Cybersecurity and Privacy: A Survey of the GDPR and CCPA

July 2019

Ari Schwartz | Venable LLP

Timothy Yim | Imperva

Adriana Beach | 23andMe

Shannon Yavorsky | Venable LLP

VENABLE LLP

Agenda

- Overview of the General Data Protection Regulation
- Overview of the California Consumer Privacy Act
- Comparison
- Hypos
- Questions

VENABLE LLP

GDPR - Overview

- Replaced the EU Data Protection Directive; became effective May 25, 2018
- Largest data protection fines ever imposed by the UK ICO in mid-July

VENABLE LLP

GDPR – Definitions

- **Personal data**—any information relating to an identified or identifiable natural person
  - **Identifiable person**—one who can be identified, directly or indirectly, by reference to an identifier including identification number, location data, or an online identifier. Online identifiers can include device identifiers, applications, tools and protocols (such as an IP address), cookie identifiers, or RFID tags.
- **Data Controller**: legal person; which, alone or jointly with others, determines the purposes and means of the processing of personal data
- **Data Processor**: legal person; which processes personal data on behalf of the controller

VENABLE LLP

GDPR - Territorial Scope

- The GDPR applies to EU based controllers and processors but also to non-EU based organizations
- Where no EU presence exists, the GDPR will still apply where: (1) an EU resident's personal data is processed in connection with goods/services offered to him/her; or (2) the behavior of individuals within the EU is "monitored"

VENABLE LLP

Penalties/Fines

Three tiers:

- Infringement of controller/processor obligations, certifications
  - 2% of worldwide turnover or €10M (whichever is higher)
- Infringement of basic principles of processing, data subjects' rights, international transfer
  - 4% of worldwide turnover or €20M (whichever is higher)
- Noncompliance with order of supervisory authority
  - 4% of worldwide turnover or €20M (whichever is higher)

VENABLE LLP

7 Data Protection Principles

1. Lawfulness, fairness, & transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity & confidentiality
7. Accountability

VENABLE LLP

GDPR - Core Concepts

- Lawful basis of processing
- Consent
- Transparency
- Individual Rights
- Privacy by Design
- Data Processing Agreements
- DPO/EU legal representative
- Cross Border Data Transfer
- Information security
- Data breach

VENABLE LLP

GDPR - Data Security

Article 32

- "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk"
- Linked to other concepts:
  - Pseudonymization/Anonymization
  - Data minimization
  - Privacy by Design

VENABLE LLP

GDPR - Data Breach

- Must report to regulator promptly and within 72 hours
- Controller must also report the breach to individuals unless:
  - Breach unlikely to affect their rights and freedoms
  - Controller had taken measures to protect the data e.g. encryption
  - Notification would involve disproportionate effort – if so, use public communication e.g., notice in newspaper, website announcement
- Processor must inform controller once aware of incident

VENABLE LLP

Background on CCPA

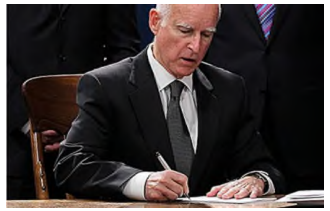
October 2017 – Ballot initiative submitted to the California Attorney General's Office by consumer advocates.

May 3, 2018 – Advocates announced the initiative had obtained enough signatures to go to voters.

June 21, 2018 – CCPA introduced to replace the ballot initiative.

June 28, 2018 – Governor Brown signs the CCPA into law.

September 23, 2018 – Governor Brown signs bill making limited amendments to CCPA.



VENABLE LLP

Scope of CCPA

Any company that does business in California and meets one or more of these standards:

- Annual gross revenue over $25 million
- Collects or shares personal information annually from 50,000 consumers, households, or devices
- Derives at least 50% of annual revenue from sale of personal information

Obligations and limitations extend to all **personal information** maintained about **consumers**.

- Consumer = any natural person who is a California resident
- Personal Information = information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with consumer or household

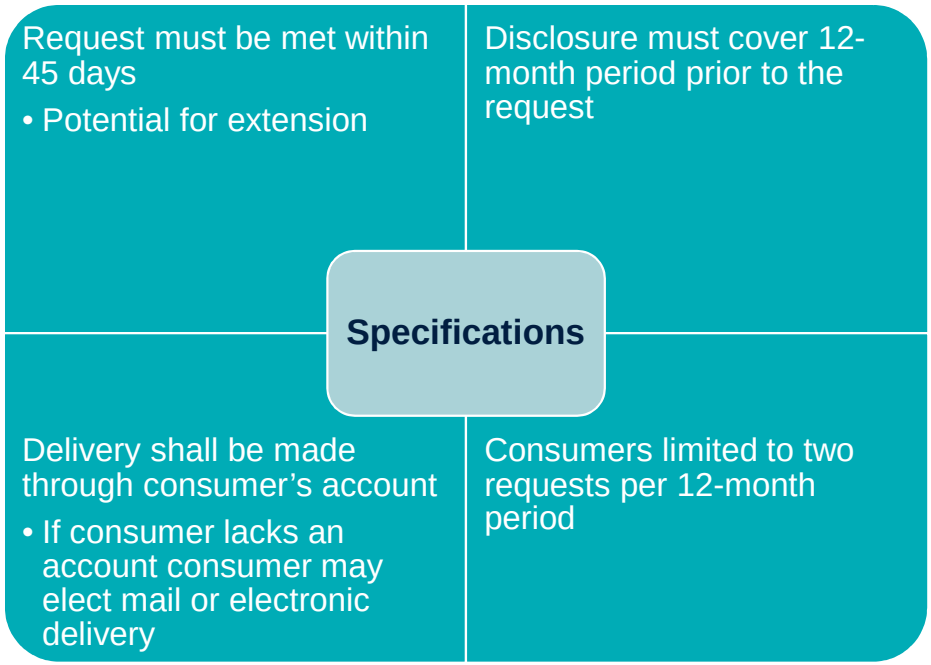
VENABLE LLP

Key Requirements

- Consumer right to request certain information about practices, and *specific pieces of personal information*
- Consumer right to request deletion of personal information, with some exceptions
- Consumer right to opt out of "sales" of personal information
- "Do Not Sell My Personal Information" link and webpage
- Business must not discriminate against consumers who exercise rights
- Implementation requirements
- Becomes effective January 1, 2020

VENABLE LLP

Requests for Information

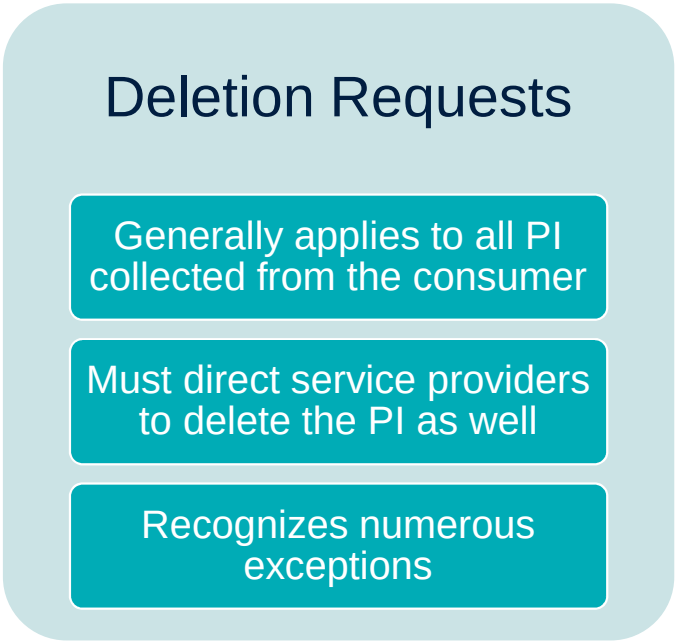


Considerations

- Third-party requests
- Security
- Verification
- Specificity of Response
- Extensions

VENABLE LLP

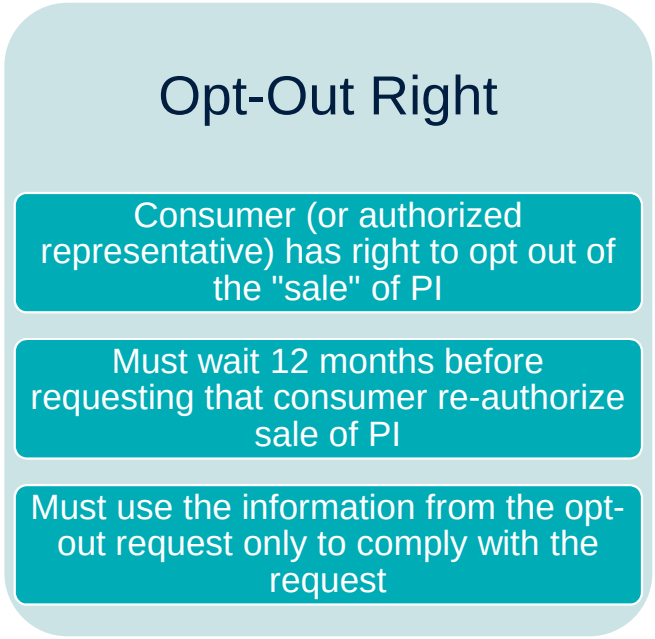
Deletion Rights



Considerations	Third-party requests
	Security
	Verification
	Exceptions
	Consumer regret

VENABLE LLP

Opt-Out for “Sales”



Considerations	Broad definition of "sale"
	Narrow exceptions, contract updates may be needed
	Consumer fraud

VENABLE LLP

Service Providers

Service Provider Definition

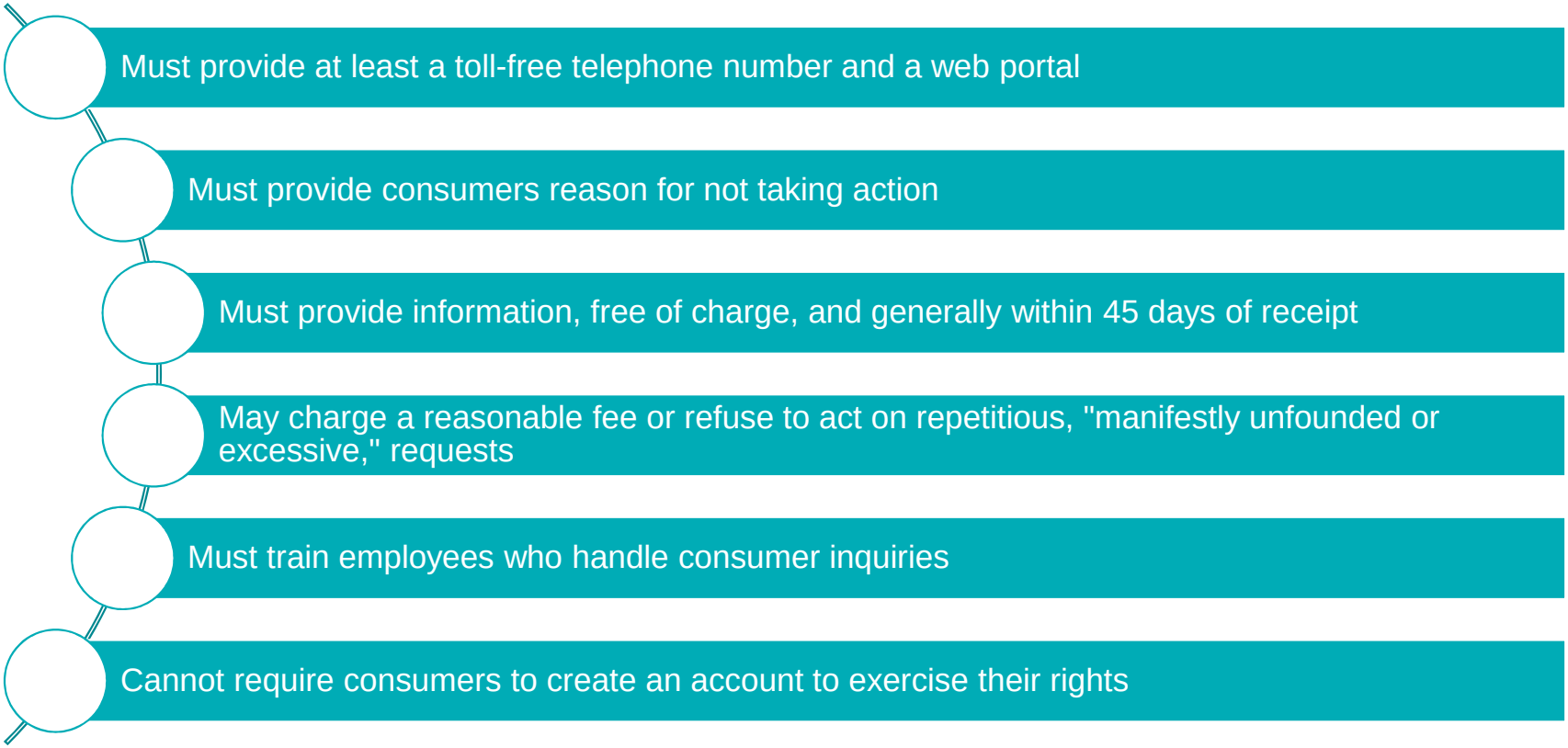
- Third parties receiving personal information are "service providers" **only if:**
  - The third party is processing personal information on your behalf for a business purpose
  - You and the third party have a written contract that prohibits the third party from retaining, using, or disclosing the personal information for any purpose other than performing the services or as otherwise permitted by the CCPA

Benefits

- Disclosures to service providers are not "sales" requiring an opt-out, if certain conditions are met
- You are generally not liable for CCPA violations by your service providers
- You must direct service providers to delete personal information when requested, but exemptions to deletion requirements apply to both you and your service providers

VENABLE LLP

Implementing Consumer Rights



VENABLE LLP

Non-discrimination

General prohibition on discriminating against consumers that exercise their CCPA rights

- Denying goods or services
- Charging different prices, including via benefits or penalties
- Providing a different level or quality
- Suggesting that the consumer will receive a different price or quality

Considerations	
	Incentives allowed
	Different price/service allowed if reasonably related to value
	Determining the value-incentive relationship

VENABLE LLP

Attorney General Enforcement

California Attorney General Enforcement

- Businesses have a 30-day cure period after being notified
- Can seek an injunction plus civil penalties of up to $2,500 per violation and up to $7,500 per intentional violation

Considerations

- No cap on civil penalties
- Attorney General is incentivized to seek enforcement – penalties and settlement proceeds placed in state fund

Rulemaking

- By July 1, 2020, the Attorney General will adopt regulations as directed by the CCPA
- Topics include rules and procedures for “sales” opt outs, verifiable consumer requests

VENABLE LLP

Private Right of Action

Encryption and redaction exception

Different definition of personal information for this section, limited to individual's first name/initial, plus last name, plus:

Social security number	**Driver's license or state identification card number**	**Financial account number, credit or debit card number in combination with access code**	**Medical information**	**Health insurance information**

VENABLE LLP

Amendments

- 18 bills across Assembly and Senate. At least 9 live in committee.
- AB-25 (employees x DSRs)
- AB-874 (scoping out publicly available PII)
- AB-1202 (data broker registry)
- AB-1564 (toll-free telephone for data subject request intake)

Regulations from Cal AG

- July 2020, private litigation, and 20 month look back.

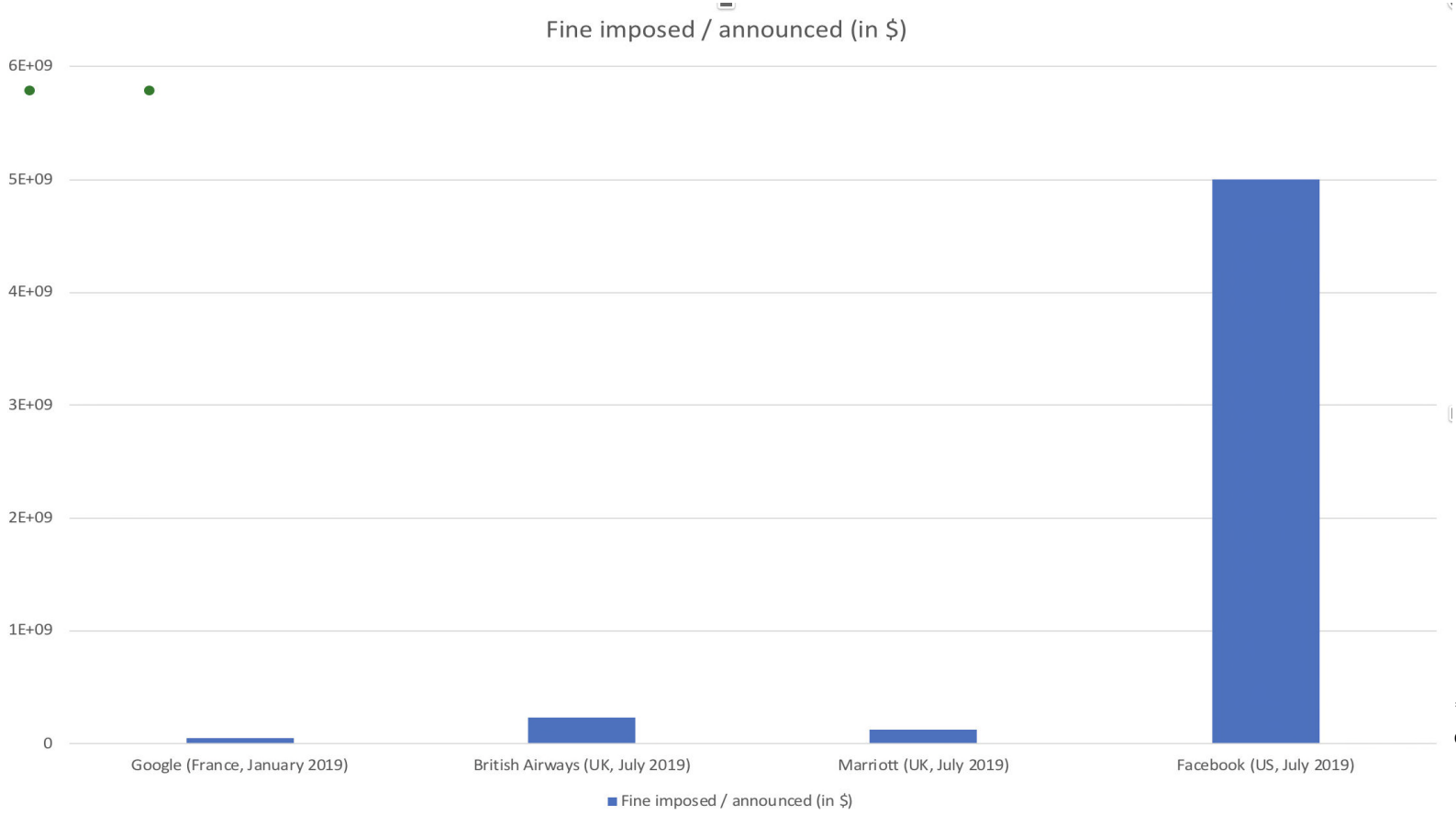
VENABLE LLP

Comparing CCPA to GDPR

- CCPA does not go as far as GDPR
  - CCPA does not require a lawful basis of processing
  - CCPA does not include terms in relation to cross border data transfer
  - CCPA does not require the appointment of a DPO or EU legal rep
  - CCPA does not require impact assessments
- Overlap
  - Individual rights
  - Contracts
  - Security

VENABLE LLP

Global Fines



* From one of my outside counsel, Phil Lee's LinkedIn

VENABLE LLP

Hypo Example #1

- You **have already** conducted a GDPR compliance exercise, what do you need to do for CCPA?

VENABLE LLP

Hypo Example #2

- You **have not** conducted a GDPR compliance exercise, what do you need to do for CCPA?

VENABLE LLP

Questions?

VENABLE LLP

Thank You

VENABLE LLP

VENABLE LLP