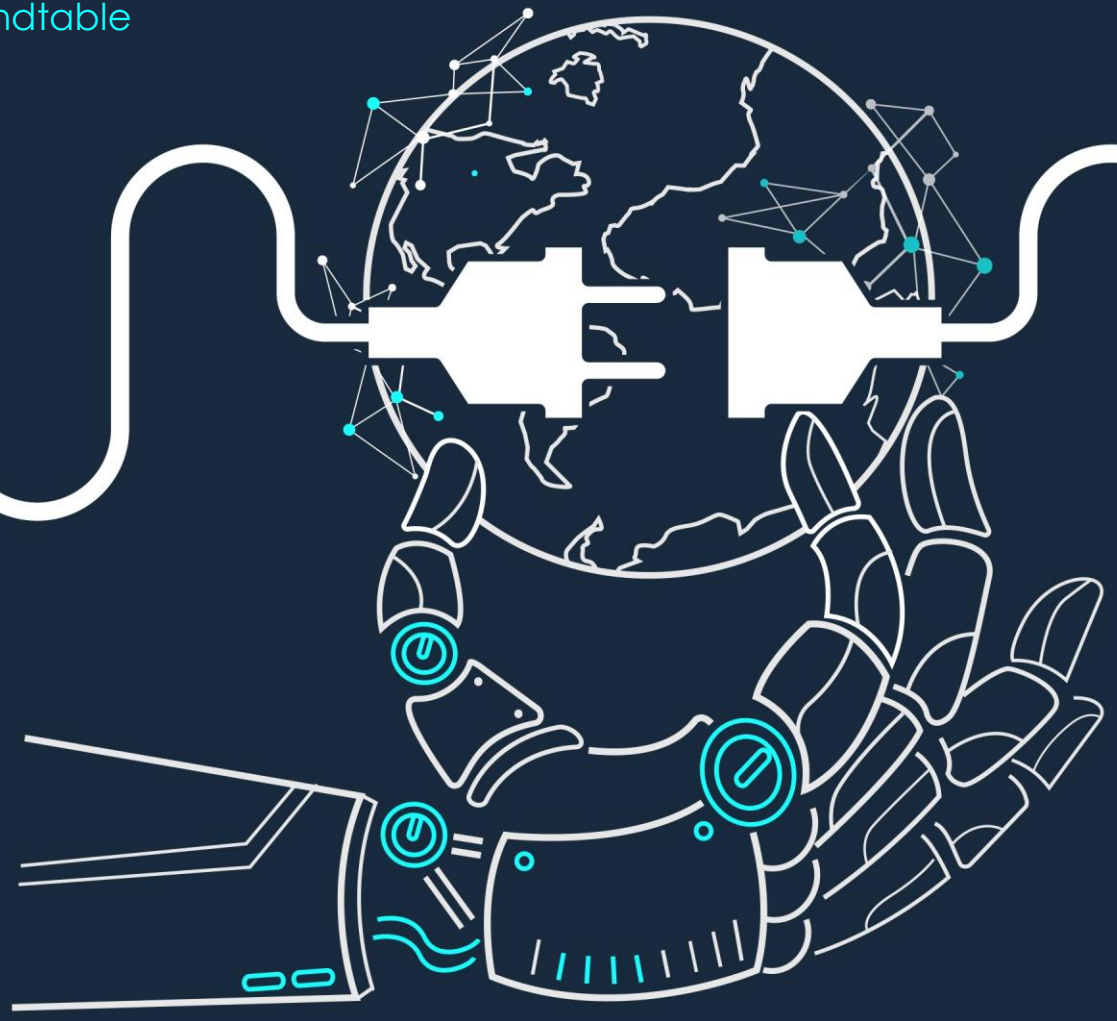
March 19, 2019

Association of Corporate Counsel Regulatory Law Roundtable



Plugging Into the Internet of Things

Demystifying the Regulatory Landscape

SPEAKERS

Elizabeth Balfour
Partner
Sheppard Mullin

Rebeca Perez-Serrano
SaaS and Digital Health Technologies Senior Counsel
ResMed

Justine Phillips
Partner
Sheppard Mullin

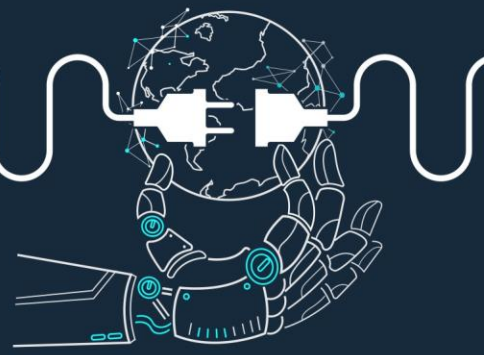
MEDICAL DEVICE CONNECTIVITY

- Trend toward value-based care in Healthcare
- Promote patient engagement to achieve improved compliance and better outcomes
- Digital therapeutics: could apps supplant medications?
- Data analytics to manage conditions, predict behavior

- Facilitate coordinated care
- Potential regulatory changes to align with care coordination: proposed HIPAA rule changes that encourage the sharing of PHI amongst covered entities and between healthcare providers and loved ones/caregivers

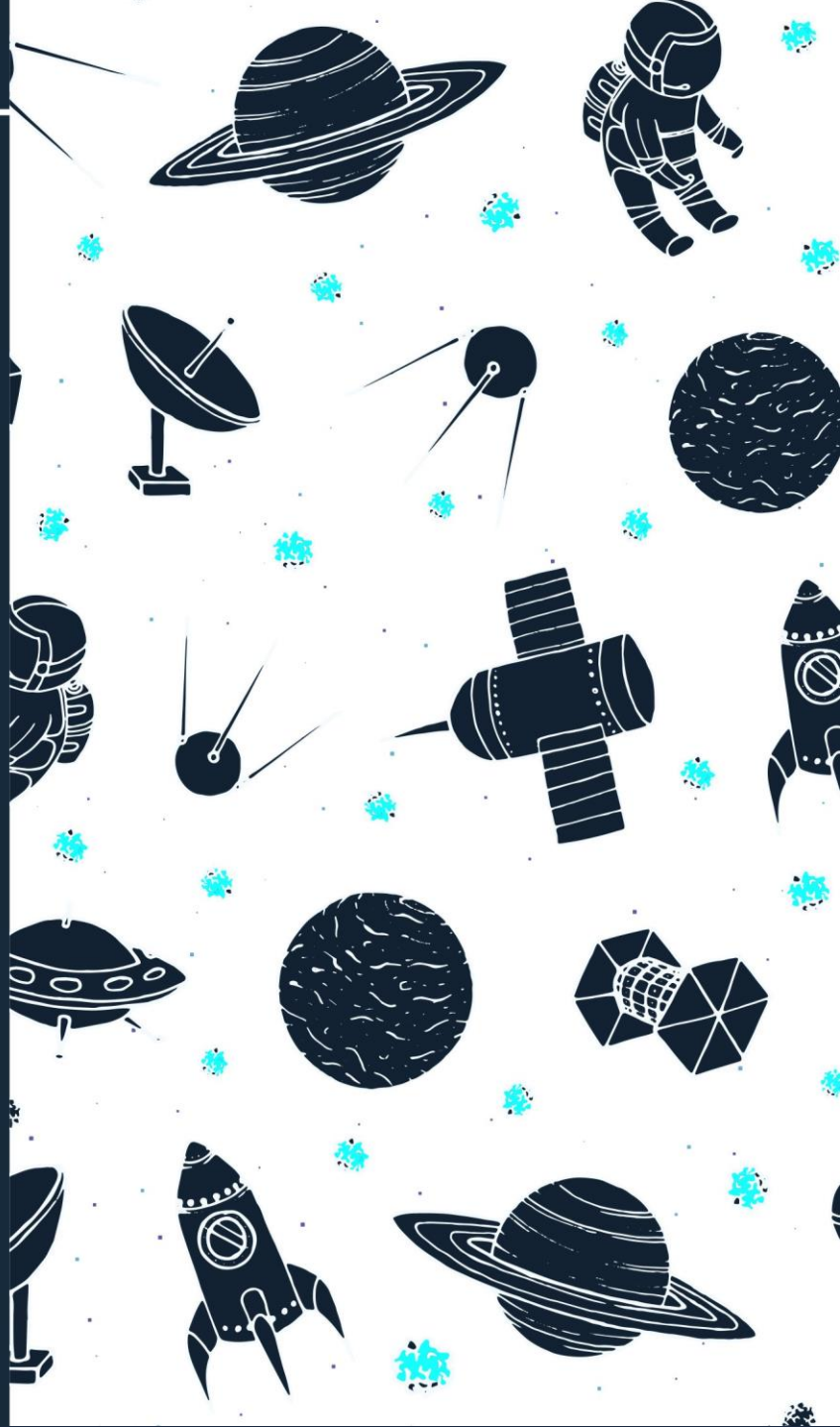
CONNECTED DEVICES IN HOMES

- Devices such as Nest, Alexa, and even baby monitors facilitate access and control over our surroundings
- These devices collect an enormous amount of data that gets sent to the cloud
- What are the protections that need to be built into these devices under the Internet of Things Law?
- What must be done with the consumer data gathered by these devices under CCPA?
- We'll take you and your Alexa device on a journey to explore answers to these and other questions



THE PRIVACY FRONTIER

- 1972 California amends Constitution to include right of privacy
- 2000 California legislation established an Office of Privacy Protection
- 2002 California passes online "breach notification" law
- 2004 Online Privacy Protection Act
- 2005 Shine the Light



IOT LEGISLATION

Mirai Malware 2018

- California passes SB 327 Internet of Things: “smart device” security and privacy
- Requires manufacturer of a connected device to equip the device with reasonable security features designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.
- Effective 1-1-2020

IOT LEGISLATION

Who Does it Apply To?

- All manufacturers of connected devices, which include companies that manufacture, or contract with a third party to manufacture, connected devices sold or offered for sale in California

What is a reasonable security feature?

- If a device has the ability to authenticate outside a local area network, the security feature is deemed reasonable if either:
(1) the preprogrammed password is unique to each device; or
- (2) the security feature requires the user to generate a new means of authentication before access is granted to the device for the first time

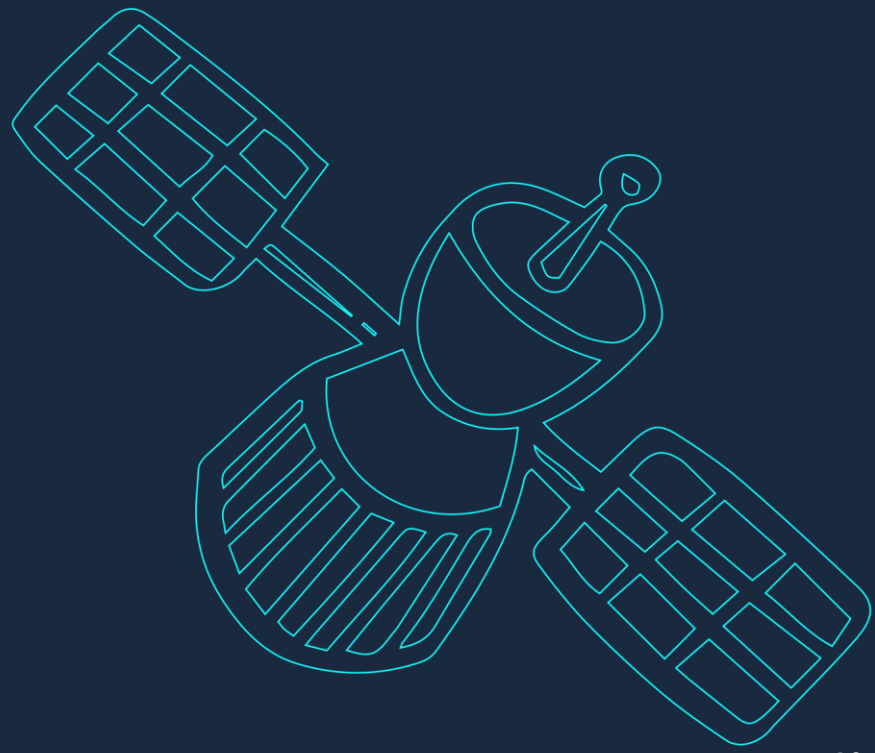
CALIFORNIA CONSUMER PRIVACY ACT

A rushed piece of legislation that:

- **Requires businesses to implement "reasonable security" and be more transparent** about the way they use consumers' personal information
- **Provides consumers with**
  - The right to limit collection, use, or disclosure of their data
  - The right to request a business delete their personal information (the right to be forgotten)
  - The individual right to sue businesses if their data is breached
- **Permits the Attorney General and consumers to recover fines and damages**

WHO DOES THE CCPA APPLY TO?

- **For-profit Businesses** that:
  - Have **gross annual revenue** in excess of **$25 million**; or
  - Buy, receive, sell, or share personal information from **50,000 or more consumers, households, or devices**; or
  - Derive **50% or more of their annual revenue** from selling personal information



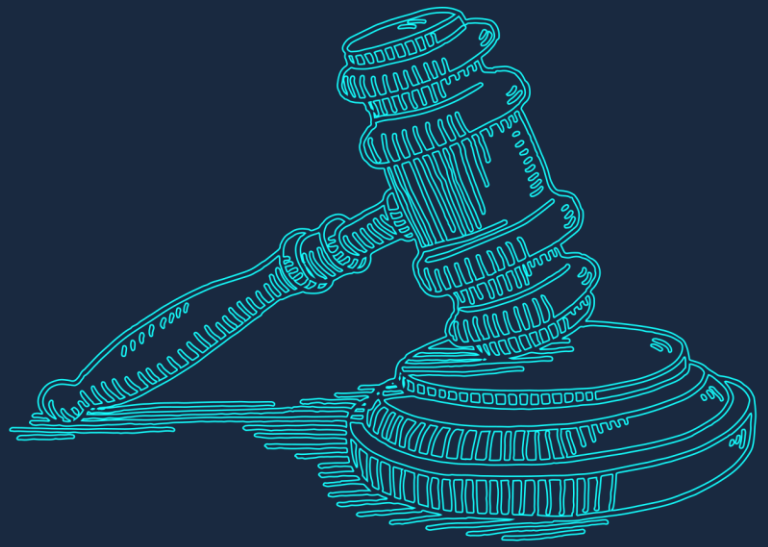
WHAT IOT DATA DOES CCPA APPLY TO?

- Security and breach aspects of CCPA apply to “personal information” as that phrase is defined under Civil Code 1798.81.5
- Privacy aspects of CCPA applies to 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…see next slide because it is so broad we could not fit it on this slide.

"PERSONAL INFORMATION" INCLUDES IOT GENERATED DATA

- **Biometric data**
  - Biological or behavioral characteristics
  - DNA
  - Iris image or retina
  - Fingerprint, hand, or palm
  - Facial recognition
  - Vein patterns
  - Voice recordings
  - Keystroke patterns or rhythms
  - Sleep
  - Health
  - Exercise data
  - Gait patterns or rhythms
- **Commercial information**
  - Records of personal property
  - Product or service purchase, review, consideration history
- **Geolocation data**
- **Medical information**
- **Health insurance data**
- **Characteristics of a protected classification under California or Federal law**
  - Race
  - National origin
  - Ancestry
  - Religion
  - Physical or mental disability or other medical condition
  - Marital status
  - Sex
  - Age
  - Sexual orientation
- **Internet or network activity information (cookie data)**
  - Browsing history
  - Search history
  - Information about a consumer's interaction with a website or application
  - Advertisement interaction
- **Personal information**
  - Real name
  - Alias
  - Postal address
  - Telephone number
  - Unique personal identifier
  - Online identifier
  - IP address
  - Email address
  - Account name
  - Social security number
  - Driver's license, identification, passport number, etc.
  - Signature
  - Insurance policy number
  - Education
  - Employment
  - Bank, credit, or other financial account number

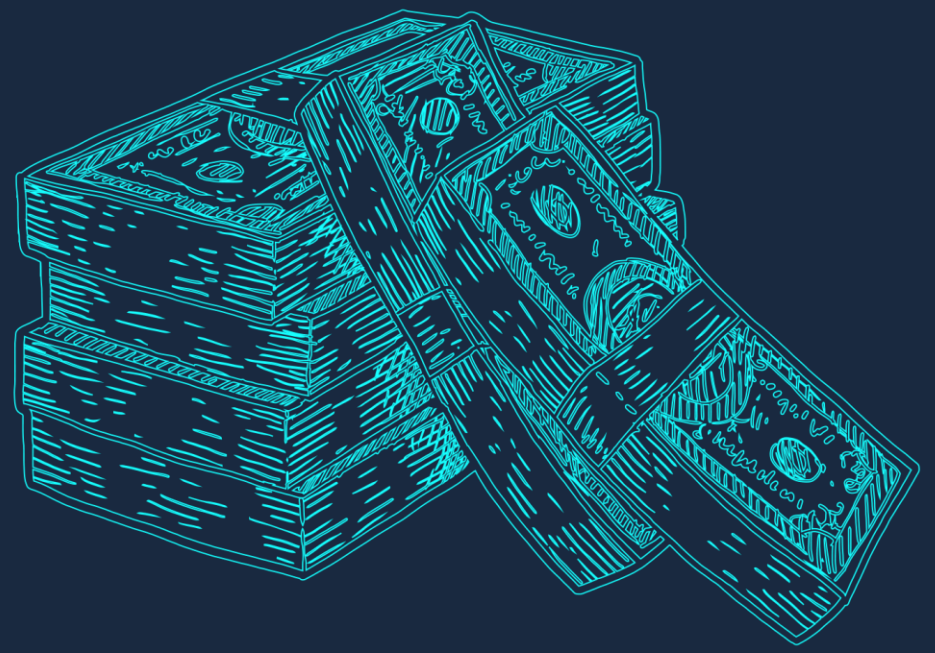
WHEN DOES THE CCPA COME INTO EFFECT?



- Companies must comply by **January 1, 2020**
- **Enforcement actions** by the Attorney General begin **July 1, 2020**
- Businesses need to be thinking about CCPA **now** because in responding to consumer requests about their data, businesses must provide information **dating back 12 months**
  - If a consumer access request is made on January 1, 2020, then businesses must provide information dating back to January 1, 2019

ENFORCEMENT BY ATTORNEY GENERAL

- Privacy enforcement is currently only by State Attorney General.
- Public forums being held throughout California.
  https://oag.ca.gov/privacy/ccpa/rsvp
- Attorney General may assess **$2,500 to $7,500 in penalties for each violation** of the CCPA's provisions generally



WHAT IS "REASONABLE SECURITY" UNDER CCPA?

- CCPA gives Californian's the right to bring a civil action against a business for failing to "implement and maintain **reasonable security** procedures and practices appropriate to the nature of the information."
- Statutory damages range from $100-$750 per consumer, per incident.
- "Reasonable security" is explained in the Attorney General's 2016 Data Breach Report and includes:
  - 20 Controls from the Center for Internet Security's Critical Security Controls (formerly the "SANS Top 20")
  - multi-factor authentication
  - data minimization
  - encryption

CRITICAL CONTROLS

- **1:** Inventory of Authorized and Unauthorized Devices
- **2:** Inventory of Authorized and Unauthorized Software
- **3:** Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- **4:** Continuous Vulnerability Assessment and Remediation
- **5:** Controlled Use of Administrative Privileges
- **6:** Maintenance, Monitoring, and Analysis of Audit Logs
- **7:** Email and Web Browser Protections
- **8:** Malware Defenses
- **9:** Limitation and Control of Network Ports, Protocols, and Services

DIGITAL ASSET MANAGEMENT TIPS

- Identify hardware and software including all IOT devices and databases
- Rally key stakeholders and interview them to identify data
- Locate all the places the data lives
- Classify the data
- Cost/benefit analysis to collect and maintain data
- Automate deletion/destruction based on creation or use data
- Establish processes/protocols to identify and delete data

INFORMATION GOVERNANCE AND SERVICE PROVIDERS

- SaaS agreements: embedding data security and privacy into the language
- Vendor diligence
- Privacy impact assessments
- Auditing of cloud providers and vendors to ensure compliance with contractual provisions
- Effective tools:

  OneTrust
  Free, open-source options that will track cookies ("cookiepedia")
- SECURE SECURE SECURE Personal Information and document your good cyber practices

QUESTIONS