Data privacy and security regulation is growing rapidly around the world, including in the United States. In addition to strengthening the requirements to secure personal data, individuals are being given an increasing array of rights concerning the collection, use, disclosure, sale, and processing of their personal information. Meanwhile, organizations’ growing appetite for more data, and more types of data, persists, despite mounting security risks and concerns about permissible use. The recently enacted California Consumer Privacy Act (CCPA) is intended to address some of these risks and concerns.

The CCPA, which becomes effective on January 1, 2020, is in some ways the most expansive privacy law currently in the United States. Organizations familiar with the European Union’s General Data Protection Regulation (GDPR), which became effective on May 25, 2018, certainly will understand CCPA’s implications. Perhaps the best known comprehensive privacy and security regime globally, GDPR solidified and expanded a prior set of guidelines/directives and granted individuals certain rights with respect to their personal data, such as the right of access, the right of erasure (popularly known as the “right to be forgotten”), and the right to restrict the processing of personal data. In addition to mandating security for personal data, GDPR requires that individuals be notified of such things as the purpose and legal basis for processing their personal data, the categories of recipients of that data, and if the data has been breached. Many of these same principles are present in the CCPA.
5376 (WPA). That bill would establish GDPR-like requirements on businesses that collect personal information related to Washington residents. In addition to requirements for notice, and consumer rights such as access, deletion, and rectification, the WPA would impose restrictions on use of automatic profiling and facial recognition.

With the CCPA’s effective date fast approaching, regulations being prepared by California Attorney General Xavier Becerra’s office, and considering that certain provisions may reach back prior to the effective date, businesses need to begin preparing as soon as possible. These FAQs are intended to call attention to some of the pressing issues relating to the CCPA’s application to employee personal information, and highlight action items that can help businesses’ compliance efforts.

1. What businesses does the CCPA apply to?

The CCPA will apply to any entity that does business in the State of California and satisfies one or more of the following: (i) annual gross revenue in excess of $25 million, (ii) alone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices, or (iii) derives 50 percent or more of its annual revenues from selling consumers’ personal information.

Regulations may clarify one or all of these prongs, but some small businesses will not be able to escape the CCPA’s reach. The law is trying to reach businesses with significant amounts of data, and that could very well be smaller companies. Additionally, businesses with small operations in California that meet one of these requirements will have significant privacy obligations with respect to those operations.

2. Does the CCPA apply to employment data?

The application of the CCPA to employee data remains an open question. On its face, the CCPA appears to apply only to California “consumers.” However, the CCPA's definition of consumer (a California resident), combined with California’s longstanding practice of protecting individual privacy rights, suggests that the CCPA also may extend to the personal information of California residents maintained as part of the employment relationship. If so, this would include residents of California who are job applicants, full- or part-time employees, temporary workers, interns, volunteers, independent contractors, and even such persons’ dependent(s) or beneficiary(ies). For purposes of these FAQs, we refer to these individuals as “Workforce Members.”

The definition of “consumer” states: “a natural person who is a California resident.” 1798.140(g). That definition is not qualified by requiring such natural persons to be purchasing goods or services from businesses subject to the CCPA. It includes all persons who are residents in California. Additionally, one of the examples for what constitutes “personal information” under the law is “[p]rofessional or employment-related information.” 1798.140(o).

On the other hand, the name of the law itself, and the fact that the law does not mention employers or employees, suggests that the legislature intended to protect the personal information of California residents in their role as consumers, and not employees (or Workforce Members). Additionally, prohibited discriminatory acts under the law include (i) denying goods or services, or providing a different level or quality of the goods and services, to the consumer, (ii) charging different prices or rates for goods or services, or (iii) suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. Unlike what one might expect for a law protecting Workforce Members, the CCPA does not include acts that relate to the employer-employee relationship.

So, perhaps the CCPA’s reference to professional or employment-related information intended to reach such data not in the hands of employers, but businesses handling such data for commercial purposes (such as a recruiting
to the definition of “consumer” or any other change that would indicate an intention to exclude Workforce Members personal information from protection under that law.

Employers will have to wait and see whether there will be any additional amendments, or whether the Attorney General will clarify the issue through regulation. Currently, Attorney General Becerra is in the middle of six rulemaking workshops around the state in order to assist his office in formulating those regulations. Employers should watch these developments closely, but they also should consider taking some preliminary steps in order to be prepared to comply.

The remainder of this article assumes that the CCPA will be found to apply to Workforce Members data.

3. What is personal information under the CCPA?

The CCPA defines personal information broadly to include information that can identify, relate to, describe, be associated with, or be reasonably linked directly or indirectly to a particular consumer or household. This might be a name, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver’s license number or passport number, biometric information, bank account number or any other financial information, geolocation data, audio, electronic, or visual information, employment–related information, certain education information, or medical or health insurance information. It also may include inferences drawn from any such information used to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

In the employment context, personal information is likely to be present in:

- A job application, resume, or CV;
- An employment contract or independent contractor agreement;
- A performance review or disciplinary record;
- A photo used for an identification badge or organizational chart, marketing, or website;
- Biometric data used for timekeeping or facility access;
- Backup files;
- Information from company devices or vehicles, including geolocation data;
- Browsing history or search history;
- Information used for payroll processing and benefits administration;
- Internal or external contact information maintained in the electronic onboarding, HRIS system, or Active Directory; or
- Information captured from video, audio, systems, or other forms of monitoring or surveillance.

Personal information also might include data collected about Workforce Members as part of an organization’s human capital analytics or talent management programs. As noted above, the law applies to information used to create a profile about a natural person who is a California resident that would reflect such person’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
The CCPA does not apply in certain situations, some of which may be relevant in an employment context. For example, the CCPA does not apply to medical information governed by the Confidentiality of Medical Information Act (CMIA) or protected health information collected by a covered entity or business associates governed by the privacy, security, and breach notification rules of HIPAA/HITECH. Thus, the CCPA is unlikely to apply to a Workforce Member’s personal information accessed, created, or maintained in connection with the employer’s group health plan. Likewise, medical information that an employer receives in connection with an Family and Medical Leave Act certification, Americans with Disabilities Act reasonable accommodation, workers’ compensation claims, and so on, likely would not be subject to CCPA to the extent it is covered under the CMIA. See Cal. Civ. Code Sec. 56.20.

4. If the CCPA applies to certain employers and their Workforce Member data, would it apply to personal information collected in connection with the administration of employee benefits?

Yes, but perhaps not to all of those employee benefits. If the CCPA applies to Workforce Member data, and considering the broad definition of personal information discussed above, data involved in the administration of employee benefits generally would be within the scope of that definition. However, the CCPA provides specific exemptions that may exclude certain benefit plan data from its reach; namely, plans subject to the HIPAA privacy and security regulations (such as medical plans, dental plans, and health flexible spending arrangements).

There are, of course, may other kinds of employee benefits, such as pension and 401(k) plans, life and disability insurance plans, tuition assistance programs, employee discount programs, wellness program, transportation fringe benefit programs, and others. However, some of these employee benefits may involve plans that are subject to the Employee Retirement Income Security Act of 1974 (ERISA), which preempts certain state laws to the extent those laws relate to ERISA-covered employee benefit plans. A complete discussion of ERISA preemption is beyond the scope of this article, but a significant purpose behind it is to promote uniform administration of benefit plans nationally, avoiding a state-by-state approach. The application of the CCPA, and similar laws in other states likely to follow, certainly would complicate the national administration of such plans.

5. What rights would a Workforce Member have?

A Workforce Member would be entitled to each of the rights set forth in the CCPA. For example, under the CCPA, Workforce Members would have the right to request that a business, including an employer, disclose or provide access to personal information it has collected about the Workforce Member, the business or commercial purposes for using the information, and the third parties with whom the business shares the information. For many employers, meeting these obligations may not be too difficult. Employers generally will know the data they collect about their Workforce Members, why they collect it, and the third parties to whom they share the information. However, some employers may be using Workforce Member data in ways that they would prefer not to announce to their workforce or be available to their competitors. For instance, certain talent management strategies or other uses of information could be indicative of future business decisions such as layoffs or expansions into new markets.

Workforce Members also would be able to request deletion of their personal information and opt-out of the sale of their personal information to third parties. While most employers are probably not selling Workforce Member data, having to delete Workforce Members’ personal information could be a significant challenge. Being in a position to carry out this obligation requires knowing where the data is to be deleted. It also means knowing which vendors maintain the data so they could delete it as well. Thus, some kind of inventory or data mapping exercise would be needed to track the data and answer some basic questions such as what data is maintained, why it is maintained, and where it is. Knowing why the data is being maintained is important because employers would be able to push back on deletion requests if the employer, for example, has a legal obligation to retain it. In short,
The rights under the CCPA also include the right to receive notice of the business's personal information collection and processing activities before or at the point of collection, as well as notice of the Workforce Member’s rights. Similar notices may need to be made on the businesses’ website(s) and online privacy notices. These notices are intended to help ensure individuals are aware of how their personal information is being processed, as well as the rights they have to control their personal information. Employers will have to carefully consider these notices, balancing efforts to ensure they are compliant, but also avoiding creating an administrative burden.

6. What obligations do the notice and rights provisions of the CCPA place on businesses?

As discussed above, under the CCPA, covered businesses, including employers, will need to provide notice to Workforce Members that includes the types of personal information collected by the business and how it is used; the Workforce Member’s right to access that personal information; the right to delete the information; the right to know the third parties with whom it is shared; and the right to object to its sale to third parties, if applicable.

The CCPA also demands that covered businesses take steps to enable consumers to exercise these rights. Thus, for example, covered businesses will be obligated to make available two or more mechanisms for submitting requests for information required to be disclosed under the CCPA, including, at a minimum, a toll–free telephone number and, if the business maintains an internet web site, a web site address. When requests for information are made under the CCPA, businesses generally must respond to verifiable Workforce Member requests within 45 days. That period may be extended as long as the Workforce Member is notified within the first 45–day period. The response must cover the 12–month period preceding the receipt of the request. Responses must be in writing and the business is not required to respond to more than two requests for the same Workforce Member during a 12–month period. The CCPA requires that the employees designated to handle the responses to these requests receive training.

7. Can a Workforce Member agree to waive his or her rights?

No. The CCPA specifically prohibits any contractual provision or agreement that attempts to waive or limit the CCPA’s rights, including the right to remedy or enforcement. As a result, any attempt to limit a Workforce Member’s rights, whether by employment contract, agreement, or policy, would be unenforceable.

8. Where is Workforce Member personal information typically stored by organizations?

Protections under the CCPA apply to personal information regardless of its format. Thus, when thinking of where to look, employers should look broadly. For example, Workforce Member personal information can be stored in multiple locations, such as: a business’s electronic onboarding system, HRIS system or Active Directory; file shares or backup files; in benefits or training records; in file cabinets or on a copy machine’s hard drive; a manager’s “desk copy”; or with third party services providers, such as a payroll processor or travel agency. It is imperative that covered businesses review, assess, and understand their existing data storage practices.
The CCPA’s focus is on privacy of personal information and extending greater control to individuals concerning their data. However, security is an element of privacy and while the CCPA does not expressly require the implementation of specific security measures, it notes a business’s duty to “implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.” To do so, organizations typically would need to conduct a risk assessment that reviews the types and sensitivity of its Workforce Members’ personal information, as well as the risks to the security and privacy of this information. If California employers have questions about specific safeguards for maintaining security, they can refer to the California Attorney General’s February 2016 Data Breach Report, which discusses best practices for data safeguarding. Employers should be aware similar frameworks are mandates in other states, such as Colorado, Massachusetts, and Oregon.

10. Can a covered business be sued for violating the CCPA?

The CCPA authorizes a private cause of action against a covered business for damages resulting from a failure to implement appropriate security safeguards which result in a data breach. The definition of personal information for this purpose is much narrower than the general definition of personal information under the CCPA. Here, the CCPA incorporates much of the definition of personal information under the California breach notification law. See Cal Civ. Code Section 1798.81.5(d)(1)(A). What should be troubling for covered businesses is that, if successful, a plaintiff can recover damages in an amount not less than $100 and not greater than $750 per incident or actual damages, whichever is greater, as well as injunctive or declaratory relief and any other relief the court deems proper. Thus, in addition to notifications a covered business may have under the state’s breach notification law, class action lawsuits brought pursuant to this provision of the CCPA could be very costly.

Before a Workforce Member would be able to bring a lawsuit following an employer’s data breach, he or she must provide the employer 30 days’ written notice identifying the specific provisions of the CCPA that were violated. If cure is possible, and if within the 30 days the employer actually cures the noticed violation and provides an express written statement that the violations have been cured and that no further violations shall occur, the Workforce Member would not be able to pursue the action for individual statutory damages or classwide statutory damages. The Workforce Member still could seek actual pecuniary damages suffered as a result of the alleged violations.

11. What happens to Workforce Member personal information if the business is acquired?

Workforce Member personal information may be part of business assets that are transferred to a third party in the course of a merger, acquisition, or bankruptcy when the third party assumes control of all or part of the business. This type of transfer is not deemed a sale of personal information for the purposes of the CCPA. Notwithstanding, if the third party materially alters how it uses or discloses the Workforce Member’s personal information and that use or disclosure is a materially inconsistent with the notice provided to the Workforce Member at the time of collection, the third party must provide the Workforce Members with prior notice of the changed practices.

12. Does the CCPA apply if a Workforce Member is no longer a resident of California?

In the event a Workforce Member moves or is transferred to a location outside of California, depending on the facts, the Workforce Member may no longer be a resident of California and his or her personal information will no longer be protected by the CCPA. Notwithstanding, the Workforce Member’s personal information may be protected by other laws and the organization may still have the same, or even heightened, obligations to safeguard the Workforce Member’s data. Employers should consider this and similar issues when drafting notices for employees concerning their rights under the CCPA. For example, if a notice extends rights to an “employee” and not an “employee who is a California resident,” a transfer that would change the person’s residency may not
The CCPA specifies that its obligations are a matter of statewide concern in California and supersede and preempt all rules, regulations, codes, ordinances, and other laws adopted by a city, county, municipality, or local agency regarding the collection and sale of a consumer’s personal information by a business.

However, the CCPA also specifies that its obligations shall not restrict a business’s ability to comply with federal, state, local laws, or regulations. In addition, while the CCPA is drafted to supplement federal and state law, it shall not apply if it is preempted by or in conflict with federal law, the United States Constitution, or the California Constitution. To determine which laws or regulations will govern, an organization will need to identify all the purposes for which Workforce Member information is collected, processed, and retained. For example, the federal Fair Labor Standards Act (FLSA) expressly requires the retention of employee identifying information for a specified period of time. These requirements would preempt the employee Workforce Member’s ability under the CCPA to request deletion of certain personal information that must be retained to satisfy compliance under FLSA. Similarly, as discussed above, ERISA includes certain recordkeeping requirements relating to an employer’s employee benefit plans. Specifically, section 209 requires that an employer maintain employee records sufficient to determine benefits. Again, an employee Workforce Member’s request for deletion of certain personal information may be information subject to ERISA retention requirements. In such a case, the employer’s obligations under CCPA would yield to ERISA’s requirement.

**Recommended Action**

While it is presently unclear whether the CCPA will apply to Workforce Member personal information, the question has been raised and efforts to remove Workforce Member data from the CCPA’s reach have thus far been rejected. Regulations from the California Attorney General’s office may provide some clarity on this point. It is also reasonable to believe further guidance or amendments from the California legislature may be forthcoming. In the interim, there are several steps an employer can take to better position itself for potential compliance obligations.

1. Monitor the status of the CCPA to ensure the organization is aware of additional amendments and the regulations that will be issued.

2. Begin staging resources to be able to identify and map the Workforce Member personal information in the organization’s possession or under the organization’s control. All successful compliance activity is built upon knowledge of what information is collected, who it is collected from, how it is collected, why it is collected, all purposes for which it is used, all locations where it is stored, and any third party with whom it is shared. Of course, the organization may already have obligations to safeguard personal information, which may include deleting information that is no longer needed. To meet such requirements, the organization needs to answer many of the same questions.

3. Review and identify existing or needed organizational and technical procedures to facilitate compliance with Workplace Member rights under CCPA. These should include:

   - Developing or identifying at least two mechanisms for permitting Workforce Members to exercise their rights to request information on what the business collects, the purposes for which it is used, the third parties with whom it is shared.
   - Review and identify existing or needed organizational and technical procedures to facilitate compliance with Workplace Member rights under CCPA.
whom it is shared (such as a payroll processor). Mechanisms can include an email address, postal address, website link, phone number, and so on.

- Developing or identifying internal mechanisms that could be made available to respond to an employee’s exercise of access rights, including verifying their identity, responding within the mandated timeframe, and documenting the request and response.
- Developing or identifying an internal mechanism for deleting a Workforce Member’s personal information on request. This will include determining whether any state or federal laws preempt the deletion and notifying third parties with whom the organization has shared the information (such as payroll processors and IT vendors) to delete the information.
- If applicable, developing or identifying an internal mechanism to track third parties to whom Workforce Member personal information is sold in order to comply with the Workforce Member’s request to opt out of that sale.
- Developing or identifying procedures for handling Workforce Member personal information upon separation from employment. This includes identifying what state and federal laws address record retention and destruction and how they interact with the CCPA and an organization’s operational needs.

4. Review or create a data retention schedule that reflects the types of data the organization maintains. The obligation to safeguard data, both under the CCPA and Cal. Civ. Code 1798.81.5, is a significant reason to reduce the amount of personal information retained after it is no longer necessary for the purpose for which it was collected. Consider operational and regulatory retention requirements such as those imposed by FLSA and ERISA.

5. Identify whether the organization’s standard employment contracts or employee manual or handbook should be updated to include notice of collection and processing activities, as well as Workforce Member access and deletion rights. The organization also may need to convey similar information in other places, such as its intranet, business website, website privacy policy, and consumer rights notice.

6. Begin identifying the staff who would be responsible for handling employee access rights and other requests under the CCPA, and how the organization might train these staff members. It will be important to maintain consistency when carrying out these obligations.

7. Review vendor contracts for those vendors with access to Workforce Member personal information (such as IT providers, HRIS software and service providers, payroll processors, travel agencies, and professional service providers). Provisions should address appropriate security safeguards, data breach reporting obligations, use and disclosure limitations, data retention and disposal, and the ability to assist the business in responding to a Workforce Member rights request. Employers should be negotiating, reviewing, or renegotiate existing vendor contracts to ensure the vendor’s ability to comply with access rights relating to information collected and retained. This practice dovetails with the requirements of Cal. Civ. Code 1798.81.5(c) to contractually require that a third party with whom the business shares personal information maintains reasonable security procedures to safeguard the business’s personal information.

8. Review organizational and technical access controls. As discussed above, the CCPA permits a consumer to bring a private cause of action against a business for the unauthorized access and exfiltration, theft, or disclosure of personal information as a result of the business’s failure to implement and maintain reasonable security procedures and practices. California’s breach notification law excepts from the definition of a breach an unauthorized but good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business, as long as the information is not used or subject to further unauthorized disclosure. However, in permitting a private cause of action for a data breach, the CCPA does not provide for this exception. As a result, an employer may be liable for the unauthorized access of Workforce Member personal information by its employees and agents even if the incident is not a reportable breach under Cal. Civ. Code section 1798.82. To guard against this, businesses should ensure their organization has appropriate policies and procedures in place, including role-based access, password management, system auditing, and
9. Review the business’s written information security program (WISP) or internal administrative and technical policies and procedures to reflect and demonstrate compliance with the CCPA requirements of security safeguards appropriate to the nature of the information to protect the personal information.

Conclusion

Many of the steps listed above may be adapted to satisfy other data privacy protection frameworks, assist in developing a robust internal data protection program, or position the business for future regulatory obligations. All 50 U.S. states have now enacted data breach notification laws. Many have enacted laws addressing data safeguarding, disposal, or vendor management, and many, like the state of Washington, may begin advancing legislation similar to the CCPA. Several federal data protection laws are under consideration and countries around the world continue enacting national data privacy laws to protect individuals. This legislative activity, combined with the growing public awareness of data privacy rights and concerns, makes the development of a meaningful data protection program an essential component of business operations.

Jackson Lewis P.C. © 2019
The increased focus on protecting personal privacy may pose a new challenge to the bounds of e-discovery in U.S. litigation as courts reconcile whether and how new data protection laws apply to a litigant's obligation to produce relevant information.

**Discovery in the U.S.**

Traditionally, U.S. litigation has favored broad civil discovery, permitting litigants a wide berth to explore the factual underpinnings of their cases. Until its amendment in 2015, Federal Rule of Civil Procedure 26(b)(1) was read to empower litigants to obtain discovery with respect to any non-privileged matter provided it generally was "relevant" to a party's claim or defense. However, partially in response to the burden associated with the exponential growth of electronic discovery, this rule as amended now underscores that discovery not only be relevant, but also "proportional to the needs of the case." Fed. R. Civ. P. 26(b)(1). Some state rules, including in New York's Commercial Division, have followed suit by emphasizing proportionality in discovery.

In theory, this focus on proportionality could result in discovery requests and productions that are more tailored to the issues and electronically stored information (ESI) in question. What potentially complicates the process, however, is that relevant information can be mixed with certain additional data of both a business and personal nature; accordingly, even under a proportionate approach, that data may be swept up in a production. The U.S. legal system typically addresses any resulting privacy concerns with confidentiality agreements or protective orders and in limited instances redactions, but this approach may still result in some personal information—that may not otherwise be relevant to the case—being reviewed and produced.

A new challenge to the bounds of U.S. discovery, therefore, will be addressing the intersection of discovery with the increased awareness and focus on privacy and data protection.

**General Data Protection Regulation**

The European Union's (EU) General Data Protection Regulation (GDPR) became effective on May 25, 2018, and already is presenting a significant testing ground for how U.S. discovery can be reconciled with data protection requirements.

The GDPR addresses individuals' "fundamental ... right to the protection of personal data." GDPR, art. 1(2). It covers the personal data of individuals in the European Economic Area (EEA) (data subjects) and any processing of personal data by organizations directly (data controllers) or those acting under written instructions of data controllers (data processors), even if the entity is not located in the EEA but provides goods and services to data subjects in the EEA or monitors data subjects' behavior taking place in the EEA. GDPR, art. 3. As such, the GDPR impacts crossborder discovery sought in U.S. litigation because its requirements could reach parties that are foreign organizations, or domestic entities with a presence abroad, that have relevant sources of information located in the EEA. Given the global economy, this scenario is increasingly common.

This article describes some of the primary ways in which U.S. practitioners engaging in cross-border discovery may encounter the GDPR's requirements, but practitioners who may handle data covered by the GDPR would be well advised to understand the intricacies, and practical implications, of this comprehensive regulation.

**Personal Data.** As a threshold matter, the GDPR defines "personal data" far more broadly than what typically is understood as personal information in the United States and includes "any information relating to an identified or identifiable natural person," such as "a name, an identification number, location data, an online identifier" or "one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity" of a person. GDPR, art. 4(1). At least some of this
information may be included in such mundane places as the signature block of an email, a type of ESI that necessarily would be produced in many cases.

**Processing Personal Data**: The GDPR governs "processing" of personal data, which covers a wide range of actions, including "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." GDPR, art. 4(2).

In terms of U.S. discovery of GDPR protected data, processing encompasses, at a minimum, collection, review, deletion, production and cross-border transfer of that data. Under the GDPR, personal data must be processed "lawfully, fairly and in a transparent manner" and in accordance with the data minimization principle, which requires that processing be "adequate, relevant and limited to what is necessary in relation to the purpose" for which the data is processed. GDPR, art. 5(1). There are six lawful bases for processing, including consent, where it is necessary for the legitimate interests of a data controller or third party, compliance with a legal obligation or a contractual obligation. GDPR, art. 6(1).

Notably, litigants may have a legitimate interest in accessing information that is necessary to make or defend a legal claim, subject to demonstrating that the data subject's privacy rights do not override the litigant's legitimate interests in processing the data. Moreover, corporations may have a legitimate interest in conducting internal investigations and in responding to government investigations. Where special categories of personal data are present—such as data that reveals racial or ethnic origin, political, religious or philosophical beliefs, or health or biometric data—litigants also will be required to fulfill additional conditions.

In exceptional circumstances, consent by the data subject can serve as a basis for processing, but it must be a "freely given, specific, informed and unambiguous indication of the data subject's ... agreement to the processing of personal data." GDPR, art. 4(11). Consent should be relied on cautiously because (1) it is unlikely to be valid in the common employer and employee context due to an imbalance of power and (2) if a data subject does not consent (or later withdraws consent), the litigants can no longer process the data.

Practitioners should be aware of the GDPR's heightened transparency requirements. Data subjects must be provided with notice of the intended processing activity, which should be communicated to data subjects prior to processing any of their personal data. The notice must be "concise, transparent, intelligible," in "clear and plain language," and may be incorporated directly or by reference into legal hold notices. GDPR, art. 12(1).

**Transferring Personal Data.** There are additional requirements for the cross-border transfer of personal data outside of the EEA, such as to the United States for use in a litigation. Generally, transfer is only permitted to a country that the European Commission (EC) has designated as providing an adequate level of protection, or through a valid transfer mechanism providing for appropriate safeguards. The EC does not consider the United States to offer an adequate level of protection, so impacted parties must make the transfer to the United States subject to appropriate safeguards or rely on one of the legal exceptions or "derogations." GDPR, arts. 46, 47 and 49. In some cases, organizations transferring data may rely on appropriate standard contract clauses or the EU-U.S. Privacy Shield, a framework allowing U.S. companies that have aligned with certain provisions of the GDPR to self-certify and transfer data from the EEA to the United States.

Explicit consent by the data subject can be a basis for transferring data to a country that is not considered by the EC to offer an adequate level of protection, but, as with processing, this method should be used cautiously. Moreover, derogations to the transfer requirements should only be relied upon sparingly and in addition to other safeguards, if applicable.

**Potential Fines.** The GDPR is notable in terms of the fines it prescribes for violation: up to €20 million (approximately $23.5 million) or 4 percent of the violating company's total annual global revenue, whichever is higher. GDPR, art. 83(5). The GDPR also grants individuals the right to compensation for material and non-material damage caused by a data controller's or processor's breach of the GDPR requirements, as well as discretion for EEA countries to legislate for additional criminal sanctions for infringements.

The threat of these penalties, even if remote, makes it even more crucial to understand, and comply with, the GDPR in the context of cross-border discovery.

**Protections in Other Jurisdictions**

A number of other jurisdictions, including in the United States, also have passed privacy and data protection laws which may impact discovery of covered data.

U.S. Jurisdictions. On June 28, 2018, California became the first state to enact comprehensive data protection legislation with the California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100 to 1798.199, which will become operative in approximately one year, on January 1, 2020. Like the GDPR, the CCPA has an expansive definition of covered personal information for California residents. The CCPA applies to businesses that, among other things, do business in California with annual gross revenue exceeding $25 million, as well as certain service providers processing personal information on behalf of a covered company. The CCPA focuses on the sale of personal information and includes giving consumers the right to know specifics about the personal information a business has collected from them and to have that personal data deleted. The CCPA prescribes that in case of any conflict with another California law, the law that affords the greatest privacy protections shall control. The CCPA also instructs that the new law "shall be liberally construed to carry out its purposes."

Notably, although the U.S. does not have comprehensive national data protection legislation, in mid-January 2019, a new bill was introduced in Congress aimed at creating federal privacy standards in the context of consumer protection, which could (if enacted) pre-empt state laws such as the CCPA. Laws such as these might impact the preservation, collection and production of personal information for e-discovery purposes.

Foreign Jurisdictions. Laws that may impact the processing and transfer of data exist in foreign jurisdictions in addition to the EU—including in Canada, Latin America, and Asia. As but one example, Brazil's first General Data Protection Law, which goes into effect in February 2020, applies not only to companies that collect or process data in Brazil but also extraterritorially to companies that process data related to persons in Brazil or for the purpose of offering goods or services in Brazil. Therefore, when conducting crossborder discovery in these or other jurisdictions, privacy or data protection requirements should be carefully considered.

Reconciling U.S. Discovery Rules and Various Data Protection Laws

Undoubtedly, U.S. courts will continue to examine the breadth of permissible discovery and balance it against the need to protect personal privacy, particularly as electronic data and the technology that handles it proliferate. However, how U.S. courts specifically will enforce discovery rules in response to the breadth of the GDPR requirements or new national privacy legislation may be somewhat unchartered territory. In reconciling foreign data protection laws with U.S. discovery rules, courts have, to date, applied a balancing test the U.S. Supreme Court established in its 1987 decision, Société Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa, which held that a French blocking statute did not preclude American courts from ordering discovery from a party subject to U.S. jurisdiction. 482 U.S. 522 (1987). More recently, courts have continued to hold that the interests of U.S. discovery outweigh foreign data protection laws. See, e.g., Royal Park Invs. SA/NV v. HSBC Bank USA, N.A., No. 14 Civ. 8175, 2018 WL 745994 (S.D.N.Y. Feb. 6, 2018) (Belgian Data Privacy Act); Knight Capital Partners Corp. v. Henkel AG & Co., 290 F. Supp. 3d 681 (E.D. Mich. 2017) (German Data Protection Act); Laydon v. Mizuho Bank, Ltd., 183 F. Supp. 3d 409 (S.D.N.Y 2016) (EU privacy laws). In a different test of privacy concerns, the New York Court of Appeals, while recognizing privacy rights, has held that photographs and information posted under a privacy setting on Facebook were material and necessary evidence subject to civil discovery. Forman v. Henkin, 30 N.Y.3d 656 (2018).

In one of the first cases involving the GDPR since it became effective, Microsoft recently argued that retention and production of data relevant in a patent infringement case "raises tension" with the GDPR and would require burdensome steps to anonymize the personal data. Corel Software, LLC v. Microsoft Corp., No. 2:15-cv-00528, 2018 WL 4855268, at *1 (D. Utah Oct. 5, 2018). Nonetheless, the court ordered retention and production, finding that the benefit of the data, which was relevant and proportional, outweighed the burden or expense of compliance.

Originally published in New York Law Journal

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.
California, home to more than 40 million people and the 5th largest economy in the world, has passed the California Consumer Privacy Act (CCPA), its omnibus consumer privacy law. The law creates sweeping new requirements concerning the collection, maintenance, and tracking of information for both employees or customers who are residents of California. Many aspects of the implementation and enforcement are still being finalized by the California Attorney General. However, companies with employees or customers in California need to take stock of the information they are processing that could qualify as “personal information” for California residents, and they need to begin establishing mechanisms for compliance before the end of 2019.

The California Consumer Privacy Act

Effective January 1, 2020, the law applies to businesses collecting, selling, or disclosing personal information in California. In sum, its intended purpose is to require impacted businesses to provide enhanced transparency and to give consumers the right to control their personal information. Specifically, its goal is to further a California consumer’s right to privacy by ensuring various rights including: 1) knowing what personal information is being collected; 2) knowing whether their personal information is sold or disclosed and to whom; 3) saying no to the sale of their personal information; 4) access to their personal information; and 5) equal service and price, even if they exercise their personal rights.

What Companies Are Affected?

The CCPA applies to any company doing business or with employees in California if they:

- generate $25 million or more a year in revenue;
- annually buy, receive, sell, or share personal information of 50,000 or more consumers, households, or devices for commercial purposes; or
- derive 50% or more of their annual revenue from selling consumer personal information.

Its Implications and Why It’s Important

First, several terms integral to the law’s application are given broad stroke meaning. These terms: 1) determine which organizations must comply with the law; 2) determine the scope of what is considered personal information; 3) determine whose personal information the law applies to; and 4) acknowledge personal information as an asset through a broad definition of ‘sell.’ These terms include:

1. **Business** is defined as any company that does business in California for a profit that collects personal information and that either (i) has annual gross revenue more than $25 million; (ii) annually buys, sells, receives, or shares for a commercial purpose the personal information of 50,000 or more consumers, households, or devices; or (iii) derives 50% or more of its annual revenues from selling consumer’s personal information. Note that both “sell” and “personal information” are integral parts of the definition of business.

2. **Personal information** is defined to include anything that identifies, relates to, describes, is capable of being associated with, reasonably linked, directly or indirectly, with a particular consumer or household and includes, but is not limited to, such things as:
   - Individual identifiers such as real name, alias, postal address, unique personal identifier, Internet Protocol Address, email address, account name, social security number, passport number, or other similar identifiers; Geolocation data; Biometric
Information; Internet or other electronic network activity; Audio, electronic, visual, thermal, olfactory, or similar information; Inferences that can be drawn from any of the previous information in order to create a profile; and the list goes on.

3. **Consumer** is defined as a natural person who is a California resident including by any unique identifier. (NOTE: Resident means (1) every individual who is in the state for other than a temporary or transitory purpose and (2) every individual who is domiciled in the state who is outside the state for a temporary or transitory purpose. All other individuals are nonresidents.)

4. **Sell** or variants of the word means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by one covered business to another business or a third party for monetary or other valuable consideration.

Together, these terms, along with other definitions, as applied to legal requirements under the law, result in compliance obligations for many organizations doing business in California.

**Second,** under the CCPA, the state legislature has tasked the California Attorney General with the primary responsibility to enforce its provisions. As its enforcement arm, the Attorney General has various enforcement mechanisms at its disposal. For example, this includes the ability to penalize non-compliant organizations through administrative fines upon the expiration of a 30 day notice of violation and opportunity to correct. These fines may not exceed $2,500 per violation or $7,500 for intentional violations.

More importantly, the Attorney General has the authority to decide how organizations must comply. In the above example, this could include defining what constitutes a violation. Depending on how the Attorney General defines a violation, it could result in vastly different penalties. Given that the law has just passed, it is unclear how the Attorney General will enforce the statute or determine whether a violation has taken place for a particular situation. That said, the law gives the Attorney General broad discretion to make those determinations.”

**Actions Required**

**What Companies Conducting Business in California Need to Know**

Despite an effective date of January 1, 2020, for an impacted California business to be in compliance, companies are advised to begin coordination efforts to comply far sooner than this because of the complexity of the law.

In addition to taking certain steps to be in compliance and reinforcing consumer rights regarding the privacy of personal information businesses must:

- Perform a data inventory in order to identify informational flow. Following completion, the business will need to identify issues impacting compliance and develop controls or countermeasures to address them.
- Provide California consumers with two or more methods for submitting their requests for information—including, at a minimum, a toll free telephone number.
- On its online privacy policy or policies (if in existence) or otherwise on its website, disclose a description of a consumer’s rights pursuant to this law regarding the collection, use, and sale of personal information and one or more designated methods for submitting requests, and provide a list of the categories of personal information it has collected, disclosed for a business purpose, or sold in the preceding 12 months by reference to specific categories of personal information in the law—or if the business has not done so, to disclose that fact. Information so posted must be updated at least once every 12 months.
- On its website home page, provide a link to a web page titled ‘Do Not Sell My Personal Information’ in order to allow a customer (or their agent) to opt out on the sale of their personal information to a third party. In addition to this link, the business is required to include a description of a consumer’s rights, along with a separate link to the above titled ‘Do Not Sell My Personal Information’ page in its online privacy policy or policies (if in existence) as well as any California-specific description of consumers’ privacy rights.
- Implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information.

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.
California Consumer Privacy Act: The Challenge Ahead – The CCPA’s Anti-Discrimination Clause

This is the tenth installment in Hogan Lovells’ series on the California Consumer Privacy Act.

One of the most controversial elements of the California Consumer Privacy Act (“CCPA”) is the establishment of an “anti-discrimination” right – businesses may not “discriminate” against consumers for exercising certain rights under the CCPA, and they will need to assess whether and how they can require consumers to accept certain data practices as a condition of service. Compliance would be challenging even if the provision were articulated clearly, but as we have discussed in this blog series, the accelerated drafting process and passage of the CCPA earlier this year left little time for public comment and responsive amendments. As a result, the law includes a series of ambiguities that complicate compliance, and nowhere is that more apparent than in the anti-discrimination provision.

This entry in Hogan Lovells’ ongoing series on the CCPA focuses on the law’s anti-discrimination clause, its ambiguities and potentially contradictory provisions, and impact on businesses.

1. The Prohibition on Discrimination

Section 1798.125 of the CCPA prohibits a business from discriminating against California consumers for exercising certain rights under the law. Those rights include requests to access personal information, to delete information, and to opt out of the sale of personal information.

The statutory language specifies that discrimination includes, but is not limited to:

(a) denying goods or services to consumers;
(b) charging different prices or rates for goods or services, including through the use of discounts, benefits, or other penalties;

(c) providing a different level or quality of goods or services; and

(d) suggesting that a consumer will receive a different price or quality of goods or services if the consumer exercises rights under the law.

The CCPA provides certain exceptions to the general prohibition on discrimination. Businesses may charge consumers different prices or offer different levels of service if the difference is “reasonably related to the value provided to the consumer by the consumer’s data.” The CCPA also permits businesses to offer financial incentives—including payments to consumers as compensation for the collection, sale, or deletion of personal information—if the programs are not “unjust, unreasonable, coercive, or usurious in nature,” and if businesses notify consumers of these financial incentives, obtain opt in consent prior to enrolling a consumer in a financial incentive program, and provide consumers with the opportunity to revoke consent for such programs at any time.

The language suggests that the CCPA was intended to allow businesses to offer tiered pricing or service levels so long as the differences are reasonable or supported with affirmative consent. However, as you delve deeper, the provisions for engaging in such activities require further analysis.

2. The Financial Incentive Provision is in Need of Further Clarification

The CCPA generally prohibits discrimination against those who opt out of the sale of personal information or otherwise exercise a right under the law. But the law expressly allows businesses to offer reasonable financial incentive programs on an opt-in basis, as long as consumers can opt out and withdraw consent for such programs.

If a consumer opts out of a financial incentive program, they have exercised a right under the CCPA. But can a business impose consequences for opting out of a financial incentive program to which a consumer has previously consented after being presented with the material terms of the program?

Looking at the statutory language, there is no clear answer. Although the CCPA expressly supports financial incentive programs, there is a general prohibition on discriminating against consumers for exercising their CCPA rights. So, the lawfulness of financial incentive programs may turn on whether the consequences of opting out are reasonable, as reasonableness is viewed under the CCPA.

3. The Challenge of Calculating the Value of the Data to the Consumer

Prohibited discrimination under the CCPA includes offering different prices, qualities of goods, or levels of service. But businesses are permitted to offer different prices or levels of service, if the difference is “reasonably related to the value provided to the consumer by the consumer’s data.” This leads to the question, “What is the value provided to the consumer by the consumer’s data?”

There is no single standard or process via which to measure the value of consumer data to each consumer. Are businesses supposed to gauge the value of the data to a reasonable consumer? Or must the value be assessed for each individual consumer? The value of data to a consumer may be highly context-driven. Absent clear guidance on how to calculate the value, businesses face a high degree of uncertainty.

Some have argued, including law professor Eric Goldman, that this language may have been a drafting error. And that a more appropriate measurement should be the value provided to the business, suggesting that discounts or
incentives directly related to that value provided to the business would be permitted. If the law were written this way, it would preserve commonly used discounting programs.

4. The Practical Impacts on Businesses’ Data Sharing Relationships

As discussed in our previous post, in light of the broad definition of “sale,” consumers’ right to opt out of the sale of their personal information could disrupt many existing data sharing relationships. Businesses or affiliates exchanging data about their mutual customers, even as part of a broader relationship, could potentially be viewed as engaging in a “sale” if it could be viewed as in exchange for “other valuable consideration.” Such “sale” transfers would therefore be subject to consumer opt out. And this broadly framed right to opt out of the sale of personal information, combined with the anti-discrimination provision, has the potential to significantly impact data-supported business models.

For example, a consumer could sign up for a free or discounted ad-supported version of a service and then opt out from the business’s provision of their personal data to the advertisers that make the service financially viable. But if a consumer opts out of the sale of his or her data, the CCPA’s anti-discrimination clause may prohibit the business from taking certain actions in response. And some responses would be permitted only if the difference in the level of service provided was “reasonably related to the value provided to the consumer by the consumer’s data.” As noted above, businesses are currently left wondering what that standard means and how to implement it.

5. The Anti-Discrimination Clause in Employment and the Workplace

In the context of employment, as discussed in our previous post, there is still uncertainty as to whether the California legislature intended for the CCPA to apply to employee and HR data. Employers collect personal information from employees as a necessary part of doing business.

If the CCPA does apply to employee data, employers will have to assess how they can best engage in routine data practices while respecting CCPA rights, particularly as the rights seem designed for traditional consumers. For example, many employers share employee personal information with their affiliates, in some cases for compliance or investigation functions.

Conclusion

The CCPA’s anti-discrimination provisions limit businesses’ ability to deny services, charge different prices, or offer different qualities of services to consumers who exercise their rights under the law. The drafters allowed for businesses to offer financial incentives for data practices but did not define the term “financial incentives” or more clearly lay out the conditions under which they may be allowed as compensation for the collection, sale, or deletion of personal information. And while the CCPA may be amended during the next legislative session to address its ambiguities and potential contradictions, businesses facing the challenge of CCPA compliance in the coming years will need to proactively assess and develop reasonable approaches to understanding data collection, use, and differential pricing practices for the goods and services offered to consumers.