FEATURE

The California Consumer Privacy Act and Encryption

Theory, Practice, Risk Assessment and Risk Mitigation

The US State of California Consumer Privacy Act of 2018 (CCPA) will have an impact on security professionals, auditors, managers and boards responsible for ensuring its effective implementation. The act, which governs the disclosure of data and the sharing of California residents' personal information, became effective 1 January 2020.[1]

Provisions of the CCPA

The CCPA requires that an enterprise's privacy policy include the following four components:[2]

1. Information about selling users' information and how to opt out of that process
2. Methods of verifying the identity of the person who requests access, change or erasure of data
3. Methods for submitting such requests
4. An explanation of to whom the law applies

The CCPA also requires that an enterprise obtain the consent of minors (defined as individuals between the ages of 13 and 16 years of age) before selling their personal data. Individuals who are 13 to 16 years old can give consent themselves. For younger children, their parents or guardians must give prior consent.[3] There are fines for violation of the CCPA.

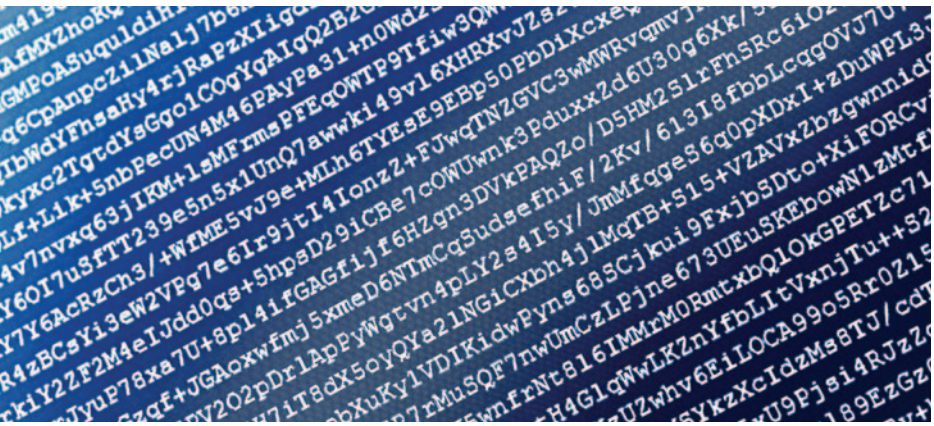
Fines under the CCPA will cap at $7,500 per violation—and even that maximum penalty is reserved for only intentional violations of the CCPA; violations lacking intent will remain subject to the preset $2,500 maximum fine under Section 17206 of the California Business and Professions Code. Of course, cumulative fines for large and systemic abuses may add up to be costly, but they are unlikely to be bank-breaking. [It also allows] persons to bring lawsuits for the breach of their "nonencrypted or nonredacted personal information"—even in the absence of evidence of actual damage. The CCPA allows individuals to recover between $100 and $750 per such incident—or greater in the showing of actual damages exceeding $750. Businesses have greater incentive to deploy encryption where they have not done so already—even for data that organizations have not traditionally encrypted.[4]

Applicability

The CCPA applies to every organization in the world if the following conditions are met:[5]

- It collects personal data of California residents.
- It (or its parent organization or a subsidiary) meets at least one of the following three thresholds:
  - Has annual gross revenue of at least US$25 million
  - Obtains personal information of at least 50,000 California residents, households and/or devices per year
  - Generates at least 50 percent of its annual revenue from selling California residents' personal information

Larry Marks, CISA, CRISC, CISM, CGEIT, CFE, CISSP, CRVPM II, ITIL, PMP
Is a senior manager of governance, risk and compliance at BDO. Prior to joining BDO, Marks was principal subject matter expert for technology and security, supporting the implementation of cyber and operational risk frameworks, ensuring regulatory compliance. He has led cyber/information security risk control self-assessment (RCSA) and programs/projects, while mentoring team and business to implement policies and procedures aligned with regulatory and compliance requirements. As a business advisor, he has also had responsibilities involving internal/IT audit, development, quality assurance/quality control and risk. Marks is a thought leader, publishing regularly on subjects related to security, risk, regulatory compliance, governance, leadership and program/project management.



GDPR Vs. CCPA Compliance

There is overlap between the CCPA and the EU General Data Protection Regulation (GDPR). However, under the CCPA, an enterprise must meet the following requirements:[6]

- Its home page must include a "Do Not Sell My Personal Information" link.
- It must establish methods for users to request access to, change of and erasure of data.
- It must establish a method for verifying the identity of the person making a data-related request.
- It must establish a method for obtaining consent from minors before selling their personal data.

Definition of Personal Data

The CCPA defines personal data as any information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household.[7] Unlike other personal privacy laws, the CCPA includes household information in the definition of personal data.

> "OF PARTICULAR CONCERN IS THE CCPA'S REQUIREMENT THAT ENTERPRISES DEMONSTRATE USE OF THE PROPER LEVEL OF ENCRYPTION TO MITIGATE THE RISK OF A DATA BREACH."

Personal information includes but is not limited to name, email address, biometric data, IP address, Internet of Things (IoT) information, geolocation data, and professional or employment information. Publicly available information is not considered personal information under the CCPA.

Encryption Requirements

Of particular concern is the CCPA's requirement that enterprises demonstrate use of the proper level of encryption to mitigate the risk of a data breach. Of what relevance is this provision to enterprises that are not doing business in California? These same requirements are delineated in the Federal Information Security Management Act (FISMA), a US law passed in 2002 that requires federal agencies to develop, document and implement information security and protection programs.[8] The required controls are covered in Federal Information Processing Standards (FIPS) 199 and 200 and the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800 series.

Encryption: SSL and TLS Protocols

The Secure Socket Layer (SSL) Protocol, the original encryption protocol used with HTTPS, evolved in three versions—SSL 1.0, SSL 2.0 and SSL 3.0—and has now been replaced by the Transport Layer Security (TLS) Protocol. It should be noted that Version 3.0 was redesigned to become TLS 1.0. TLS currently has the following versions: 1.0, 1.1, 1.2 and 1.3. TLS 1.0 and 1.1 are not allowed in PCI DS. Both protocols are part of Layer 4, Transport Security, of the Open Systems Interconnection (OSI) Model. (At this point, people are still more familiar with SSL, although TLS is increasingly being used within the industry. In the meantime, SSL/TLS is a common compromise and is used here.) SSL/TLS is used to secure electronic applications or functions. Applications incorporate the transport layer as part of their architecture, including secure coding and other best practices, to ensure a secure application. The transport layer is important because it controls the reliability of data through various processes such as segmentation/desegmentation and error control. The transport layer also provides the

acknowledgment response after successful data transmission and sends the next data if no errors have occurred. It creates segments out of the message received from the application layer.

However, "SSL/TLS by itself will not be the most secure protocol without using a level of IP security (IPsec) and key exchange."[9] This can be called "defense in depth." SSL/TLS is all about secure key exchange to ensure privacy controls over communications with a website. To connect securely with a website, one must exchange symmetric private keys that can be used to communicate. Specifically, a public/private key pair from the TLS cert is used to create a shared symmetric encryption key that is used to encrypt the session. SSL/TLS (and Public Key Infrastructure [PKI] in general, the trust model that facilitates public key encryption) is just a fancy mechanism for creating and exchanging those session keys. TLS establishes an encrypted, bidirectional network tunnel that allows arbitrary data to travel between two hosts. TLS is most often used in conjunction with other Internet protocols such as HTTPS, Secure Shell (SSH), secure File Transfer Protocol (FTPS) and secure email. **Figure 1** lists the differences between SSL and TLS.[10]

Mitigating Risk in the Implementation of SSL/TLS

Given CCPA and regulatory requirements to encrypt

Figure 1—SSL-TLS Comparison

Attribute	SSL	TLS
Cipher suite	Supports Fortezza (algorithm)	Does not support Fortezza
Cryptography secret	Uses message digest of pre-master secret to create master secret	Uses pseudorandom function to create master secret
Record protocol	Uses Message Authentication Code (MAC)	Uses Hashed MAC (HMAC)
Alert protocol	Includes the "No certificate" alert message	Eliminates alert description ("No certificate") and adds a dozen other values
Message authentication	*Ad hoc*	Includes availability of MAC algorithm suites such as HMAC–Secure Hash Algorithm (SHA)-256/384 and Authenticated Encryption with Associated Data (AEAD) in latest TLS versions
Key material authentication	*Ad hoc*	Pseudorandom function
Certificate verify	Complex	Simple
Finished	*Ad hoc*	Pseudorandom function
Implementation: key exchange and key derivation	Not applicable	1. Supports new authentication and key exchange algorithm suites such as Elliptic Curve Diffie-Hellman (ECDH), Rivest-Shamir-Adleman (RSA), ECDH-Elliptic Curve Digital Signature Algorithm (ECDSA), pre-shared key (PSK) and Secure Remote Password protocol (SRP) 2. Uses stronger encryption algorithms and has the ability to work on different ports 3. (TLS version 1.0) does not interoperate with SSL version 3.0
Vulnerabilities: general	Has a lot of bugs and is susceptible to known attacks	In latest TLS versions, most bugs have been fixed, making them immune to attacks. TLS 1.0 and 1.1 are no longer recommended for use.
Vulnerability: poodle attack	Is vulnerable, and in new versions of web browsers, is disabled by default	In all web browsers, is enabled by default

data—whether at rest, in transit or in motion—there are certain risk factors that must be assessed and mitigated. Encryption disguises the information itself using a mathematical formula (algorithm) known as a cipher. **Figure 2** lists some of the risk factors that should be addressed.[11]

Layered Encryption

Imagine that Internet traffic to and from a network occurs in layered pipelines. HTTPS is actually a set of protocols that help protect and secure sensitive information online. These are: FTP, Telnet and SMPT/IMAP4.

Auditing SSL/TLS

The audit program outlined in **figure 3** highlights the significant points of reference when reviewing controls over privacy and encryption as they relate to the CCPA.[12]

To ensure compliance with the provisions of the CCPA regarding privacy and encryption, best practices require a risk assessment of the corresponding controls and a mitigation plan that is documented and discussed with management for budgeting.

Figure 2—Risk Mitigation

Risk	Mitigation
Confusing certificates with protocols	Although many vendors use the phrase "SSL/TLS certificate," in reality, they are certificates for use with SSL and TLS. The protocols are determined by the server configuration, not by the certificates themselves.
Disabling SSL 2.0 and 3.0	Only TLS protocols should be enabled
Failing to protect sensitive data	A TLS certificate is required to establish a secure connection between a browser and a web server. Certificates have a key pair: a public key and a private key. These keys are used to create a shared symmetric key for the encrypted connection. Asymmetric keys are too slow. If deployed with standard industrywide security practices, the certificate can significantly increase the security of a secure server. The certificate commonly includes: • **Issuer**—The entity that verified the information and issued the certificate (Certificate Authority) • **Common name**—Name of the web server • **Valid to**—Expiration date, after which the certificate is no longer valid • Key size and hash cipher • **Signature algorithm**—Algorithm used to create the signature (keys) and prove its integrity
Expired, forged, untrusted certificate	• All certificates should be signed by a trusted Certificate Authority—either a reputable third-party Certificate Authority or a PKI that exists within the enterprise. With the latter, the Certificate Authority's root certificate must be installed in the trusted store of all connecting clients, which can be done through modification of the Windows Group Policy or Microsoft Management Console (MMC). Not all applications share the same trusted source. • A record or attestation of certificate validity periods is maintained and the renewal process is started 30 days before the certificate expires. Recommended validity periods are currently two years. • The certificate should work with any device or operating system that uses the X.509 digital certificate. • Ensure that the Configuration file contains the server name, Domain Name System (DNS) and common Name field (key identifier for the digital certificate). Perspective Risk, "Reduce Your Risks: SSL/TLS Certificate Weaknesses," *https://www.perspectiverisk.com/multiple-ssl-tls-certificate-weaknesses/*
Weak hashing algorithm attacks	All certificates signed using weak hashing algorithms such as SHA-1 and MD5 should be reissued and required to use the SHA-2 family of hashing algorithms (SHA-224, SHA-256, SHA-384, SHA-512).
Weak RSA key length attacks	Affected certificates in the chain with an RSA key length less than 2,048 bits should be replaced with a longer key, and any certificates signed by the old certificate should be reissued.
Improperly signed SSL certificates (failure to adhere to basic constraints or key usage extensions)	• The offending certificates' extensions should be altered and the certificates re-signed or reissued. • The X.509 digital certificate should be used at one end of the server end point.

Figure 3—Audit Program for Encryption, Privacy and Procedures	
Audit Step	**Technique**
Encryption	
Conduct an audit of SSL certificates in order.	Verify that there are no certificates using the enterprise's name anywhere on the Internet.
Maintain compliance with regulations through certificate audits.	Use of HTTPS and valid certificates by commercial enterprises that must comply with the GDPR to authenticate and encrypt communications. Continuous monitoring and situational awareness demonstrate that the transfer of personally identifiable information meets data protection requirements.
Deliver certificates.	The US Department of Homeland Security issued Emergency Directive 19-01 in response to a series of incidents involving DNS infrastructure tampering. This directive requires all government agencies to regularly deliver newly added certificates to the Certificate Transparency (CT) logs for agency domains. Although this directive is part of a standard DNS audit function, using certificate discovery to ensure that DNS and certificate footprints are in lockstep at all times is an important control that supports this effort. In addition, auditing and monitoring certificate footprints contribute to compliance with NIST Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations.
Before trying to implement Microsoft's new Internet Information Services (IIS) functionality to help identify weak TLS usage (added to Windows 2012 R2 and Windows 2016 in the July 2017 monthly rollup), make sure web servers are up-to-date.	Determine through a review policy which encryption algorithms are used for every web request to ensure that they comply with enterprise policy and standards.
Determine whether other applications use weak protocols.	Use Microsoft's System Center Operations Manager (SCOM) to detect legacy TLS Protocol usage. Nessus has many plug-ins for TLS certificate information such as weak protocols.
Determine whether the proper crypto is being used for each data type.	There are three main cryptographical types: 1. Hashing is generally defined as the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Because attackers can use different techniques such as "rainbow tables" (a unique salt approach devised for each password) before storing it in the database. 2. Symmetric encryption is used to store data such as bank account and credit card numbers. Asymmetric encryption is used to exchange secret data. 3. MAC is similar to hashing, except that it includes a secret key used to authenticate the message's integrity. MAC is generally used when data integrity is needed to ensure that the message cannot be changed in transit.
Privacy	
Ascertain whether sensitive (e.g., personal) data are stored in the database and which databases contain sensitive data.	Determine whether data elements are identified as to their sensitivity. Examples of sensitive data are user passwords, credit card information and Social Security numbers, customers' names, and addresses. In many countries, the combination of a person's name and address is considered private information and should be protected. Typically, when selling data to larger organizations or government departments, the enterprise must provide a list of sensitive data collected by the application and their data classifications and data tags. In the healthcare industry, patient records must be protected, as mandated in the United States by the Health Insurance Portability and Accountability Act (HIPAA) and in Canada by the Personal Information Protection and Electronic Documents Act (PIPEDA).
Ensure that the data classification complies with enterprise policy.	Review the enterprise's policy to determine the levels of data classification and determine the degree of compliance by speaking with data governance management.
Make sure that the proper crypto algorithm is being used.	• **Hashing**—SHA 256 is widely used. Anything less than SHA-512 is generally considered weak today. MD5 has been broken several times. When hashing is used to store passwords, they must be combined with a salt that is unique to each user. • **Encryption**—For symmetric encryption, Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3-DES) are considered secure. For key size, NIST Special Publication 800-57 has guidelines on minimum key sizes for each algorithm and how long this key size is viable. There are several well-respected asymmetric algorithms available; one of the most commonly used is RSA. • **MAC**—Use the same criteria as for hashing when choosing an algorithm. • **Key exchange**—Diffie-Hellman is most commonly used.
Determine whether data must be encrypted at rest, in transit and in motion.	Ascertain the enterprise's policy.

Figure 3—Audit Program for Encryption, Privacy and Procedures *(cont.)*	
Audit Step	**Technique**
Privacy *(cont.)*	
Ascertain whether access rules related to sensitive data have been defined and implemented using a risk-based approach.	Determine whether the access profiles are measured against the enterprise's risk framework.
Determine how data are stored when not in use.	Verify that the enterprise has a policy regarding data retention and its method of protection.
Determine how access to databases is controlled.	Verify that access to databases is granted based on user profile (role-based access control [RBAC]) or attributes (attribute-based access control [ABAC]).
Determine what mechanisms are used to transport data.	Interview personnel to determine the protocols used to transport data.
Determine whether detection tools such as Netflow are used to provide visibility into the network traffic and packet capture.	Interview personnel to determine how IT obtains visibility into the network traffic and packet capture. What tools are used?
Process and Procedures	
Ascertain whether the incident management and response process has been updated to capture the requirements of the CCPA.	Interview personnel to determine whether the incident management and response process includes CCPA requirements.
Determine whether this process has been tested recently to ensure compliance and whether the impact on the enterprise is clearly understood.	Implement a tabletop exercise testing a data breach of the CCPA.
Ascertain the governance process related to the implementation of rules and policy for sensitivity and privacy.	At a minimum, ensure periodic review (e.g., annually).

Conclusion

As the CCPA is implemented and enterprises review their controls to ensure compliance, they should also review their controls over encryption, data sensitivity and privacy to ensure compliance with the law and the protection of customer data using best practices. Enterprises should review the following:

- Implementation of HTTPS, SSL/TLS
- Access profiles
- Policies and standards regarding data privacy and encryption (and those standards should be evaluated against actual practice)

Of particular concern to enterprises is the requirement to demonstrate and validate compliance with CCPA's requirements. The areas mentioned will help to ensure that the CCPA's requirements, such as demonstrating the controls recommended or required by CCPA, are being implemented. This will also help organizations in their compliance review of the required controls covered in FIPS 199 and 200 and the NIST 800 series.

Endnotes

1 California Legislative Information, AB-375 Privacy: personal information: business. (2017–2018), 29 June 2018, *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375*

2 Secure Privacy, "Learn About the California Consumer Privacy Act (CCPA) and How to Become Compliant," *https://secureprivacy.ai/what-is-ccpa-and-how-to-become-compliant/#WhatisCCPA*
3 *Ibid*.
4 Stanganelli, J.; "California's CCPA Law: Why CISOs Need to Take Heed," *Security Now*, 26 July 2018, *https://www.securitynow.com/author.asp?section_id=706&doc_id=744859*
5 *Op cit* Secure Privacy
6 *Ibid*.
7 *Ibid*.
8 National Institute of Standards and Technology, "FISMA Implementation Project," USA, *https://csrc.nist.gov/projects/risk-management*
9 Oppliger, R.; *SSL and TLS: Theory and Practice, 2nd Edition*, Artech House, USA, 2016
10 DifferenceBetween, "Difference Between SSL and TLS," 29 December 2014, *https://www.differencebetween.com/difference-between-ssl-and-vs-tls/*
11 GlobalSign, "SSL vs. TLS—What's the Difference?" 7 July 2016, *https://www.globalsign.com/en/blog/ssl-vs-tls-difference/*
12 Koussa, S.; "How to Quickly Audit Your Cryptography Usage?" Software Secured, 21 July 2015, *https://www.softwaresecured.com/how-to-quickly-audit-your-cryptography-usage/*