The New CCPA Regulations and What They Mean for Your Information Security Program

Scott M. Giordano, Esq., FIP, CISSP
V.P. and Sr. Counsel, Privacy and Compliance
Scott.Giordano@Spirion.com

February 26, 2020

Presenter

Scott Giordano, Esq., FIP, CISSP, VP, Data Protection

- Specializing in multinational/cross-border aspects of data protection
- Former ISO 17024 Certifications Advisory Board Member, International Association of Privacy Professionals
- Created and taught the first law school course on electronic evidence and -discovery
- Member of the California, the District of Columbia, and Washington state bar associations

If you leave with nothing else…

- The CCPA is in effect now; formal enforcement on July 1, 2020
- It's the most comprehensive U.S. state-level data protection law – likely a national standard
- Not a breach notification law
- It borrows many of the elements of the GDPR, such a InfoSec mandates
- Verifying requests for information or deletion will be your biggest challenge
- Understanding where personal information lies in your business and the risk of harm to it is key
- Items in red relate to InfoSec; items in light blue relate to risk

Information Security Under CCPA

“InfoSec” á1798.150(a)(1)

- “Any consumer whose nonencrypted or nonredacted personal information … is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the **business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information** to protect the personal information may institute a civil action for any of the following:
  - (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.”
- If plaintiff wishes to pursue statutory damages, must give 30 days’ notice so the defendant can “cure” the breach; otherwise, can go directly to court
- How do you “cure” a breach?

John A. Yanchunis (*Pro Hac Vice* Forthcoming)
jyanchunis@ForThe People.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Attorneys for Plaintiffs

Barnes v. Hanna Andersson, LLC, N.D. Cal., No. 20-cv-00812, complaint filed 2/3/20

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

BERNADETTE BARNES, an individual and California resident, on behalf of herself and all others similarly situated,

Plaintiff,

vs.

HANNA ANDERSSON, LLC, and SALESFORCE.COM, INC.

Case No.:

CLASS ACTION COMPLAINT

1.) Negligence

2.) Declaratory Relief

3.) Violation of the California Unfair

negligence and violates several California statutes.

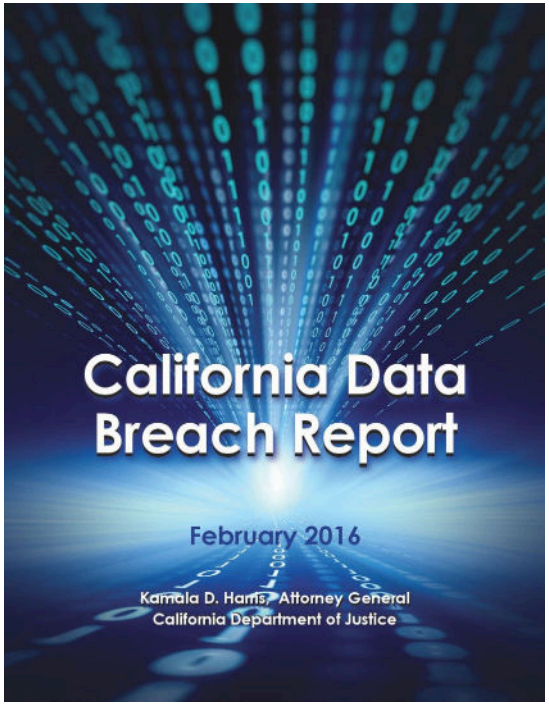
9. Plaintiff and similarly situated Hanna customers ("Class members") have suffered injury as a result of Defendants' conduct. These injuries may include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to lost time, (iv) deprivation of rights they possess under the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200) and California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq.*); (v) the continued and certainly an increased risk to their PII, which (a) remains available on the dark web for individuals to access and abuse, and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

CA Data Security and Breach Statutes

- **Security.** Under á1798.81.5(b), “A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”
- **Breach notification.** Under á1798.82(a), “A person or business that conducts business in California…shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California[.]…The disclosure shall be made in the most expedient time possible and without unreasonable delay[.]”
- Plaintiffs may bring civil action to recover damages

What are “reasonable” security procedures?

“The 20 controls in the Center for Internet Security’s Critical Security Controls [i.e., the CIS Top 20] identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.”



SPIRION

Consumer Rights and Security Under CCPA

Consumer Rights/Business Obligations Under CCPA

- Publish a notice of privacy practices
- Right to access (“Request to Know”) personal information
- Right to delete personal information
- Right of to be informed of personal information sold or disclosed
- Right to opt out of the sale of personal information
- Right to data portability
- Requirement to opt-in for children under age of 16

Consumer Rights/Business Obligations Under CCPA

- Publish a notice of privacy practices
- **Right to access (“Request to Know”) personal information**
- **Right to delete personal information**
- Right of to be informed of personal information sold or disclosed
- Right to opt out of the sale of personal information
- Right to data portability
- Requirement to opt-in for children under age of 16

Verification of Requests: Right to Access/Delete

SPIRION

Rights to access (“Right to Know”) personal information

Per CCPA áá1798.110 and 130, upon request, a business that holds personal information about a consumer must disclose within 45 days of a **verifiable consumer request**:

1. [what] the categories of personal information it has collected about that consumer;
2. [where] the categories of sources from which the personal information is collected;
3. [why] the business or commercial purpose for collecting or selling personal information;
4. [who] the categories of third parties with whom the business shares personal information; and
5. [what] the specific pieces of personal information it has collected about that consumer.

Rights to access (“Right to Know”) personal information - verification

- “Verifiable consumer request” means a **request that is made by a consumer**, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and **that the business can reasonably verify**, pursuant to regulations adopted by the Attorney General[.]
- **A business is not obligated** to provide information to the consumer…**if the business cannot verify**…that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf.

SPIRION

The CCPA Regulations and Verification

TEXT OF MODIFIED REGULATIONS

The original proposed language is in single underline. Changes are illustrated in red by double underline for proposed additions and by ~~strikeout~~ for proposed deletions.

TITLE 11. LAW

DIVISION 1. ATTORNEY GENERAL

CHAPTER 20. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

PROPOSED TEXT OF REGULATIONS

Article 1. General Provisions

§ 999.300. Title and Scope

(a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as "these regulations." These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.

(b) A violation of these regulations shall constitute a violation of the CCPA~~,~~ and be subject to the remedies provided for therein.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100-1798.199, Civil Code.

§ 999.301. Definitions

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

(a) "Affirmative authorization" means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a child under 13 years of age, it means that the parent or guardian has provided consent to the sale of the child's personal information in accordance with the methods set forth in section 999.330. For consumers 13 years and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

(b) "Attorney General" means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.

California Consumer Privacy Act Regulations Contents

Article 1. General Provisions

Article 2. Notices to Consumers

Article 3. Business Practices for Handling Consumer Requests

Article 4. Verification of Requests

Article 5. Special Rules Regarding Minors

Article 6. Non-Discrimination

Rights to access (“Right to Know”) personal information - verification

Article 4. Verification of Requests

§ 999.323. General Rules Regarding Verification

(a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information.

(b) In determining the method by which the business will verify the consumer’s identity, the business shall:

(1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.

Rights to access (“Right to Know”) personal information - verification

What’s a third-party identity verification service that complies with this section?

“Third-party identity verification service” means a security process offered by an independent third party who verifies the identity of the consumer making a request to the business.

Article 4. Verification of Requests

á 999.323. General Rules Regarding Verification

d). A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information.

Article 4. Verification of Requests

§ 999.324. Verification for Password-Protected Accounts

(a) If a business maintains a password-protected account with the consumer, the business **may verify the consumer's identity through the business's existing authentication** practices for the consumer's account….

(b) **If a business suspects fraudulent or malicious activity** on or from the password-protected account, **the business shall not comply** with a consumer's request to know or request to delete **until further verification procedures determine that the consumer request is authentic** ….

Article 4. Verification of Requests

§ 999.325. Verification for Non-Accountholders

a) If a consumer does not have or cannot access a password-protected account with the business, the business shall comply with [the following:]

b) A business's compliance with a request to know **categories** of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include **matching at least two data points provided by the consumer with data points maintained by the business**, ….

Article 4. Verification of Requests

§ 999.325. Verification for Non-Accountholders

c) A business's compliance with a request to know **specific pieces of personal information** requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may **include matching at least three pieces of personal information** provided by the consumer with personal information maintained by the business …**with a signed declaration under penalty of perjury** that the requestor is the consumer whose personal information is the subject of the request.

Article 4. Verification of Requests

§ 999.325. Verification for Non-Accountholders

d) A business's compliance with a **request to delete** may require that the business **verify the identity of the consumer to a reasonable degree or a reasonably high degree of certainty depending on the sensitivity** of the personal information and **the risk of harm** to the consumer posed by unauthorized deletion.

e) Illustrative scenarios follow [deleted]:

f) If there is **no reasonable method** by which a **business can verify** the identity of the consumer to the degree of certainty required by this section, the **business shall state so in response to any request** and, if this is the case for all consumers whose personal information the business holds, **in the business's privacy policy** [i.e., their privacy notice].

Article 4. Verification of Requests

In summary:

- As a business subject to CCPA, you must create a reasonable method for verifying that requestors are who they say they are
- When possible, leverage information about the requestor that you already have, and avoid collecting sensitive information such as SSNs, DL numbers, account numbers + passwords, and medically-related information
- Understanding the risk of harm for a given practice or action is crucial
- Develop and use reasonable security measures to detect fraudulent identity-verification activities

SPIRION

Next Steps

Your InfoSec Checklist – Complete by July 1

- Get Legal involved sooner rather than later
- Create (or update) your data inventory – there's more than you think
- Conduct your risk assessment(s) for the areas I've cited earlier in blue
- Review, update if necessary, and document your information security program and controls; assume it will be reviewed by a jury at some point
- Develop "reasonable methods" to verify a requestor and to deliver or delete the requested personal information
- Test extensively before going live
- Have a protocol to make sure that nothing falls through the cracks
- Work with Legal when preparing draft updates to your privacy statement – make sure not to state something you don't really do

Sample Data Inventory

Process Descriptions							
Nerve Center' Country (dropdown)	Business teams (dropdown)	Business process activity (e.g. recruiting, payroll calculations, payment processing, etc.)	Description, why activity is done (possible highlight if privacy notice or consent required)	Employees, Customers, Candidates, Suppliers (dropdown)	Types of Personal Data include name, address, date of birth, marital status	personal data type (Standard or Sensitive) - sensitive data type include standard personal data fields	Legal basis for processing
Country	Business Unit	Process flow name	Purpose of the processing	Category of Perso	List of data items	Data Type	Legal Basis
United States	IT	MDM Expert	Mobile Device Management (MDM). Mobile device management (MDM) is software that allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints. MDM is a core component of enterprise mobility management (EMM) which also includes mobile application management, identity and access management and enterprise file sync and share. The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise while simultaneously protecting the corporate network.	Employee	IMSI, IMEI, Device ID, ESN	Standard	Legitimate Interest
United States	IT	DLP Master	Data loss prevention; specifically, file centric actions - e.g., copying from a Word document to Yahoo mail or a USB drive. Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.	Employee	Equipment identifier (laptop, desktop ID or processor serial number), UserID, AD credentials	Standard	Legitimate Interest

Reproduced with permission from Robert Half Legal Consulting

SPIRION

On the Horizon: CCPA 2.0

On September 24, 2019 one of the sponsors of the original CCPA ballot initiative submitted a proposal for another initiative focused on data protection.

The *California Privacy Rights and Enforcement Act of 2020* ballot initiative would, among other things:

- create a new category of "sensitive personal information,"
- offer additional consumer rights, and
- create a dedicated state agency, the **California Privacy Protection Agency**, to protect consumer privacy.

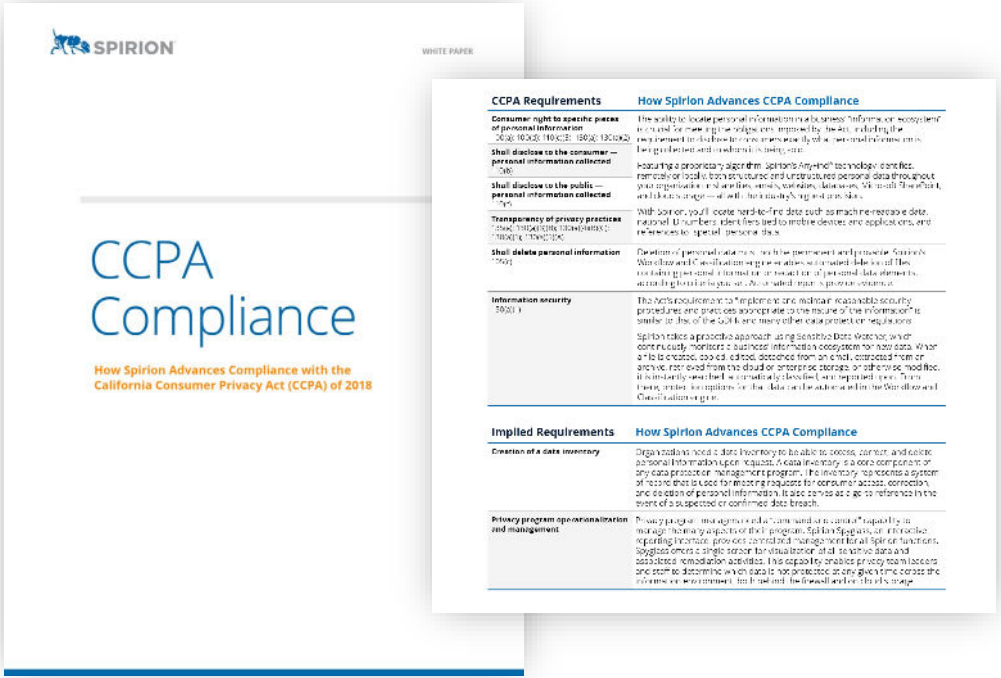
If approved, would be set in stone and a default national standard

Thank you!

Scott M. Giordano, Esq.
Scott.Giordano@Spirion.com

Learn more about how Spirion can help accelerate CCPA compliance through automated accurate data discovery, classification and monitoring.

Visit www.spirion.com



Appendix A: State Data Protection Laws Enforceable in 2020

Compliance Deadlines

State	Bill Number and/or Name	Compliance Mandate Area(s)	Enforcement Begins
California	S.B. 327, A.B. 1906	Internet of Things (IoT) security	January 1, 2020
California	A.B. 375, S.B. 1125	Comprehensive personal data privacy; security	January 1, 2020
Oregon	H.B. 2395	Internet of Things (IoT) security	January 1, 2020
Illinois	S.B. 1624	Breach notification	January 1, 2020
Oregon	S.B. 684	Personal information; breach notification for vendors	January 1, 2020
Texas	H.B. 4390	Breach notification	January 1, 2020

Compliance Deadlines

State	Bill Number and/or Name	Compliance Mandate Area(s)	Enforcement Begins
Washington state	H.B. 1071	Breach notification	March 1, 2020
New York	S. 5575-B, the SHIELD Act	Identify and protect “private information”; breach notification; secure disposal	March 21, 2020
Alabama	S.B. 54, the Insurance Data Security Law	Comprehensive written information security program	May 1, 2020

Compliance Deadlines

State	Bill Number and/or Name	Compliance Mandate Area(s)	Enforcement Begins
Maine	L.D. 946	Sales of personal information	July 1, 2020
Delaware	H.B. 174, Insurance Data Security Act	Comprehensive written information security program	July 31, 2020
Connecticut	the Insurance Data Security Law	Comprehensive written information security program	October 1, 2020
Michigan	H.B. 6491, the Insurance Data Security Law	Comprehensive written information security program	January 1, 2021
New Hampshire	S.B. 194, Insurance Data Security Law	Comprehensive written information security program	January 1, 2021

Summary of GDPR vs. CCPA: 3 Primary Differences

	GDPR	CCPA	Comments
Threshold for Becoming Subject/ Territorial Scope	• Applies to business, government bodies, and non-profits operating within the "four walls" of the EU • Also applies to those entities outside the EU that offer goods or services into the EU or study the behavior of EU data subjects. Art. 3(2).	Satisfies one or more of the following thresholds: A. (A) Has annual gross revenues in excess of $25M B. (B) Annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices. C. (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information. §1798.140(c)(1).	CCPA: • For-profit entities only • Unclear whether the $25M threshold is limited to business in California or applies to overall revenues. The California AG will decide.
Sale/Transfer of Personal Information – Right to Opt-Out	• Sale/transfer must have a "legal basis" such as consent of the data subject, contract, "legitimate interest" of the business, etc. If basis is consent, data subject could revoke it. Art. 6. • Right to opt out of marketing. Art. 21(2).	"A business that sells consumers' personal information to third parties shall provide notice to consumers…that this information may be sold and that consumers have the right to opt out of the sale of their personal information." §1798.120(b).	Under GDPR, there must be a legal basis for processing. In principle, if a data controller subject to GDPR uses a basis other than consent, it could sell/transfer the data to another party and the data subject could not stop it.
Right to Erasure/ Deletion	"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay[.]" Art. 17.	A consumer may request that personal information that "the business has collected from the consumer" be deleted. §1798.105	The CCPA has a long list of exceptions, some of which are very wide-ranging (e.g., "compatible with the context in which the consumer provided the information.")

GDPR vs. CCPA: InfoSec, IR, and BN

	GDPR	CCPA	Comments
Information Security	"[T]he controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk[.]" Art. 32(1).	Businesses have a "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information[.]" §1798.150(a).	CCPA's §150 almost identical to Civ. Code §1798.81.5(b), "shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."
Incident Response	GDPR does not use the phase "incident response," but cites the necessity to have "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident[.]" Art. 32(1)(c).	CCPA does not use the phase "incident response," but cites the option to "cure" a breach if a victim of the breach pursue statutory damages. §1798.150(b). However, what qualifies as a "cure" is not defined.	The proposed "CCPA 2.0" adds this to §150 of the CCPA: "The implementation and maintenance of reasonable security procedures and practices following a breach does not constitute a cure."
Breach Notification	• To Supervisory Authorities. "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it[.]" • To Data Subjects. "[T]he controller shall communicate the personal data breach to the data subject without undue delay."	CCPA is not, per se a breach notification statute. Under §1798.82(a), businesses "shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California[.]…The disclosure shall be made in the most expedient time possible and without unreasonable delay[.]"	The CCPA works side-by-side with the existing data security and data breach statutes, Civ. Code. §§1798.81.5 and 1798.82, respectively.