Blockchain and the New Data Protection Law in California

General information only. Not legal advice.

Michelle Tsing, Esq.

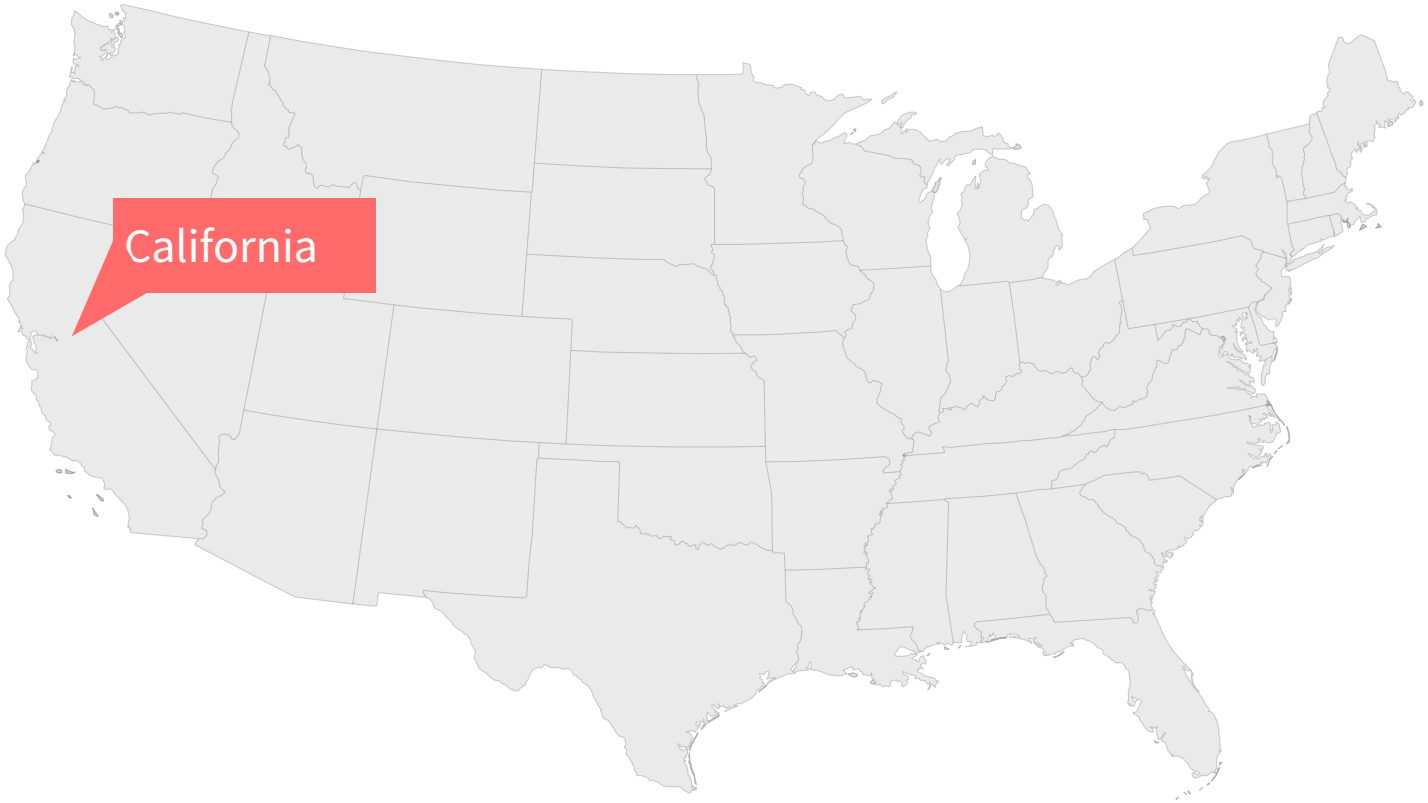
Michelle Tsing was an attorney at PayPal, where she helped the Large Merchant Services team achieved ubiquity. Prior to PayPal, she was at Cisco, eBay, Samsung and Apple.

She co-founded a blockchain payments startup in 2015 and is a strategic advisor to a number of AI, blockchain and 3D printing companies. She is also a mentor for Singularity University Ventures, Berkeley Blockchain Accelerator, SVI Academy and Hack Temple, which are tech incubators located in the United States.

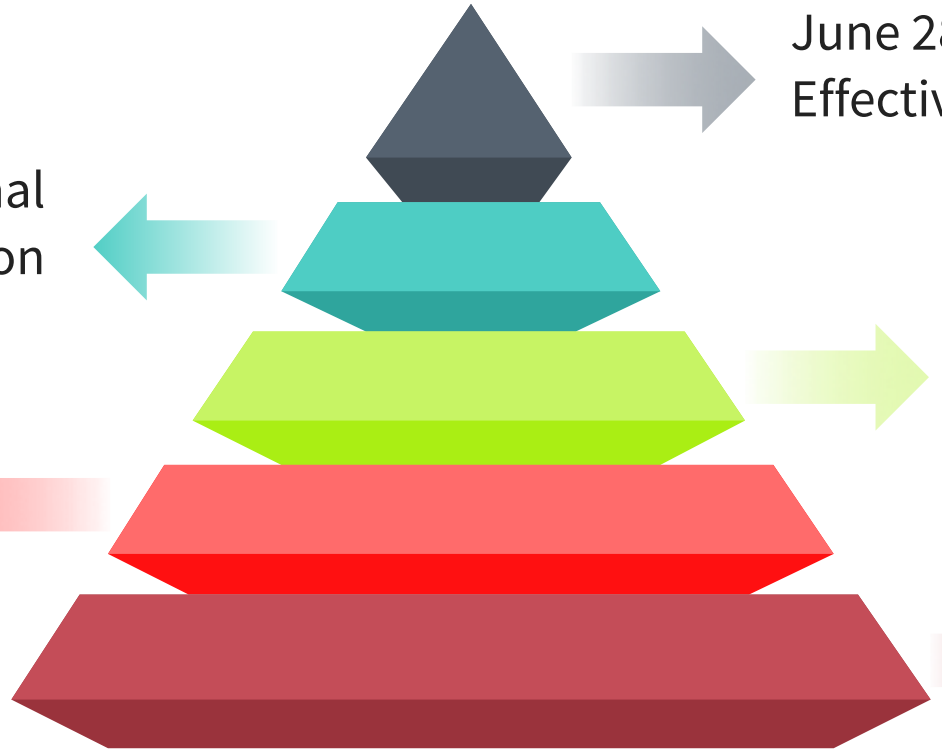
She founded Robotics for Good: Chatbots, Messaging and AI community; and had donated her time to both The Loving AI/XPRIZE Project and Robots Without Borders. She is a member of the California and Georgia blockchain advocacy coalitions. She is also producer and host of Laptop Radio at Stanford University.

California Consumer Privacy Act (CCPA)

California Consumer Privacy Act (CCPA)



CCPA - Applicability



June 28, 2018
Effective January 1, 2020

Collects personal information

Customers in California

Annual gross revenues over $25M; buys, receives, sells or shares personal information of 50K or more consumers; derives 50% or more revenues from sale of personal information

Online and Brick & Mortars

BUSINESS

CCPA

California based businesses with a revenue above $25M USD; or primary business is the sale of personal information

GDPR

All businesses that process data of EU citizens, regardless of revenue, location or size

BASIS

CCPA

Opt out

GDPR

Must have a legal basis

NOTICES

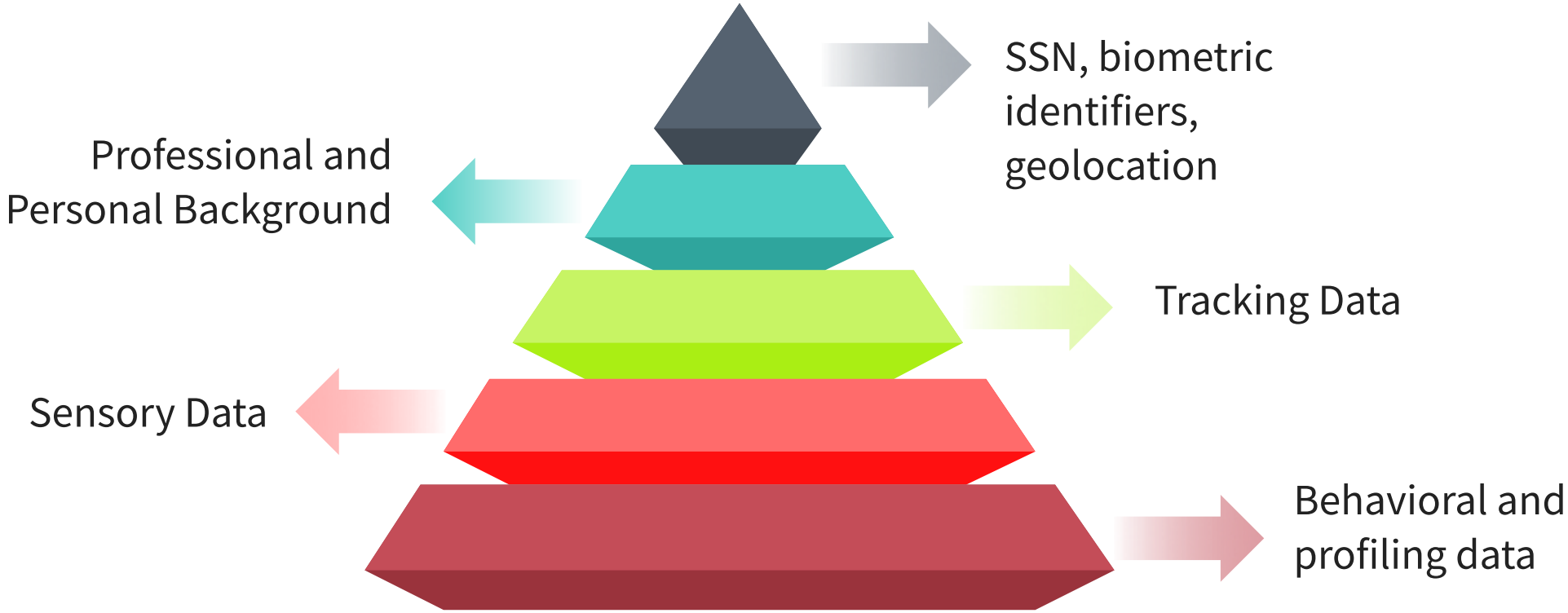
999.301(i) “Notice at collection” means the notice given by a business to a consumer at or before the time a business collects personal information from the consumer as required by Civil Code section 1798.100(b) and specified in these regulations.

NOTICES

999.305. Notice at Collection of Personal Information

(a) Purpose and General Principles (1) The purpose of the notice at collection is to inform consumers at or before the time of collection of a consumer's personal information of the categories of personal information to be collected from them and the purposes for which the categories of personal information will be used.

CCPA - Personal Information



DATA

CCPA

Focuses on consumer data, whereas “consumers” are California residents or people living in California for an extended period of time. Includes customers, households, devices, business to business transactions, employees and goods and services.

DATA

GDPR

Personal data is “information relating to an identified or identifiable natural person (data subject).”

P*seudonymous* data is data that has been processed in such a manner that it can no longer be attributed to a specific data subject without the use of additional information.

Sensitive data is data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning a natural person’s sex life or sexual orientation.

PERSONAL INFORMATION

CCPA

Social Security Numbers, biometric identifiers, geolocation information, etc.

Tracking data and unique identifiers including IP address, cookies, beacons, pixel tags, mobile ad identifiers, customer numbers, unique pseudonyms, “probabilistic identifiers” and other persistent identifiers

Behavioral and profiling data including browsing history, search history, purchasing history, purchasing tendencies, inferences drawn to create a profile reflecting preferences, characteristics, psychological trends, predispositions and attitudes.

PERSONAL INFORMATION

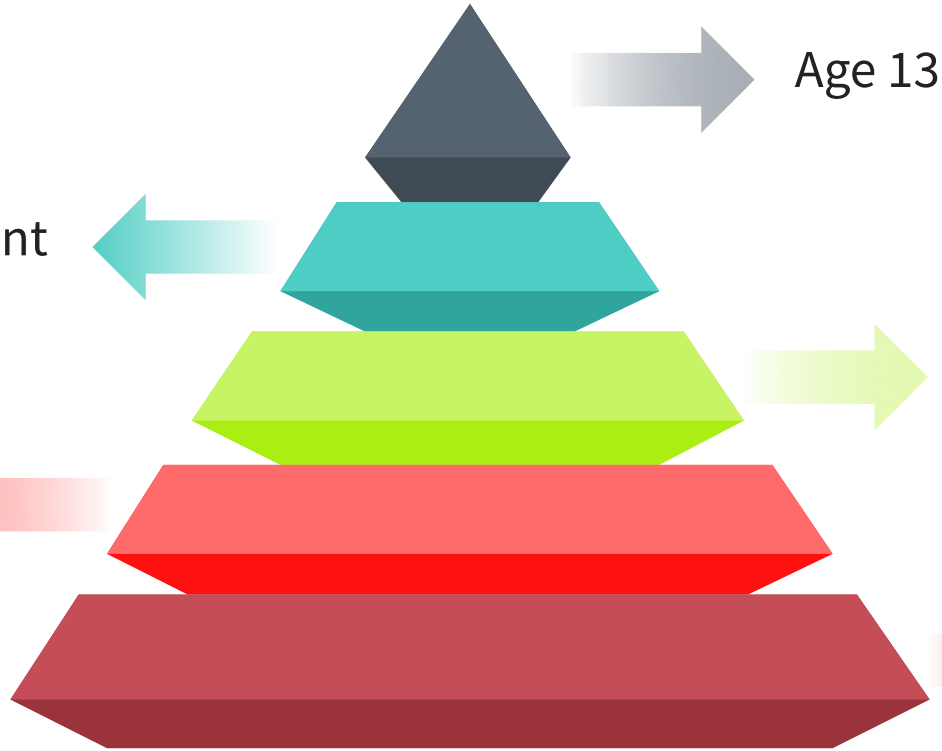
CCPA

Professional and personal background information including employment and education information that is not considered publicly available personally identifiable information under the Family Educational Rights and Privacy Act (FERPA) and “characteristics of protected classifications under California or federal law.”

Sensory data including “audio, electronic, visual, thermal, olfactory or similar information”

*Besides biometric data, no mention of health data.

CCPA - Children



Age 13-16

Consent

Parent's Consent is Required to Sell or Disclose Personal Information of a Child under 13 to 3rd Party

13-16 Years Old Have Right to Opt In

Tracking Technology - Knows Children Use the Websites

CHILDREN

CCPA

Children between 13 and 16 years of age must affirmatively authorize the sale of their personal information.

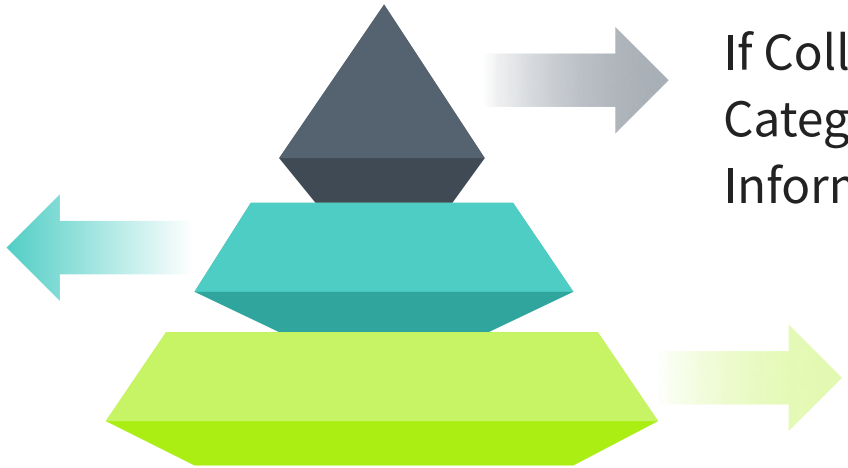
If the child is under the age of 13 years old, a parent or guardian must authorize the sale of information for them.

GDPR

Children under 16 needs to get parental consent for the processing of their personal information.

CCPA - Disclosure

If Purchases Third Party Data, Then Categories, Specific Personal Information, Origin, Purpose, Third Parties



If Collects Information, Then Categories and Specific Personal Information

If Sells or Discloses to Third Party, Then Personal Information Category Collected, Personal Information Category Sold, Categories of Third Parties, Personal Information Category Disclosed

SELLING

CCPA

1798.140(t)(1)

“Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.

SELLING

CCPA

A business does not “sell” personal information when

1. It shares the information with a service provider pursuant to a written contract that prohibits the service provider from retaining, using, or disclosing the personal information for any purpose other than the specific purpose of performing the services; and the service provider does not collect, sell or use the personal information beyond the scope of the services provided or

2. That information is transferred as an asset as part of a merger, acquisition or other change in control of a business provided that if a purchaser materially changes how it uses consumer personal information as a result of a merger & acquisition, then the purchaser must provide new notice of the changed practice to consumers.

SELLING

CCPA

A business does not “sell” personal information when

3. Consent

4. Personal Information is shared with third party to advise consumer is opting out of a sale

SELLING

CCPA

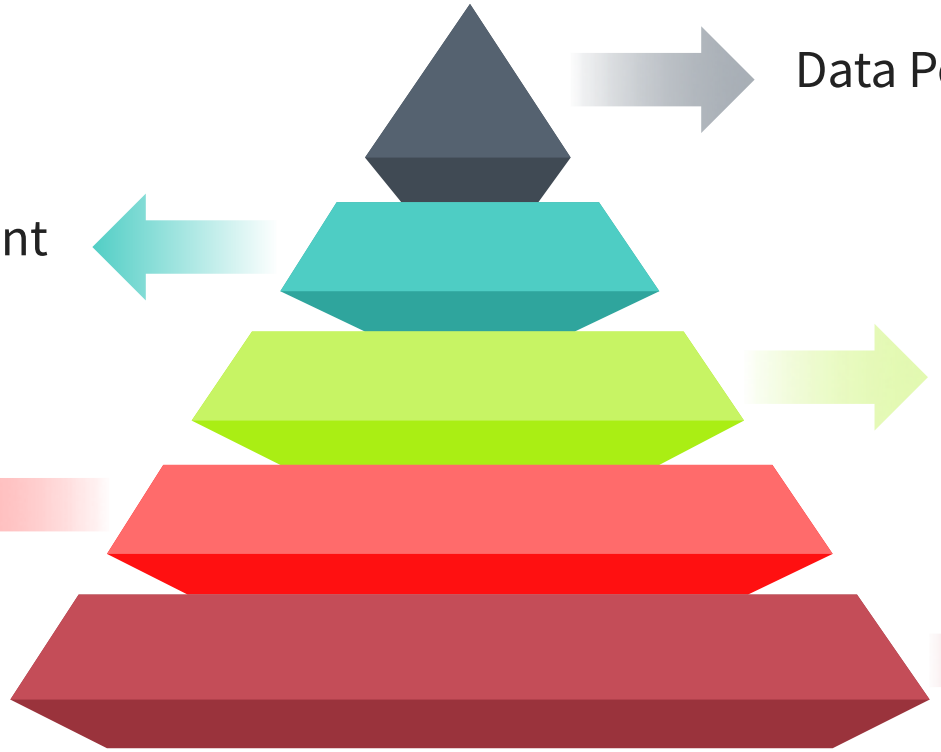
Consumers have the right to the following:

1. Request that a business disclose what categories of personal information it has collected, sold or disclosed for a business purpose;

2. Request that a business delete any personal information collected from the consumer; and

3. Opt out of the sale of the consumer's personal information.

CCPA - Access, Deletion & Third Party Transfers



Data Portability

Consent

Parent's Consent is Required to Sell or Disclose Personal Information of a Child under 13 to 3rd Party

13-16 Years Old Have Right to Opt In

Tracking Technology - Knows Children Use the Websites

RIGHT TO DELETE

CCPA

Applies to data that a business has collected from the consumer and not any data about the consumer that was collected from third parties.

Broad exceptions including legal obligations as well as internal lawful use and completion of a transaction.

RIGHT TO DELETE

GDPR

Right to inform other data controllers except when processing collides with freedom of expression and information, when processing is necessary to comply with a legal obligation, to support a public interest, for archiving or scientific, statistical, and historical purposes, or when it is necessary for establishing, exercising, or defending legal claims.

DATA PORTABILITY

CCPA

Not required to transfer personal information to another business on behalf of consumer.

GDPR

Right to receive pesonal data from data controllers in a commonly used machine-readable format.
Right to demand data be transmitted to another data controller.

RIGHT TO RECTIFY

CCPA

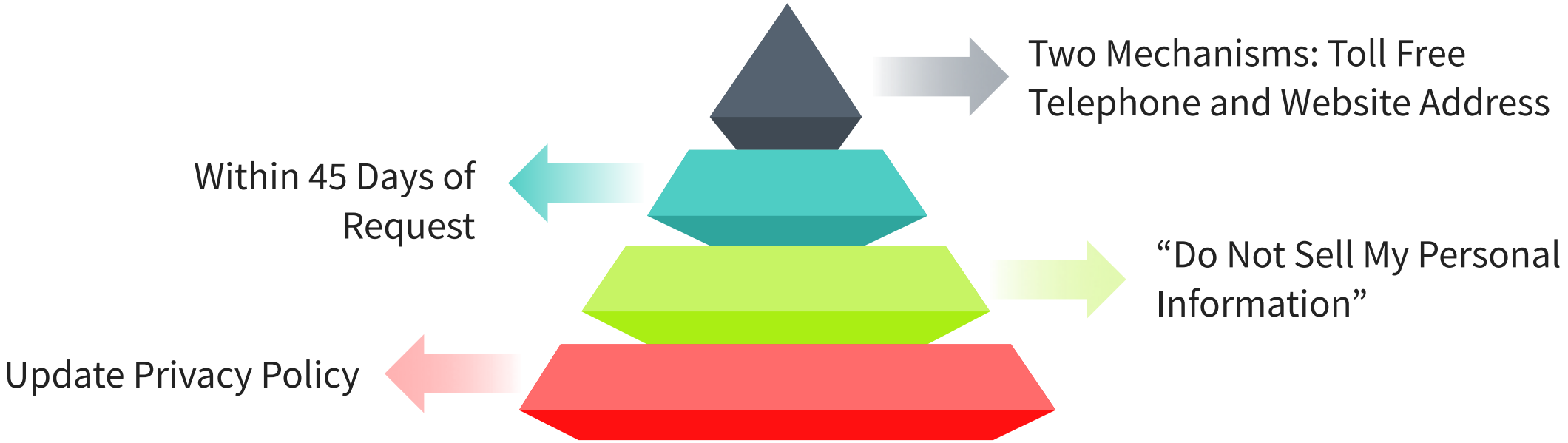
No specification.

GDPR

Right to correct inaccurate personal information or complete personal data.

Right to object the processing of personal data for purposes such as research, direct marketing or profiling.

CCPA - Compliance Mechanisms



REQUEST SUBMISSION

CCPA

Consumers may submit requests via toll free number and the business' website.

GDPR

No specification as to how consumers should be able to submit requests.

CONSUMER REQUESTS

CCPA

45 days upon receipt of request

GDPR

One to three months as long as the requesting party is notified.

Both: Reasons why the business cannot comply

OPT OUT RIGHTS

CCPA

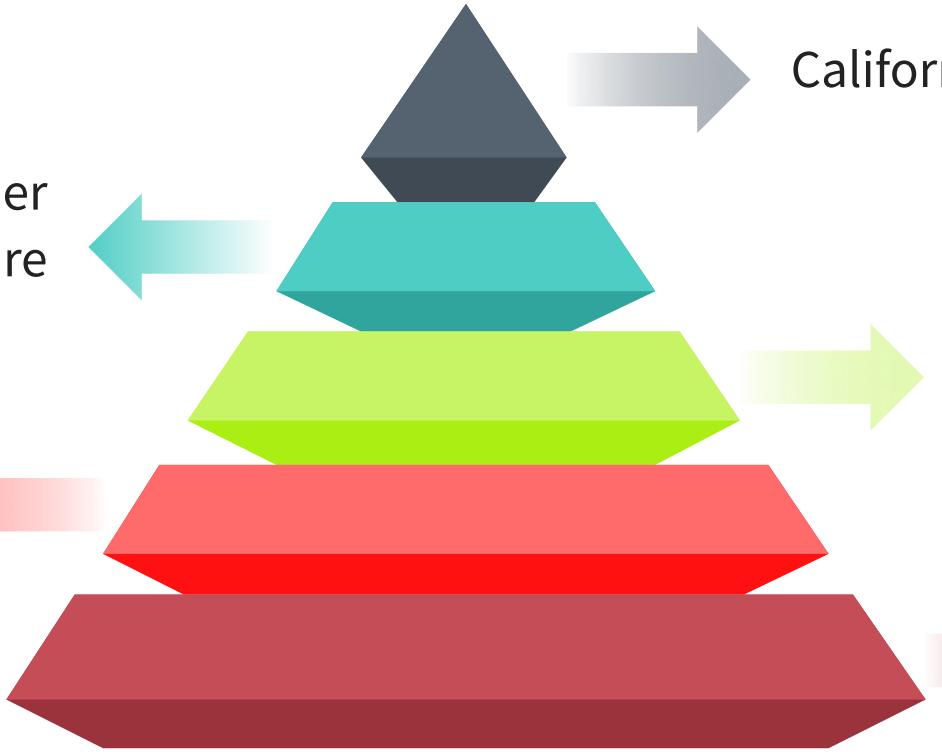
Businesses are required to create a conspicuous link on their homepage written “Do Not Sell My Personal Information.”

The business cannot request this authorization for at least 12 months after receiving the opt-out request.

GDPR

GDPR requires businesses to provide customers with a way to opt out of data collection for sales purposes.

CCPA - Enforcement



California Attorney General

Civil Penalties - up to $2,500 per violation after a 30 day cure

Civil Penalties - up to $7,500 for each intentional act

Civil Actions - Data Breach Because of Failure to Implement Security Measures

Civil Actions - Statutory Damages $100-$750 or actual damages, which is greater

DATA SECURITY

CCPA

Consumers has an option to sue businesses in the event of a data breach.

Consumers are entitled between $100-$750 in compensation per incident or actual damages, whichever is greater, if a company did not take reasonable security measures in the event of a breach of sensitive personal information.

DATA SECURITY

GDPR

Article 32 of GDPR on encryption to mitigate risks

PENALTIES FOR NON COMPLIANCE

CCPA

The California Attorney General may bring an action against a company and ask for $2,500 per violation and $7,500 for a willful violation.

Uncapped. A single incident affecting millions of California residents could result in a lawsuit that greatly exceeds $22M USD.

Applies at point of breach.

No sanctions for non-compliance.

30 day notice and cure period.

PENALTIES FOR NON COMPLIANCE

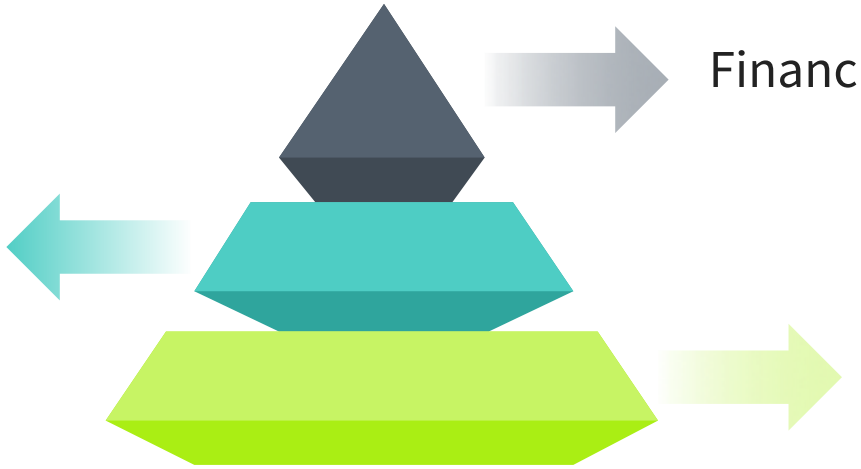
GDPR

Up to 4% of the business' annual global turnover or 20M Euros, whichever amont is greater.

Sanctions if business is at risk of a breach.

CCPA - Incentives & Discrimination

Financial incentives are acceptable



Different price, rate, level or quality of goods and services reasonably related to the value

Cannot discriminate by charging different price/ quality/services

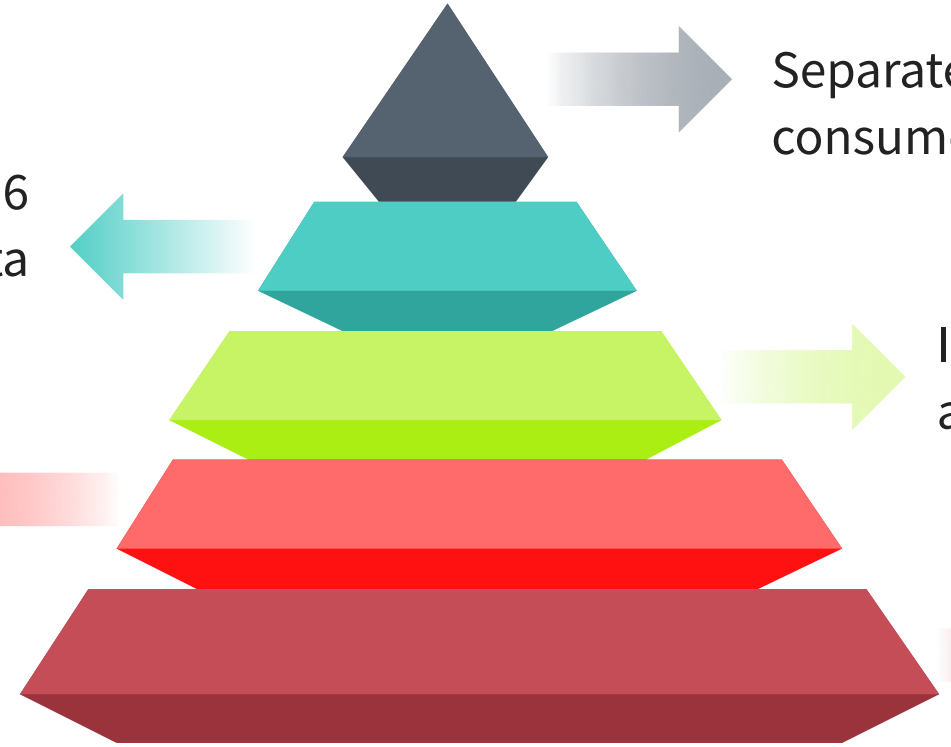
ANTI-DISCRIMINATION

Anti-discrimination:

CCPA

Businesses are not allowed to treat you any different whether or not you choose to opt-out.

CCPA - Best Practices



Separate home page for California consumers

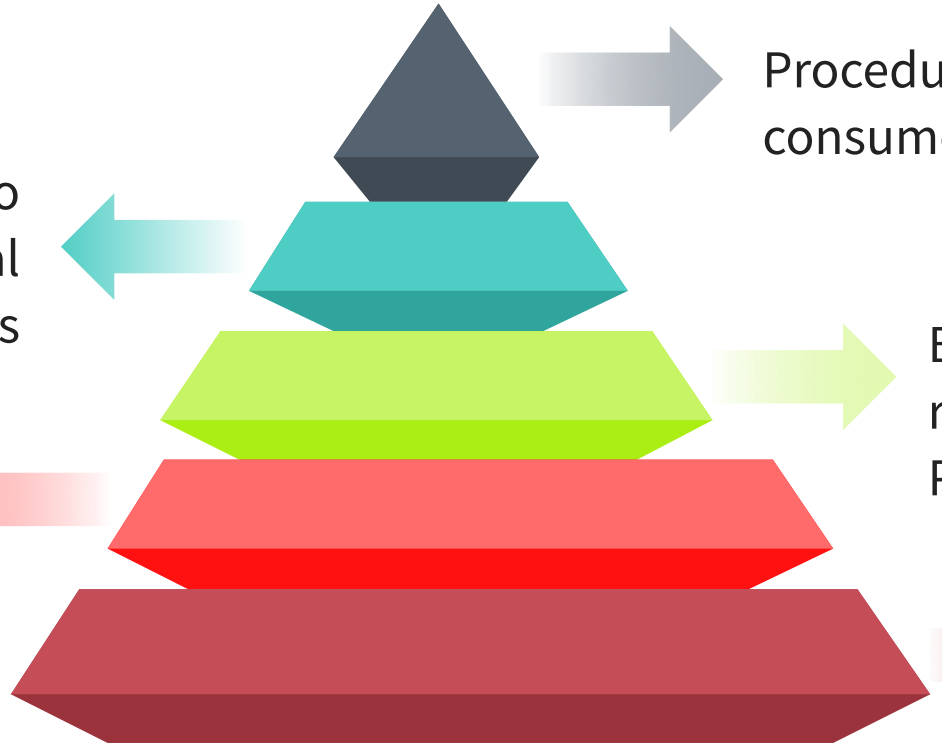
Consent from children 13-16 before cookies and pixel data

If opted out, disable cookies and pixel data

Review agreements with service providers to ensure use of personal information is restricted

Information from Employees, contractors and job candidates

CCPA - Best Practices



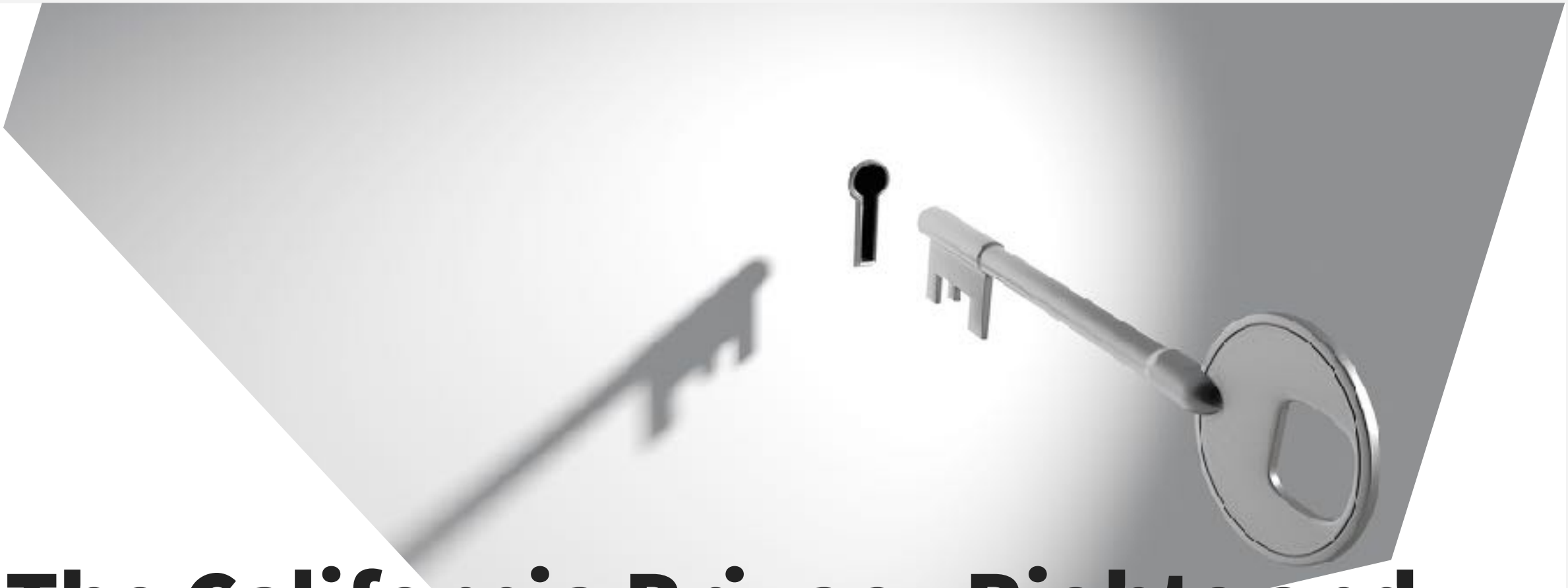
Procedures to prevent bad faith consumer requests

Terms with Service Providers to delete Consumer's Personal Information from their Records

Be conscious of any warranties regarding California Consumer Privacy Act

Develop a process to handle notices of violations

Have security measures in place to protect consumer's personal information



The California Privacy Rights and Enforcement Act (CPREA) - November 2020 election

CPREA

April 21, 2020 deadline for ballot measure petitions

Creation of California Privacy Protection Agency

Funding for 1,600 employees to enforce privacy protection and investigate abuses.

Allows state Attorney Generals to bring civil actions for violations.

Permits consumers to file suit for injunctive or declaratory relief and seek damages individually.

Gives nonprofits the right to bring class actions on behalf of their users.

CPREA

Security Requirements for Businesses:

Minimize the data they collect and employee and contractor access to such data.

Obtain consumer's explicit consent to disclose or sell the individual's personal information.

Have transparent privacy policies and consent processes.

CPREA

Privacy Rights:

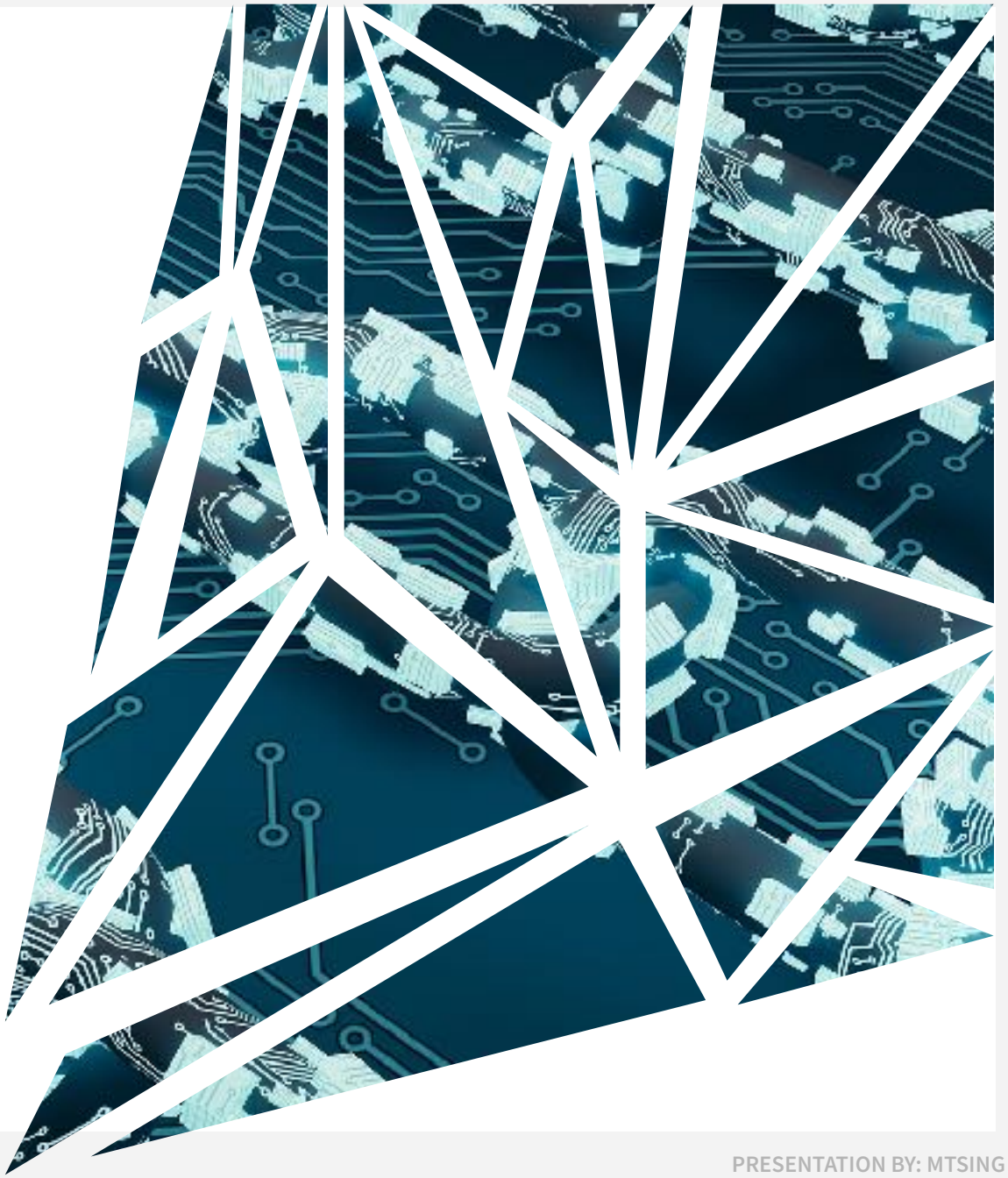
The right to access, correct, delete and port their personal information.

The right to be informed of any automated decisions that could have a significant privacy harm on the individual.

The right to request human review of such decision.

The right to provide express affirmative consent before personal information is used for behavioral personalization.

Blockchain



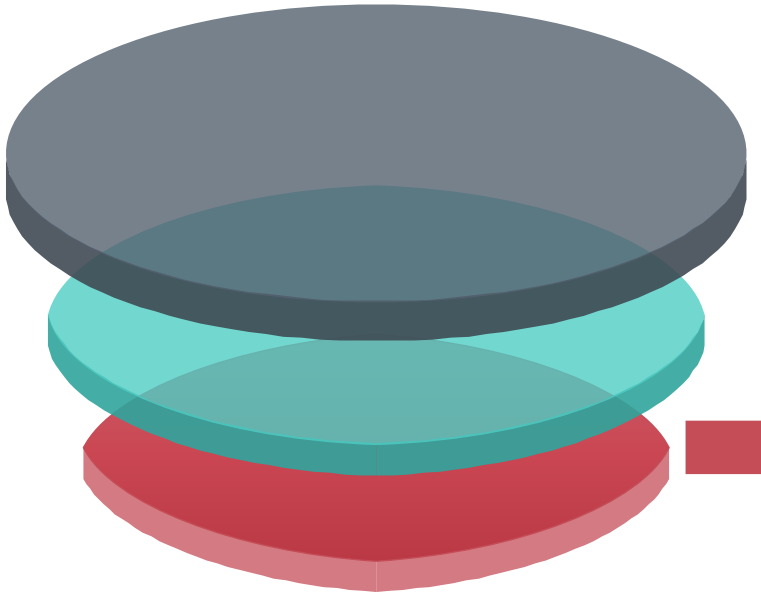
01. HASHES OF TRANSACTIONS OR GROUPS OF TRANSACTIONS

02. PUBLIC YET PRIVATE

03. IMMUTABLE RECORDS

04. VERIFIABLE BY PRIVATE KEYS

PCI Standards

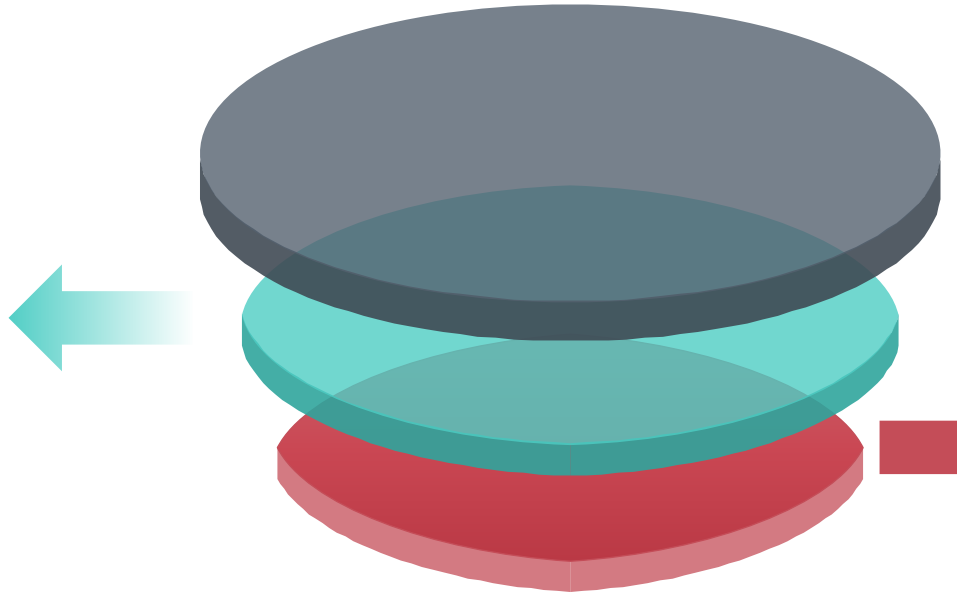


Secure Network: Firewalls and Passwords

Cardholder Data Storage and Transmisson

Software: Antivirus and other secure systems and applications

PCI Standards (continue)

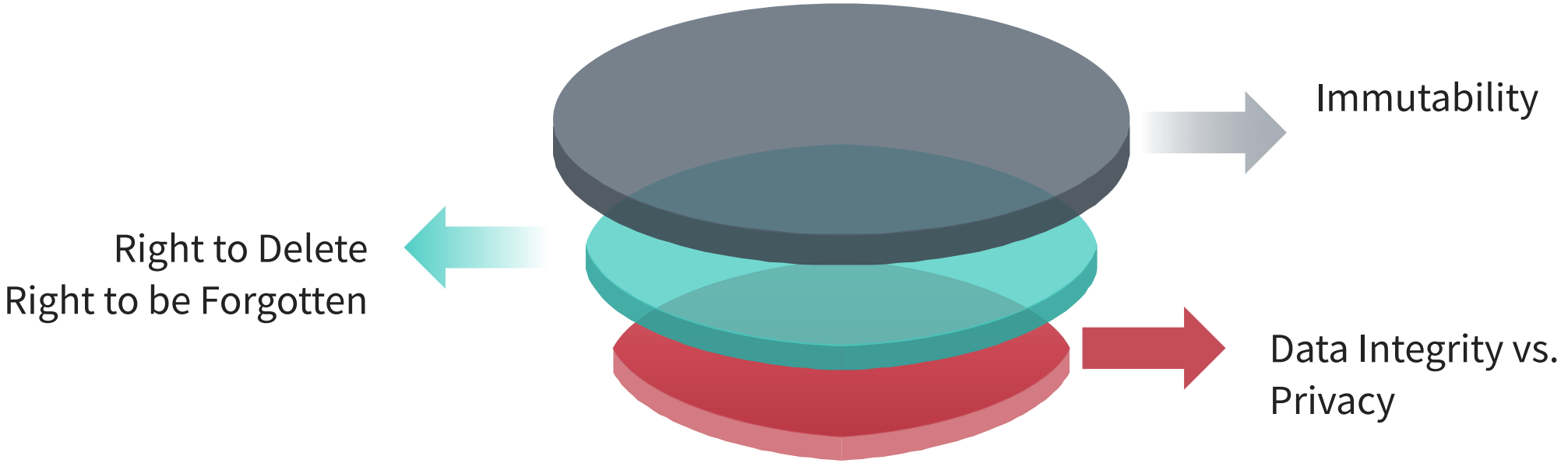


Assess control: Need to Know, Unique ID and Physical Access

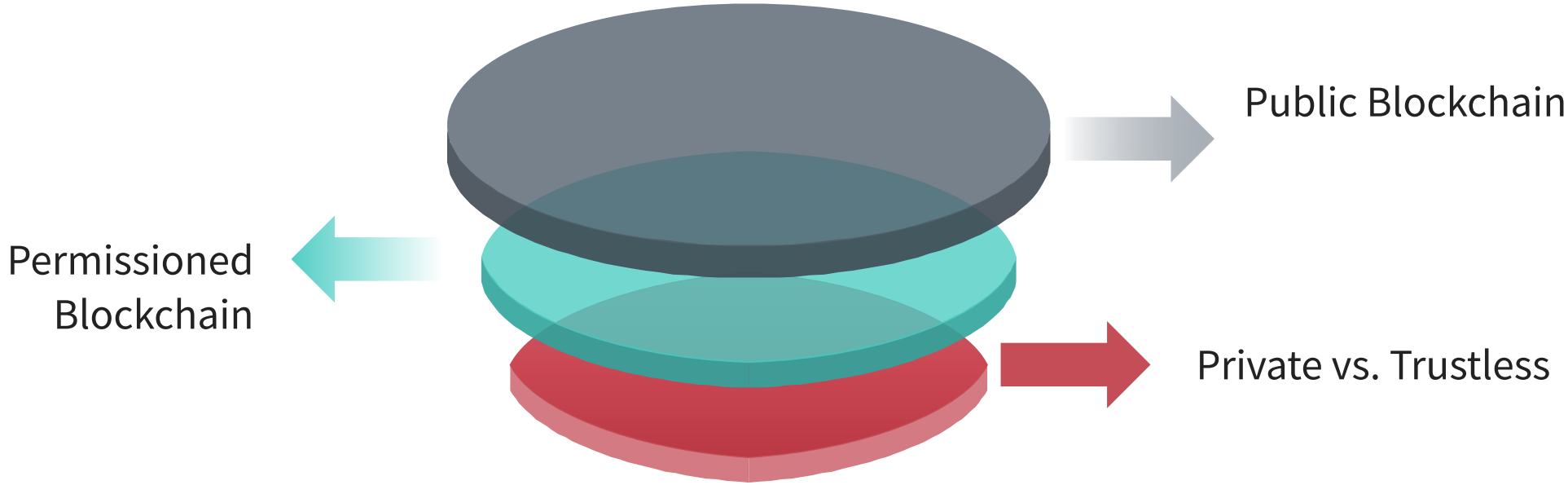
Monitoring and Testing: Network Resources and Security Systems and Processes

Information Security for Insiders

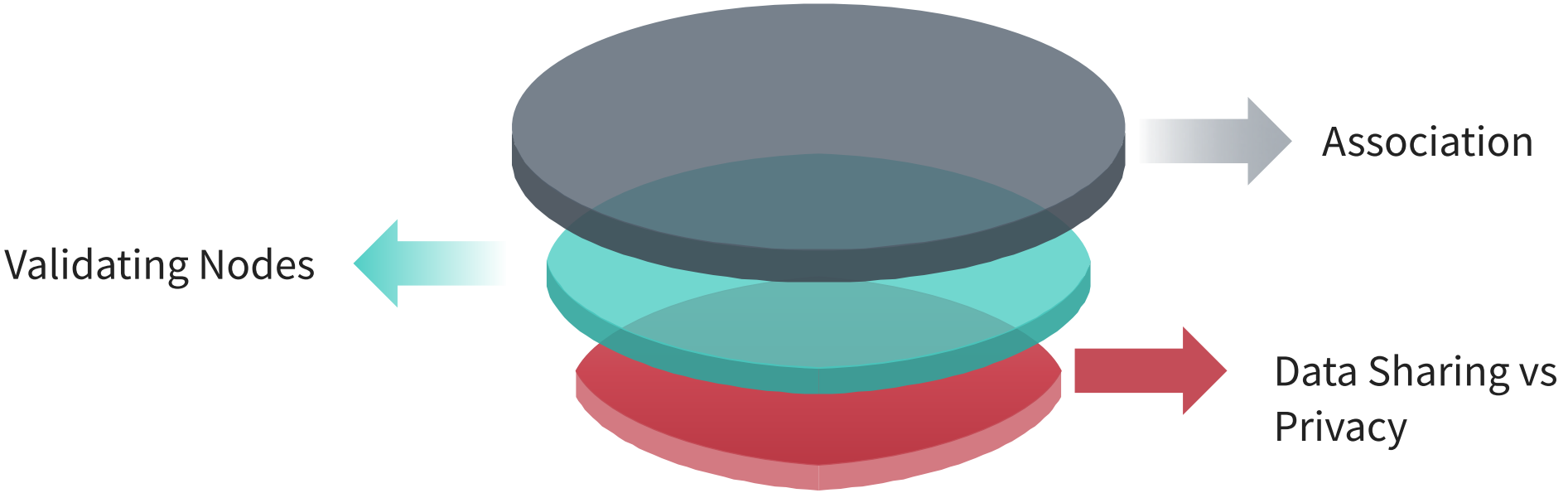
Blockchain, Data and Privacy: The Right to Delete vs. Immutability of Blockchain



Blockchain, Data and Privacy: Security



Blockchain, Data and Privacy: Data Sharing



Blockchain and the New Data Protection Law in California

Contact:
Michelle Tsing
email: mtsing@gmail.com
Twitter: @salutemichelle