Osterman Research

# WHITE PAPER

**White Paper** by Osterman Research
Published **December 2019**
Sponsored by **MessageSolution**

# Key Steps in Satisfying Your CCPA and Other Privacy Obligations

# Executive Summary

The California Consumer Privacy Act (CCPA) represents a major advancement in privacy rights for California residents – and a major set of obligations for companies that have customers in the state, regardless of where in the world they are located physically. The CCPA imposes a number of obligations on companies that process or control information on California residents, much like the General Data Protection Regulation (GDPR) did for companies with customers and prospects in the European Union.

The CCPA is part of a growing trend toward increasing privacy regulations being enacted worldwide, including Australia's new data breach notification law, India's Personal Data Protection Bill of 2018, and Brazil's new General Data Privacy Law 2018, among others. Add these to the already existing laws that address data privacy, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Children's Online Privacy Protection Act (COPPA), as well as a growing number of proposed laws that are similar in scope to the CCPA.

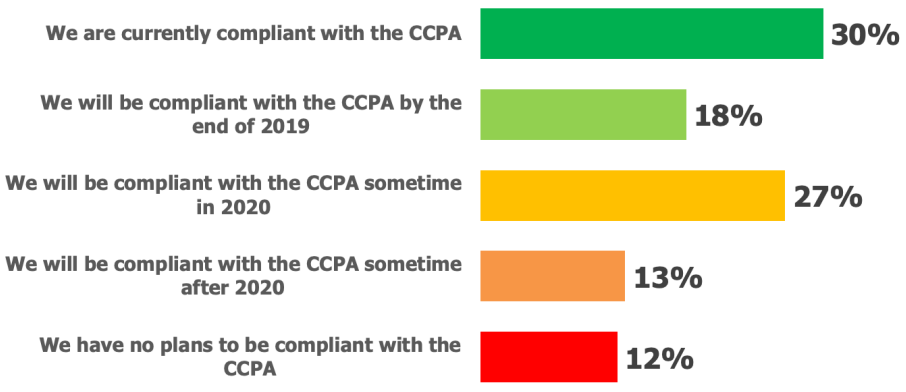
## KEY TAKEAWAYS

Here are the key takeaways discussed in this paper:

- Millions of businesses worldwide will be subject to the CCPA. Those subject to the law will be any company that has information about California residents and generates at least $25 million in annual revenue, those that have personal data on at least 50,000 California consumers, or any organization that generates more than 50 percent of its revenues from the sale of personal data.
- The CCPA may be more far-reaching than other privacy regulations like the GDPR and will require a different, albeit overlapping, set of capabilities to address properly.
- The majority of businesses in the United States are not yet compliant with the CCPA, as shown in Figure 1, despite the fact that the law goes into effect on January 1, 2020. For example, most do not consider their data protection practices to be mature, most senior business managers do not understand the importance of compliance with the CCPA, and nearly one-half of organizations have not yet allocated budget for the CCPA nor will they do so by the end of 2019.

***Millions of businesses worldwide will be subject to the CCPA.***

**Figure 1**
**Current and Planned CCPA Compliance**




*Source: Osterman Research, Inc.*

- To comply with the CCPA, organizations should implement a variety of best practices and deploy appropriate technologies to ensure that they can protect and access personal data. The CCPA has clear directives to help business decision makers decide on the right set of controls that need to be implemented.

### ABOUT THIS WHITE PAPER

This white paper was sponsored by MessageSolution; information about the company is provided at the end of this paper.

# Why is the CCPA Important?

### WHO IS SUBJECT TO THE CCPA?

The CCPA applies to a wide range of organizations:

- Any company that has information about California residents and generates at least $25 million in annual revenue, or
- Has personal data on 50,000 or more California consumers, or
- Generates more than one-half of its revenues from sales of personal data.

However, an amendment to the CCPA exempts "insurance institutions, agents and support organizations" because these organizations are already subject to the California Insurance Information and Privacy Protection Act. Some estimate that at least 500,000 businesses in the United States will be subject to CCPA, in addition to millions of businesses worldwide that also will be subject to it.

***The CCPA applies to any "natural person who is a California resident".***

### WHAT IS PERSONAL INFORMATION UNDER CCPA?

The CCPA applies to any "natural person who is a California resident". The law defines these residents' "personal information" as "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." It includes an individual's actual name; any aliases they may be using; postal addresses; unique personal identifiers; online identifiers; IP addresses; email addresses; account names; Social Security numbers; driver's license numbers; passport numbers; records of personal property; products or services that have been purchased, acquired or considered; consumption histories and tendencies; biometric information; browsing history; search history; any data related to their interaction with a website, application or advertisement; geolocation data; audio, electronic, visual, thermal, olfactory, or similar information; professional or employment-related information; non-public personally identifiable information as defined under the Family Educational Rights and Privacy Act; or inferences drawn from any of the information identified above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes [Section 1798.140].

### THE PENALTIES FOR NON-COMPLIANCE

If an organization is responsible for the breach of non-encrypted or non-redacted information about a California consumer, there are two penalties that can apply to the company that allowed the breach to occur:

- Each consumer whose data was breached may be entitled to recover damages of $100 to $750 or the actual damages from the breach, whichever is greater; injunctive or declaratory relief; or any other relief determined by a court [Section 1798.150(a)(1)(A-C)].

- The State of California Attorney General's office can also impose fines of $2,500 or $7,500, respectively, for each non-intentional or intentional violation of the CCPA.

## THE GROWING TREND TOWARD GREATER PRIVACY AND CONSUMERS RIGHTS OVER THEIR DATA

The CCPA represents part of the growing trend toward privacy regulation that is becoming more popular around the world. Perhaps the best-known of these regulations is the GDPR, but there are many others, including:

- The State of Colorado implemented the Colorado Protections for Consumer Data Privacy (CPCDP) in September 2018. The CPCDP requires companies that retain personal data (e.g., Social Security numbers, driver's license numbers, medical information, biometric data, credit card numbers, etc.) on Colorado residents to track this data and report any breaches of it within 30 days. In the event of a breach involving more than 500 Colorado residents, the breach must also be reported to the state's Attorney General's office.

- Australia recently introduced a data breach notification law that extended its existing data privacy legislation. Australia lacks a GDPR-type law at present, although some murmurs are starting to be heard about Australian's owning their online footprint and personal data, which could indicate a GDPR-type initiative will be forthcoming.

- Brazil's General Data Privacy Law 2018 (Lei Geral de Proteção de Dados Pessoais, LGPD), was signed into law in August 2018 and will go into effect in February 2020. LGPD includes many of the same privacy principles of the GDPR, it requires a legal basis for collection and processing, it applies in-country and extra-territorially, and it adopts the two percent of global revenue fine level (but not the four-percent one) of the GDPR. Data breach notifications are also required.

- India's Personal Data Protection Bill of 2018 is closely aligned with the GDPR, including rights for individuals, the tiers and scope of administrative fines, and the need for a legal basis for processing personal and sensitive personal data. Several differences also exist, such as the requirement for absolute data localization for "critical personal data," (although this phrase is not specifically defined) and that the State gets its own legal basis.

***The CCPA represents part of the growing trend toward privacy regulation that is becoming more popular around the world.***

## WHAT IS DRIVING PRIVACY LEGISLATION?

The key issue driving privacy legislation is the growing number of data breaches. The extremely large data breaches over the past several years – such as those from Yahoo!, Marriott International, British Airways, Equifax, Target et al – have angered many people, and so their legislators and others in government have responded by enacting privacy legislation with varying degrees of penalties associated with a breach of personal data. It is also important to note that the GDPR has served as an impetus for many governments around the world to enact their own privacy legislation and California has followed suit.

Is privacy good for business? While compliance is definitely a painful process for organizations that don't have their information governance house in order, there are some benefits that organizations can realize from implementing a program to comply with the CCPA: they can avoid reputational damage by implementing solutions designed to protect sensitive and confidential data, they can increase revenue by building loyalty among customers who believe their data will be protected, they can gain operational efficiencies through legacy data cleansing, and safe data exposure enables value creation across the enterprise.

## WHY THE CCPA?

The State of California has a history of supporting privacy rights. For example, in 1972 the majority of the state's voters voted to amend the state constitution to make privacy an "inalienable" right. The state has also passed other privacy legislation over the years, such as the Privacy Rights for California Minors in the Digital World Act, and the Online Privacy Protection Act.

Interestingly, the CCPA actually represents something of a compromise. A privacy initiative was to be brought to a public vote of California residents, but legislators feared that this plaintiff-friendly initiative went too far, and so enacted the CCPA to entice the authors of the initiative to withdraw their push for a public vote. However, the authors of the original initiative that was withdrawn have proposed a new bill, the California Privacy Rights and Enforcement Act of 2020[i], that would dramatically strengthen the provisions of the current CCPA. The new legislation would create the California Privacy Protection Agency, add a new category of personal information to the CCPA, and otherwise significantly amend the current legislation.

While there is significant overlap conceptually between the CCPA and the GDPR, there are some important differences between these regulations. For example:

- The CCPA applies to consumers, which are defined as customers of virtually any household good or service, B2B transactions and employees; whereas the GDPR applies to "data subjects", which is essentially any resident of a European Union country.
- The CCPA does not explicitly call out data security, whereas the GDPR requires any data controller or processor to implement appropriate technical safeguards.
- The CCPA specifically calls out consumers' right not to have their data sold (and requires web sites to include a "do not sell my data" option), whereas the GDPR does not include a provision about data sales.
- The CCPA does not include a consumer right to rectification of data, whereas the GDPR does.

***While is there significant overlap conceptually between the CCPA and the GDPR, there are some important differences between these regulations.***

## WHY IS THE CCPA IMPORTANT?

The CCPA is important for a couple of reasons:

- As of 2018, California's population represented 12.1 percent of the US population, making the state's consumer economy a vital element of virtually any online business and any organization that has even one customer in the state.
- California's economy had a GDP of $3.0 trillion in 2018, making it the fifth largest economy in the world.

In short, California's economy is essential to the world economy, and so what the government of the State of California does – whether good or bad – has an impact on most other economies. Underscoring that is the fact that Microsoft will adhere to the requirements of the CCPA across the United States, not just in California[ii].

## SUBJECT ACCESS REQUESTS

Similar to the GDPR, the CCPA also includes provisions akin to the Subject Access Request of the GDPR:

- A consumer has the right to request that a business that collects his or her personal information disclose to that consumer the categories and specific pieces of personal information the business has collected [Section 1798.100(a)].
- A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver,

free of charge to the consumer, the personal information required under the CCPA [Section 1798.100(d)].

## WILL THE CCPA BE MORE IMPACTFUL THAN MANY REALIZE?

Many laws, particularly those that are written as a knee-jerk reaction to a problem or those that are drafted in haste (as was the case with the CCPA, which was deliberated over a period of just seven days), have unintended consequences. Will that be the case with the CCPA? Given that the law has not yet come into force it's hard to say, but there certainly is the potential for this to happen. For example[iii]:

- The CCPA includes "household" information as part of an individual's personal information, and so an individual exercising his or her right of data deletion under CCPA potentially has the right to delete the information of others in his or her household without their consent.

- Because the CCPA does not enable a provider to discriminate against those who opt out of the provider's data gathering, providers could be required to offer the same level of service while getting nothing in return. For example, a company that offers a white paper (such as this one) would potentially not be permitted to prevent a California consumer from downloading that paper if they refused to provide any information about their identity. This could prompt many providers to drop free services.

- The CCPA applies not only to a business that collects personal information, but also to any entity that is owned in common with that business, a parent company or any subsidiaries. Consequently, a company can become obligated under the CCPA even if it has no personal information on a California consumer. This may raise serious issues under the US Constitution and other laws around the globe.

***The CCPA applies not only to a business that collects personal information, but also to any entity that is owned in common with that business.***

## WHAT ARE THE IMPLICATIONS FOR US AND NON-US COMPANIES?

At a high level, the implications of the CCPA are not dissimilar to those of the GDPR: potentially, organizations around the world will be obligated to comply with the laws of a government in which they have no operations, no staff and no affiliation or representation other than a consumer relationship. What remains to be seen is the reach that the State of California may (or may not) have on organizations outside of the state. For example, all of the publicly available fines and penalties[iv] that have been issued under GDPR have applied solely to European companies, despite the fact that any company with data on residents of the European Union are obligated under GDPR. That's not to say that the European Union will not at some point levy fines or other GDPR penalties to organizations outside of Europe, but it is noteworthy that as of the writing of this paper (18 months after the GDPR went into effect) that has yet to happen.

## THE IMPLICATIONS FOR PRIVACY AT THE FEDERAL LEVEL

California has traditionally been at the forefront of US states in passing privacy and other types of legislation. For example, California was the first US state to pass a data breach notification law, which went into effect on July 1, 2003. Over the course of the next 15 years, all 50 US states passed similar types of legislation (Alabama was the 50th state to enact such a law, which went into effect on June 1, 2018).

What will be the impact of California passing the CCPA? If history is any indicator, it's likely that many other states will follow suit and will pass their own CCPA-like privacy regulations over the next decade or so, creating a somewhat confusing mix of regulations with a variety of different requirements with which businesses will have to contend. Potentially, it would be easier for businesses to comply with a single, national law along the lines of the CCPA or the GDPR, but Osterman Research believes that's unlikely to happen anytime soon. For example, the 115th Congress (which ran from January 3, 2017 to January 3, 2019) passed 442 new laws. Given

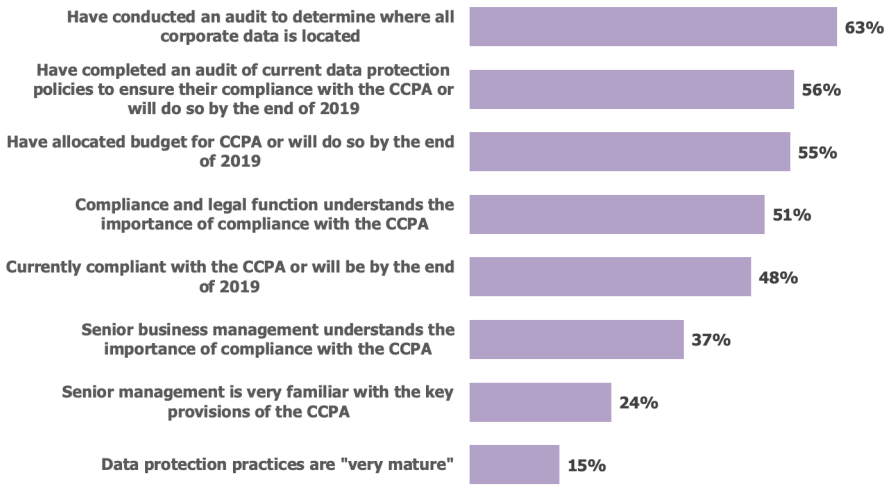
their attention to matters other than lawmaking, the 116th Congress (which will run from January 3, 2019 to January 3, 2021) is on pace to pass just 170 laws. As a result, it seems unlikely that sweeping federal privacy legislation will become a subject of Congressional attention during this or the next Congress.

# The Current State of Readiness

## MOST ARE NOT YET READY FOR THE CCPA

The survey for this white paper was conducted less than three months before enforcement of the CCPA begins, yet our research discovered that most organizations are not yet ready for compliance with the law. For example, as shown in Figure 2, fewer than two-thirds of organizations have conducted an audit to determine where all of their data is located, only 56 percent will have completed an audit of their data protection policies to ensure CCPA compliance by the end of 2019, and only 55 percent will have allocated budget for CCPA compliance by the end of 2019. Moreover, most senior managers outside of the compliance and legal function don't know much about the CCPA or its potential implications.

**Figure 2**
**Readiness for CCPA Compliance**




*Source: Osterman Research, Inc.*

***There are a number of reasons that organizations might not be ready for CCPA compliance.***

Interestingly, the low level of compliance with the CCPA is not dissimilar to the experience of many companies with the GDPR. A 2018 survey conducted by the International Association of Privacy Professionals (IAPP) found that fewer than 50 percent of those surveyed were fully compliant with the GDPR, despite the fact that the regulation went into full effect in May 2018.

## WHY AREN'T THEY READY?

There are a number of reasons that organizations might not be ready for CCPA compliance:

- Many senior managers tend to be more reactive than proactive, and so prefer to deal with problems after they occur rather than dealing with them up-front.
- Some privacy ad-related laws are not enforced vigorously, like most of the data breach notifications laws in the United States. Therefore, decision makers believe their organizations won't be subject to fines and other penalties for violating key provisions of the CCPA.

- Some may believe that in the absence of any operations with the State of California, the CCPA simply will not apply to them or cannot be enforced.

- Some may consider that the vagueness of several provisions within the CCPA will mean that it won't be enforced until the courts have had a chance to settle some test cases that will be brought. Similarly, some may believe that the California legislature will revisit the legislation to address its shortcomings before enforcement begins in earnest, as has already happened prior to the law being enacted.

### WHAT SHOULD DECISION MAKERS DO?

Osterman Research believes that it's not wise to ignore the CCPA for a couple of reasons:

1. California may aggressively enforce the current iteration of the CCPA – flaws and all – and pursue some key test cases early on. This may be driven partially by the fact that the state has indicated it needs in excess of $50 million annually to fund enforcement of the CCPA – even at $7,500 per violation, that will require a lot of fines to be levied to meet the state's budget goal.

2. Even in the absence of any real enforcement of the CCPA, it's a best practice for organizations to get their data house in order. Conducting an audit to determine where corporate data is located, implementing appropriate encryption mechanisms, implementing solutions that will help to prevent data breaches, archiving data, and so forth are all good things for any organization to do even in the absence of legislation that compels them to do so.

## How to Prepare for the CCPA

There are a number of things that organizations should do to prepare for CCPA compliance, as discussed below.

***There are a number of things that organizations can do to prepare for CCPA compliance.***

### UNDERSTAND THAT CONSUMERS OWN THEIR OWN DATA

It's essential that all businesses understand that consumers own their own data, whether that consumer is a resident of California and thus protected under the CCPA, a resident of the European Union and so protected under GDPR, or a resident of a jurisdiction that has yet to pass privacy legislation. While businesses have good reasons to retain and process personal information, they must understand that consumers have the final say over how this information is managed.

### HAVE GOOD DOCUMENTATION

The CCPA entitles a business to charge a higher price to a consumer for a product or service if the consumer opts out of the sale of their personal data, as long as the higher price is reasonably related to the value that the business loses by not being able to obtain their personal data (Section 1798.125). In order to exercise this right, businesses must have defensible documentation on the value they lose by not being able to sell personal data to third parties.

### MANAGE ORGANIZATIONAL DATA WELL

The CCPA implicitly imposes a high standard of care on the management of personal information. Organizations must protect it using a variety of technology solutions and processes that will ensure the data is cataloged, indexed, retained and protected against unauthorized access. In short, data must be treated as a highly valuable asset and protected in-transit and at-rest.

### OBTAINING AND PROVING CONSENT IS KEY

The GDPR is more explicit than CCPA on the requirements around consent, but the CCPA, at least through implication, makes it clear that businesses should obtain clear consent from owners of personal data. CCPA does not have the same concept of legal

bases, but only that Californians "know" what personal data is being collected, "know" if it is being sold or disclosed to others, and can opt-out of such sales and/or require the deletion of their personal data. Hence, consent under CCPA is implicit – if the business has provided notice of activities pertaining to their personal data, and for as long as the data subject does not exercise his or her rights, there is effectively the legal basis of consent.

What is explicit under GDPR and implicit under CCPA, therefore, still requires the following minimum common record keeping:

- That data subjects have been fully and clearly advised on the types of personal data being collected about them.
- That consent has been gained explicitly, or in case of CCPA, has not been withdrawn.
- Dates when consent was gained explicitly or implicitly, and when it was withdrawn (if applicable). Specific dates are required to safeguard the validity of data processing activities between the two dates.

The CCPA takes things one step further, however, and requires website operators to provide a clear opt-out option for sales of personal information, something the GDPR does not do.

### DATA PROCESSORS AND CONTROLLERS MUST MAINTAIN DATA SUBJECTS' PRIVACY

The fundamental intent of the CCPA is to safeguard personal data and to ensure that appropriate protections are in place to meet this requirement. While things like encryption, security, data minimization or DLP are not explicitly spelled out in the CCPA statute, the implication is clear that these types of technologies – and the processes to support them – should be implemented.

***The fundamental intent of the CCPA is to safeguard personal data and to ensure that appropriate protections are in place to meet this requirement.***

## Solutions That Should be Implemented

Organizations that are subject to the CCPA and other data protection and data privacy legislation require a multi-faceted approach to compliance that includes a robust set of organizational and technical measures. Technical measures should include:

- **Cyber security solutions**
  Endpoints, gateways, web applications and cloud services must have appropriate safeguards to prevent unauthorized access, stop unauthorized changes, and protect any type of personal data from malicious threats that attempt to compromise data integrity. Anomalous activities should generate alerts for further investigation, and in high risk situations, begin automated actions that safeguard personal data. Security tools should also continually assess endpoints, servers and other systems to new threat possibilities to determine if there are out-of-date and unpatched operating systems and applications.

  There are a number of security technologies and processes that are important to consider in the context of compliance with the CCPA and other privacy regulations. These include threat intelligence and threat analytics that can help security analysts to understand the source of potential data-breach focused threats, user and entity behavior analytics (UEBA) that can detect inappropriate actions by users or endpoints that could lead to privacy violations, Security Information and Event Management (SIEM) solutions that can help security analysts to collect and correlate log data as part of threat hunting activities,

next-generation firewalls, endpoint detection and response (EDR) solutions, web application firewalls and the like. Newer, client-side threats like Magecart attacks have to be taken into consideration to fully protect user data processed in web applications.

- **Device and data encryption**
  Encryption makes personal data unintelligible and inaccessible to people who lack access authorization and rights. While the CCPA does not mention encryption as a data protection safeguard, if personal data is encrypted to a sufficient level, it is much more difficult for a data breach to be successful. Organizations are excused from breach notification requirements if strong encryption was in place for the breached data.

- **Archiving solutions**
  An archiving solution will enable the long-term retention of data in a way that makes it impossible to modify or delete after the fact. However, archiving solutions still need to enforce data protection safeguards over personal data and must have the ability to delete personal data if it matches the conditions of a valid deletion request.

- **Data backup**
  Personal data that is copied to a backup solution to enable disaster recovery will still require safeguards and protections. This includes limiting access to backup media, limitation of access to backup files, and in the case that a backup is put back into service as part of a recovery operation, the intelligence to enforce erasure requests that were initiated subsequent to the backup being created.

- **Data governance solutions**
  Administrators must exercise appropriate care to ensure that data is retained for the right reasons, processed for as long as processing is valid, authorized, and not objected to, and deleted when a valid deletion request is received. This requires advanced data governance tools that can identify personal data, manage retention, and enforce deletion under the right conditions.

- **File analysis and data classification solutions**
  Protecting personal data in structured databases and other corporate systems is easier than protecting personal data in unstructured systems and free-form repositories. Unstructured data - email messages, file shares, SharePoint document libraries, Word documents, Excel spreadsheets, local drives, backups, and non-sanctioned cloud apps - all present significant risks to personal data. File analysis solutions can reduce the risk of unauthorized access and data breaches by proactively seeking out personal data in unstructured systems and formats and automatically applying appropriate protections. File analysis platforms can also help with defensible deletion and creating and maintaining a data map, both of which are core elements to CCPA compliance.

- **Pseudonymization and anonymization**
  While encryption uses a random mathematical key to obfuscate data values, encryption can be circumvented if the encryption key is also breached. Pseudonymization and anonymization are two alternative ways of introducing obfuscation of personal data; the first involves substituting a personal data value with a lookup identifier to a separate system, and the second replaces personal data with a meaningless string. The risk of both is unauthorized reversal of the process, with pseudonymized data holding the greater risk of the two. If used, both approaches need to be done in light of this risk, and should apply to production systems, testing and development environments, and archived data.

  It's important to note that the CCPA implies that organizations can "re-identify" an individual after pseudonymization "as long as the means of doing so 'is kept separately and is subject to technical and organizational measures.'"[v]

***Administrators must exercise appropriate care to ensure that data is retained for the right reasons.***

- **Data loss prevention**
  Data loss prevention (DLP) solutions search for personal data in email messages, attachments, and other systems that send data between people. Depending on the specific DLP solution, adaptive protection or message blocking can be applied. For example, if the recipient was authorized to receive the number, the message could be automatically encrypted to prevent unauthorized access. If the recipient is not authorized to receive the number, a DLP solution could block it from being sent. Alternatively, DLP solutions require effective pattern-matching algorithms that identify and classify personal data, and a range of mitigations to protect it. DLP solutions help prevent against accidental data breaches by employees, which continue to be the primary source of "insider" data breaches.

- **Data infiltration**
  Technologies like DLP are essential to identify and prevent data exfiltration, but there should also be solutions in place to identify and prevent data infiltration. For example, if a new employee joins from a competitor and brings a spreadsheet containing customer details (name, contact details, products used, revenue levels), it is incumbent on the new organization to block the new data from being added to their systems. A policy statement to this effect will also be necessary in the employee's code of conduct and onboarding process.

- **Identity, access and management solutions**
  Data protection depends on limiting who has access to personal data, especially sensitive personal data. Identity, access and management (IAM) solutions enforce unique identifiers for each employee, with one or more authentication demands required before access is granted to personal data. Organizations that permit shared login credentials will violate the intent of data protection requirements. Good systems and processes to enforce identity and control access limits the attack surface area for personal data, and it means that departing employees can be prevented from accessing personal data once they have left.

- **Application security testing**
  Applications that access personal data must be tested for vulnerabilities. Application security testing tools provide automated testing methods to ensure that vulnerabilities are identified, silly mistakes are not made, and mitigation pathways for weaknesses are identified before a breach takes place. Unpatched and zero-day vulnerabilities on servers will be exploited. Consider solutions that provide real-time visibility into the client-side execution of the application code in production.

- **Employee training**
  Robust employee training for both cyber security and compliance is essential since a solely technical approach is inadequate to provide complete protection. Good training can enable users to become much more proficient at recognizing threats like phishing and business email compromise attempts, it can help them to take the appropriate actions when faced with anomalies, and it can help them know how to manage personal data properly.

- **Other technologies**
  There are other types of tools that can elevate data protection measures for an organization, including privileged account management, incident response systems, mobile device management, and more. Organizations should take a wide view of the potential for undermining or compromising personal data, and put in place the best mitigations possible. While intentional actions to protect personal data may not be enough to prevent a data breach, for example, the fact that intentional actions have been taken will give strong evidence of the organizational intent to be compliant.

***Data protection depends on limiting who has access to personal data, especially sensitive personal data.***

In short, data protection for CCPA compliance requires a balanced set of organizational and technical measures. The technical measures discussed above, implemented in line with a clear view of the risks to personal data in an organization,

and in combination with complementary organizational measures, will help craft a strong data protection approach and culture.

## Summary

The CCPA is an important new privacy regulation with which most companies will need to comply. While it is similar in concept to the GDPR, it includes some important differences that will require IT, security, compliance, legal and other teams to take a fresh look at their consent, training and information management practices; as well as ensure that their cyber security, archiving, encryption, file analysis, DLP, backup and other technologies are adequate.

## Sponsor of This White Paper

MessageSolution is an industry leader for CCPA and GDPR compliance and eDiscovery management. Focusing on innovating world-class enterprise data governance, intelligent classification archiving and eDiscovery solutions, MessageSolution is a Cloud Service Provider providing native integration with Microsoft Office 365, Google G-Suite, IBM Domino and all enterprise on-premise email file SharePoint platforms. MessageSolution delivers privacy framework-based on search automation and classification of Personally Identifiable Information (PII) discovered in Exchange Online, OneDrive, SharePoint, Teams and network fileshares.

Headquartered in Silicon Valley, California with a team of dedicated professionals including technology veterans from IBM and Sun Microsystems and graduates of Stanford University, MessageSolution has operations in North America, Europe, and mainland China, along with distribution channels worldwide and enterprise customers in over 50 countries.

MessageSolution™
Enterprise Archiving, eDiscovery, Migration

**www.messagesolution.com**

**Twitter: @GlobalArchiving**

**+1 408 383 0100**

## REFERENCES

[i] https://fpf.org/2019/09/26/ccpa-2-0-a-new-california-ballot-initiative-is-introduced/

[ii] https://www.reuters.com/article/uk-usa-privacy-microsoft/microsoft-says-it-will-follow-californias-digital-privacy-law-in-u-s-idINKBN1XL2EN

[iii] https://truthonthemarket.com/2019/07/01/10-reasons-why-the-california-consumer-privacy-act-ccpa-is-going-to-be-a-dumpster-fire/

[iv] http://www.enforcementtracker.com

[v] https://www.johndcook.com/blog/2019/07/11/ccpa-deidentified-data/