TECH SAN DIEGO PRESENTS

CYBERSECURITY SUMMIT

POWERED BY

eseT® **Sheppard Mullin**

Stephen Cobb

Senior Security Researcher

ESET

Justine Phillips

Cyber Attorney

Sheppard Mullin

Alexandra Albro

VP, General Counsel

ESET

OVERVIEW

This subconscious psychology test reveals the link between vision and personality

GET STARTED!
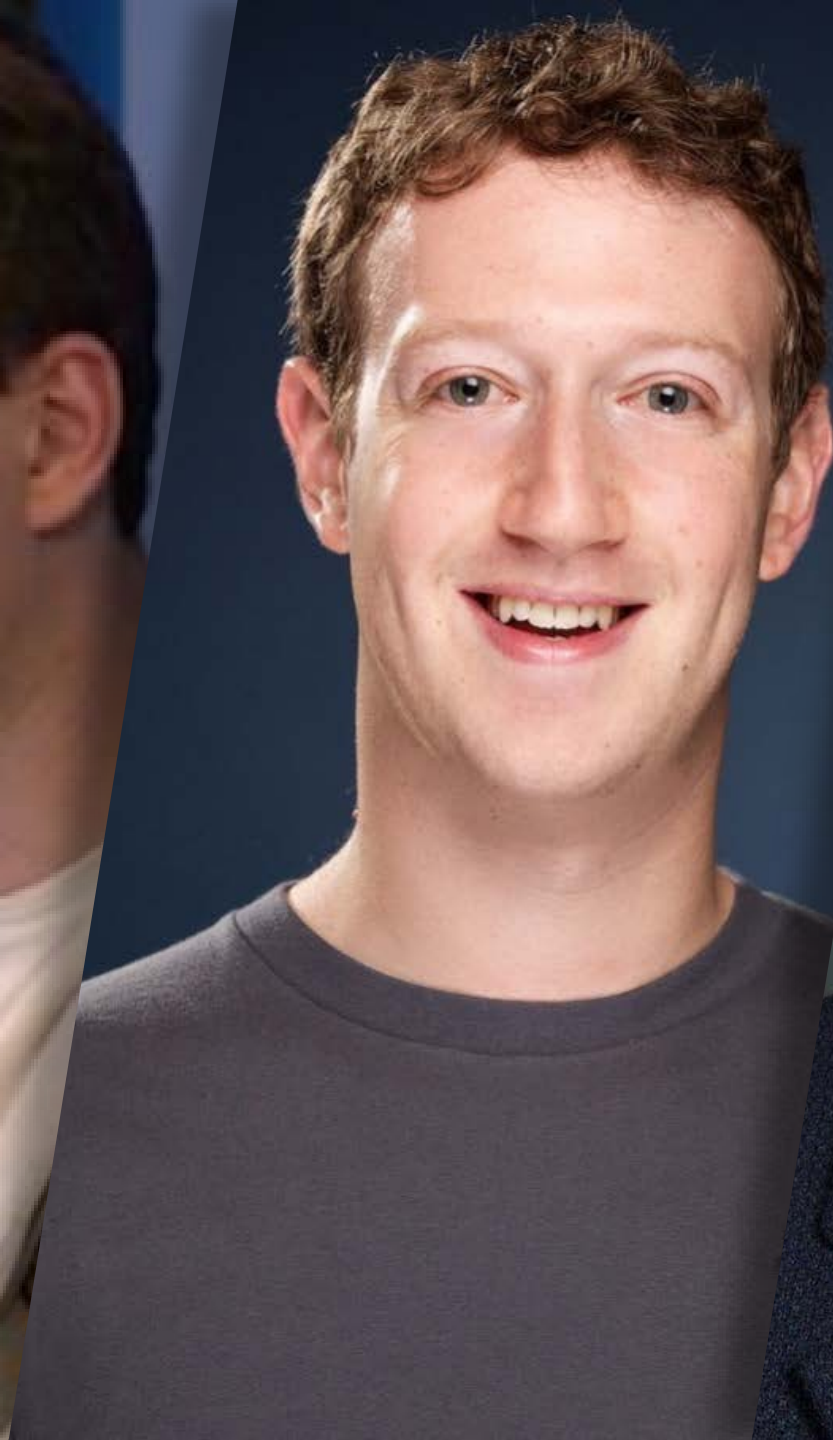
California Consumer Privacy Act

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

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

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

1. An individual's first name or first initial and 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:

    - Social security number.

    - Driver's license number or California identification card number.

    - Account number or 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.

    - Medical information.

    - Health insurance information.

    - Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

2. A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

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…
- See next slide because it is so broad we could not fit it on this slide…

"Personal information" is now incredibly broad

1. 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

2. Commercial information

- Records of personal property
- Product or service purchase, review, consideration history

3. Geolocation data

4. Medical information

5. Health insurance data

6. 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

7. Internet or network activity information (cookie data)

- Browsing history
- Search history
- Information about a consumer's interaction with a website or application
- Advertisement interaction

8. 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

(h) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and 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:

(A) Social security number.

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

(C) Account number or 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.

(E) Health insurance information.

(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

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

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

- 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

- Privacy enforcement is currently only by State Attorney General

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

- Security is private right of action, like PAGA with statutory damages set at $100-750 per consumer

Implications for BUSINESSES

IT systems

- Who is responsible for picking the right technologies for the company
- How do you track incoming requests and response times

Financial impact

- Cost of compliance implementation
- Cost of litigation/investigation

Marketing impact

- Change implementation
- Staffing needs

Business systems impact

- Systems compliance

- Attorney-client privilege serves to protect the client from information disclosure

- Attorney-client privilege – your communications with outside counsel and in-house counsel are privileged

- Make sure any questions regarding the law and your (non)compliance are communicated through the in house-outside counsel to maintain privilege

- Prevent unnecessary disclosure by communicating wisely

Impact to CYBERSECURITY

"A violation of the duty to implement and maintain reasonable security procedures and practices."

Minimum requirements for "defensible defense"

✓ A designated person in charge of security, also privacy

✓ Documentation of your relatively recent risk assessment

✓ A coherent set of security policies

✓ Adequate controls to enforce them

✓ Evidence of ongoing maintenance

- ☑ Firewalls
- ☑ Pen test reports
- ☑ User authentication and access controls
- ☑ Endpoint protection (on all endpoints)
- ☑ Encryption and multifactor authentication
- ☑ Backup and recovery systems
- ☑ Incident response and business continuity plans
- ☑ Documented employee security awareness training