CLASS ACTION TRENDS REPORT

CONTENTS

Data privacy: The newest class action threat

The sharp rise in data breaches in recent years has made it a business imperative for organizations to safeguard personal data, both of their customers (clients, patients, students, etc.) and their employees. Along with the growing threat comes an increasingly complex regulatory environment. This includes efforts to further regulate data privacy spreading at both the state and federal levels, as well as outside the United States. The threat also has ushered in a troubling new wave of class litigation. The stakes are high.

This issue of the Class Action Trends Report discusses the growing compliance mandates for organizations when collecting, using, storing, and sharing personal information, as well as the considerable risks at stake for breaching these requirements. We begin with the California Consumer Privacy Act (CCPA), a bellwether state law soon to take effect, with ramifications for covered businesses far beyond California.

California Consumer Privacy Act breaks new ground

By Jason C. Gavejian, Joseph J. Lazzarotti, Nathan W. Austin and Mary T. Costigan

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 have a growing appetite for more data, and more types of data, despite mounting security risks and concerns about permissible use. The California Consumer Privacy Act (CCPA) was enacted to address some of these risks and concerns.

The CCPA, which takes effect January 1, 2020, is in some ways the most expansive privacy law in the United States, and covered businesses must begin to

California Consumer Privacy Act continued on page 3

A WORD FROM STEPHANIE, DAVID AND ERIC

Supreme Court Justice Louis D. Brandeis, in a noted dissent, once wrote "The right most valued by all civilized men is the right to be left alone." While the right to privacy grew and evolved in the years since Justice Brandeis graced the Court, technological advances have moved notions of privacy beyond the personal sphere as businesses rely more and more on electronic data that contains information on an individual's residence, family, income, purchasing preferences, and other highly confidential information. Indeed, an entire industry has emerged that focuses on the sale of personal information on consumers.

Recurring stories of consumer data breaches have been commonplace. Full names, credit card numbers, and social security numbers may be revealed as the result of a breach. The consequences to the consumer and the company can be enormous. A recent study estimated a typical data breach costs a company, on average, $3.86 million.

Not surprisingly, state legislatures took note and have begun to consider consumer privacy protections. The California Consumer Privacy Act (CCPA), which takes effect on January 1, 2020, promises to be the most expansive consumer privacy law in the United States. The law contains a private right of action that could lead to classwide litigation in the event of a covered data breach.

In this issue, we will discuss the CCPA, its provisions, the private right of action under the law, and steps your organization may take to prevent liability under the Act. The suggestions cover not only litigation avoidance matters but sound business practices (e.g., the evaluation of vendor contracts, data systems access, and data storage). While there is no foolproof way to avoid a data breach, the steps outlined herein may limit any potential liability that could result.

Lastly, we discuss the likely proliferation of consumer privacy laws throughout the states. Since January 2019, at least six states have introduced consumer privacy legislation designed to protect personal data. While other states may attempt to model bills after the CCPA, the risk always exists for inconsistent obligations from state-to-state, creating an assortment of obligations with which companies may be required to comply.

Big data is big business. We believe this issue will provide you with crucial information to guide your business through this emerging area of law.

Stephanie L. Adler-Paindiris

Co-Leader • Class Actions and Complex Litigation Practice Group

David R. Golder

Co-Leader • Class Actions and Complex Litigation Practice Group

Eric R. Magnus

Co-Leader • Class Actions and Complex Litigation Practice Group

About the *Class Action Trends Report*

The Jackson Lewis *Class Action Trends Report* seeks to inform clients of the critical issues that arise in class action litigation practice, and to suggest practical strategies for countering such claims. Authored in conjunction with the editors of Wolters Kluwer Law & Business *Employment Law Daily*, the publication is not intended as legal advice; rather, it serves as a general overview of the key legal issues and procedural considerations in this area of practice. We encourage you to consult with your Jackson Lewis attorney about specific legal matters or if you have additional questions about the content provided here.

Jackson Lewis editorial team

Stephanie L. Adler-Paindiris
Co-Leader, Class Actions & Complex Litigation Practice Group

David R. Golder
Co-Leader, Class Actions & Complex Litigation Practice Group

Eric R. Magnus
Co-Leader, Class Actions & Complex Litigation Practice Group

Stephanie L. Goutos
Editorial Co-Leader, Class Action Trends Report

Kirsten A. Milton
Editorial Co-Leader, Class Action Trends Report

Brett M. Anders
Maya Atrakchi
Justin R. Barnes
Mary T. Costigan
Alison B. Crane
Jason C. Gavejian
Elizabeth S. Gerling
Jamie M. Goetz-Anderson
Nicky Jatana
Joseph J. Lazzarotti
James M. McDonnell
Tony H. McGrath
Paul Patten
Scott M. Pechaitis
Vincent E. Polsinelli
Kyle B. Russell
Sean S. Shahabi
T. Chase Samples
Christopher J. Steven

Employment Law Daily editorial team

Joy P. Waltemath, J.D., *Managing Editor* Lisa Milam, J.D., *Senior Employment Law Analyst*

Mail regarding your subscription should be sent to contactus@jacksonlewis.com or Jackson Lewis P.C. 666 Third Avenue, New York, NY 10017. Attn: Client Services. Please include the title of this publication.

CALIFORNIA CONSUMER PRIVACY ACT **continued from page 1**

prepare now to comply with the law's requirements. Even covered businesses based outside California must keep apprised of the statutory and regulatory developments that continue to unfold, as the CCPA creates a significant risk for massive classwide liability, even for inadvertent violations, and is certain to affect businesses across the United States and globally.

Which businesses are covered?

All entities that do business in California will need to comply with the CCPA, if one (or more) of the following factors are satisfied:

1. annual gross revenue in excess of $25 million;
2. 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
3. derives 50 percent or more of its annual revenues from selling consumers' personal information.

▶ For more information on which businesses would be covered, see Does the CCPA Apply to Your Business? in Jackson Lewis' Workplace Privacy, Data Management & Security Report blog.

What is "personal information"?

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. The statute sets out a non-exhaustive list of examples of personal information, such as:

- Identifiers including real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol (IP) address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- Characteristics of protected classifications under California or federal law;
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- Biometric information;
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information; and
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (FERPA).

The definition also pulls in 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. Thus, businesses that leverage artificial intelligence (AI) to help determine consumer preferences or identify preferred job candidates need to look more carefully at what must be considered personal information for purposes of CCPA.

Cookies? A cookie is a small text file that a website places on a user's computer (including smartphones, tablets or other connected devices) to store information about the user's activity. Cookies have a variety of uses ranging from

California Consumer Privacy Act continued on page 4

The GDPR is the model

Organizations familiar with the European Union's General Data Protection Regulation (GDPR), which took effect in 2018, will understand the 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. Some of the GDPR's key principles are in the CCPA. (For more background on the GDPR, see "GDPR set the course" on page 3.)

CALIFORNIA CONSUMER PRIVACY ACT **continued from page 3**
recognizing a user when the user returns to the website to provide advertising targeted to the user's interests. Depending on their purpose, the website publisher or a third party may set the cookies and collect the information.

The CCPA defines personal information to include a "unique identifier." This means "a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology... or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device." As a result, personal information collected by website cookies that identifies or could reasonably be linked to a particular consumer, family or device may be subject to the same disclosure notices and consumer rights, including the right to delete or opt out of the sale of information to a third party, as other personal information collected through the website.

Health information is excluded

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 associate governed by the privacy, security, and breach notification rules of the Health Information Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (such as medical plans, dental plans, and health flexible spending arrangements). This is welcomed news for health care providers, health plans, and their business associates. Note, however, these exceptions do not exclude these entities from the law. Thus, a health care provider might still have CCPA obligations, albeit not with respect to protected health information.

On the other hand, employee medical information that an employer receives in connection with a Family and Medical Leave Act certification, Americans with Disabilities Act reasonable accommodation, workers' compensation claims, and similar health-related employment events likely would not be subject to the CCPA to the extent they are covered under the CMIA.

Are employees "consumers"?

Whether the CCPA applies to employees and employment-related data remains an open question. On its face, the CCPA applies to "consumers," broadly defined as "a natural person who is a California resident." It does not mention employers or employees, which—along with the name of the statute itself—suggests that the legislature intended to protect the personal information of California residents in their role as consumers, and not employees.

California's longstanding protection of employee privacy rights suggests that the CCPA may extend to the personal information of California residents maintained as part of the employment relationship.

However, an example of "personal information" in the statute is "[p]rofessional or employment-related information." And, California's longstanding protection of employee privacy rights suggests that the CCPA may extend to the personal information of California residents maintained as part of the employment relationship.

Clarity may be provided in the current version of AB 25, a proposed amendment to the CCPA specifically addressing employee personal information. If enacted, AB 25 would exclude employee personal information from a number of CCPA's protections, including the right to request personal information be deleted. However, employers subject to the CCPA would be required to provide notice to employees about the categories of personal information collected and the purposes of the collection. (The exemption for employee data would not apply to the CCPA's private right of action, including suits brought as a class action.)

▶ For a closer look at the deliberations over AB 25 and the current status of the amendment, see CCPA Update—Maybe Employees Are "Consumers" After All—Employee PI is Still In Play in Jackson Lewis' Workplace Privacy, Data Management & Security Report blog.

For now, the uncertainty remains. Employers will have to wait and see if the state legislature will further amend

California Consumer Privacy Act continued on page 5

CALIFORNIA CONSUMER PRIVACY ACT **continued from page 4**

the statute, or whether the California attorney general will clarify this matter when formal regulatory guidance is issued. Regardless, AB 25 specifies that the exemption for employee data would only be effective only for the 2020 calendar year and would be inoperative on or after January 1, 2021. The one-year reprieve is to give business and consumer groups time to propose additional legislation to address concerns about employee personal information.

This issue of the *Class Action Trends Report* presumes that the CCPA will apply to employee data as provided in the current version of AB 25.

Consumer rights under the CCPA

Under the CCPA, covered businesses must provide a notice to consumers that describes the categories of personal information they collect, and how it is used. Consumers have the rights to:

- receive notice of the business' collection of consumer personal information and its processing activities, before or at the point of collection;
- receive notice of consumers rights under the statute;
- request that the business disclose or provide access to the personal information it has collected about the consumer, the business or commercial purposes for using the personal information, and the third parties with whom the business shares the information;
- request the deletion of their personal information; and
- opt out of the sale of their personal information to third parties.

To meet these obligations, businesses will need to know the data they collect about their consumers, why they collect it, and the third parties with whom they share the information. Often businesses purchase data systems "off the shelf" and aren't aware of how much data is being generated and retained. The CCPA requires them to learn more about the collection and processing of their data. Moreover, businesses might use consumer data in ways that they would prefer not to announce to the public or their competitors. Thus, they will need to think strategically about how their practices will affect disclosures they will have to make under the CCPA.

The CCPA also demands that covered businesses take steps to enable consumers to exercise these rights. For example, businesses must make available at least two mechanisms for consumers to submit requests regarding certain of their rights, including, at a minimum, a toll-free telephone number and a website address (if the business has an internet presence). Businesses generally must respond to verifiable consumer requests in writing within 45 days, and certain responses must cover the 12-month period preceding the receipt of the request.

A private right of action

The CCPA provides for fines against businesses that violate the Act, and an agency enforcement mechanism. The statute also authorizes affected consumers to bring a private civil cause of action for damages resulting from a failure to implement appropriate security safeguards which result in a data breach affecting personal information. The definition of personal information for this purpose is much narrower than the general definition of personal information under the CCPA. Consequently, with businesses continuing to be affected by data breaches, the business community is rightly concerned that the CCPA will prompt a tidal wave of class litigation. (Notably, the exemption for employee data created by AB 25, if it passes, does *not* apply to the CCPA's private right of action provision.)

California Consumer Privacy Act **continued on page 6**

"Employee" is a wide umbrella

Generally, "employee" is broadly construed under California laws. Therefore, assuming that the CCPA does apply to "employees," then its protections likely extend to personal information about job applicants, full- and part-time employees, temporary workers, independent contractors, interns, volunteers, and even dependents or beneficiaries of the "consumer" in question.

The burden is significant. Consider that for every one current employee, there were likely 20 to 50 applicants for the position. That means a lot of personal information in need of protection.

CALIFORNIA CONSUMER PRIVACY ACT **continued from page 5**

What is troubling for covered businesses is that, if successful, a plaintiff can recover statutory damages in an amount not less than $100 and not greater than $750 per "consumer," per incident, or actual damages, whichever is greater. Thus, class action lawsuits brought pursuant to this provision, even those without any harm or injury, could be very costly. The CCPA also provides for injunctive or declaratory relief, and any other relief the court deems proper.

Legislature rejects expanded right to sue. Several legislative attempts to expand the CCPA's private right of action failed. A proposed amendment to the CCPA would have given consumers the right to sue when any of their rights under the statute are violated. Senate Bill 561 did not survive—at least in this legislative session. Had it passed, SB 561 would have upset the careful balance that was struck in negotiating the CCPA as enacted. It should be noted that the California plaintiff's bar played a key role in promoting the CCPA. However, limiting the private right of action is believed to have been fundamental to the compromise that led to the CCPA becoming law. Had the provision passed, businesses would have faced significantly greater potential liability.

What to do now

The CCPA's effective date is fast approaching, and regulations being prepared by the California attorney general are forthcoming. Also, certain CCPA provisions may reach back prior to the effective date. The time to prepare is now. By taking the following preliminary measures, a covered business will be well-positioned to meet the CCPA's compliance obligations:

Map the organization's data. Identify and map consumer (including employee) personal information in the business's possession or control. CCPA compliance will require knowing what information is collected by the business, 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. Employers that use "off the shelf" employee data systems may not know the intricacies of what is being generated and stored, and where, including what data

California Consumer Privacy Act **continued on page 7**

Article III standing in data breach litigation

Currently, the hottest issue in data breach litigation is whether a demonstration of actual harm is required to have standing to sue. Standing to sue in a data breach class action suit largely turns on whether plaintiffs establish that they have suffered an "injury-in-fact" resulting from the data breach. Plaintiffs in data breach class actions often are not able to demonstrate that they have suffered financial or other actual damages resulting from a breach of their personal information. Instead, plaintiffs will allege that a heightened "risk of future harm," such as identity theft or fraudulent charges is enough to establish an "injury-in-fact."

Federal circuit courts over the past few years have struggled with this issue, in large part due to lack of clarity following the U.S. Supreme Court's decision in Spokeo, Inc. v. Robins, which held that even if a statute has been violated, plaintiffs must demonstrate that an "injury-in-fact" has occurred that is both concrete and particularized, but which failed to clarify whether a "risk of future harm" qualifies as such an injury. For example, the Third, Sixth, Seventh, Ninth, and D.C. Circuits have generally found standing, while the First, Second, Fourth, and Eighth Circuits have generally found no standing where a plaintiff only alleges a heightened "risk of future harm."

Businesses facing class action litigation following a data breach have long waited for the Supreme Court to weigh in on the issue of whether a demonstration of actual harm is required to have standing to sue. Most recently, in late March 2019, the Supreme Court rejected a petition for a writ of certiorari requesting the Court to review a Ninth Circuit decision which allowed customers affected by a data breach to proceed with a lawsuit on grounds of vulnerability to fraud and identity theft. The Supreme Court did not provide a reason for its denial of the petition.

CALIFORNIA CONSUMER PRIVACY ACT **continued from page 6**

employees are generating on the company's systems, particularly if this includes clocking data.

The CCPA covers personal information *regardless* of its format, so a detailed, thorough assessment of multiple locations is essential. Personal information can be stored in a CRM, a POS system, loyalty reward database, an electronic onboarding system, HRIS system or Active Directory; employee benefit or training records; file cabinets; file shares or backup files; a copy machine's hard drive; a manager's "desk copy"; as well as with third-party service providers such as cloud service providers, professional service providers, sales and marketing consultants, and payroll processors.

The CCPA covers personal information regardless *of its format, so a detailed, thorough assessment of multiple locations is essential.*

Build a CCPA infrastructure. Review existing organizational and technical procedures and identify additional practices required to facilitate compliance with consumer rights under the CCPA. This includes the following measures:

- Develop or identify at least two mechanisms for consumers to request information regarding what personal data the business collects, the purposes for which it is used, and the third parties with which the data is shared. Mechanisms can include an email address, postal address, website link, phone number, and so on.
- Develop internal mechanisms to respond to a consumer's exercise of access rights, including verifying their identity, responding within the mandated timeframe, and documenting the request and response.
- Develop an internal mechanism for deleting a consumer's personal information on request. This will include determining whether any state or federal laws preempt the deletion of the information in question. It also will require notifying third parties with whom the business has shared the consumer information to delete the information.
- Identify an internal mechanism to track third parties to whom personal information is sold, if applicable, in order to be ready to comply with a consumer request to opt out of that sale.
- Draft a procedure addressing applicable state and federal laws concerning record retention and destruction, and analyzing how these laws interact with the CCPA and the business' operational needs.
- Identify which staff will be responsible for handling consumer access rights and other requests under the CCPA, and determine how they will be trained.

Update website and employee handbooks as needed. Identify whether the business's website, standard employment contracts or employee handbook should be updated to include notice of collection and processing activities, as well as access and deletion rights. The business also may need to provide this information in other places, such as its intranet, applications, etc.

Review third-party service provider contracts. For third-party service providers with access to consumer personal information, revisit existing contracts with an

California Consumer Privacy Act **continued on page 8**

California Data Breach Report

In February, 2016, California Attorney General Kamala D. Harris issued the California Data Breach Report. The Report provides an analysis of the data breaches reported to the California AG from 2012-2015, and also sought to clarify the meaning of reasonable safeguards under the statutory provision above. According to the Report, an organization's failure to implement all of the 20 controls set forth in the Center for Internet Security's Critical Security Controls constitutes a lack of reasonable security. To mitigate the risk of statutory damages under the CCPA, businesses should work on getting the Controls in place. Review the business's written information security program (WISP) or internal administrative and technical policies and procedures to reflect and demonstrate compliance with these requirements.

CALIFORNIA CONSUMER PRIVACY ACT **continued from page 7**

eye to CCPA compliance. The contract should prohibit the third party from retaining, using, selling or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, or as otherwise permitted by CCPA. Third-party service provider contracts also should ensure that the vendor is able to comply with access rights relating to information collected and retained. If necessary, add provisions to address appropriate security safeguards, data breach reporting obligations, use and disclosure limitations, and data retention and disposal. This practice dovetails with the requirements of California's general breach notification law 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.

Evaluate data storage practices. Review, assess, and understand the business's existing data storage practices, and consider whether more sophisticated data governance practices are necessary to manage CCPA obligations (and consumer rights arising under other data privacy laws). Review or create a data retention schedule reflecting the types of information the business maintains.

The obligation to safeguard data, both under the CCPA and Cal. Civ. Code 1798.81.5, California's general data breach notification statute, 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. However, businesses also must consider operational and regulatory retention requirements imposed by other statutes.

Implement reasonable safeguards to protect personal information. If a business experiences a data breach affecting personal information and a lack of reasonable safeguards caused it, exposure to the CCPA statutory damages provisions can be significant. Under California law, "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

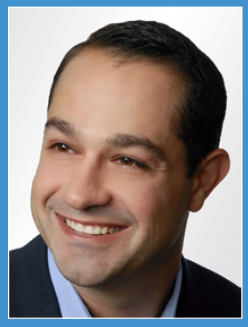
Stay abreast of ongoing CCPA changes. Monitor the status of the CCPA to ensure the organization is aware of additional amendments to the statute and the issuance of CCPA regulations. Ever since the CCPA was enacted in June 2018, it has been in a constant state of revision. Be prepared to adjust your compliance strategy accordingly.

▶ For a discussion of the CCPA's ever-changing provisions, see More Updates to the CCPA May Be Ahead in Jackson Lewis' Workplace Privacy, Data Management & Security Report blog. ■

JL focus: CCPA Team

The California Consumer Privacy Act (CCPA) is one of the most significant pieces of privacy legislation in the U.S. Effective January 1, 2020, the CCPA will affect many companies, including those headquartered outside of California, and those who do business with entities subject to CCPA. Our Privacy, Data and Cybersecurity Practice Group helps clients navigate the CCPA, including concerns with both consumer and employee data.

Joe Lazzarotti



Jason Gavejian

Please contact Joe Lazzarotti at (908) 795-5205 or Jason Gavejian at (908) 795-5139 to discuss how this may affect your company.

GDPR set the course

The California Consumer Privacy Act (CCPA) was modeled largely on the European Union's General Data Protection Regulations (GDPR). "Organizations familiar with the GDPR, which took effect in May 2018, will understand the implications of the CCPA's enactment," said Nicky Jatana, a principal in the Los Angeles office of Jackson Lewis and a member of the firm's Privacy, Data and Cybersecurity Group. "Perhaps the best known comprehensive privacy regime globally, GDPR solidified and expanded a prior set of guidelines/directives and granted individuals certain rights with respect to their personal data."

Like the CCPA, the GDPR was enacted to give individuals more control over their personal data that organizations collect, and to protect those individuals with respect to the processing of their personal data.

Like the CCPA, the GDPR was enacted to give individuals more control over their personal data that organizations collect, and to protect those individuals with respect to the processing of their personal data. The GDPR generally applies to the processing of an individual's personal data by an organization "established" in the EU or by an organization that offers goods or services to individuals living in the EU, regardless of where the business is located.

Personal data

The GDPR applies to personal data, defined broadly as "any information relating to an identified or identifiable natural person." This includes direct identifiers such as names, social security numbers and passport numbers, and indirect identifiers that alone or combined could reasonably lead to the identification of the individual such as home addresses, IP addresses, or location data. The GDPR also provides heightened protection for "special categories of data" that include data relating to race, ethnicity, religious or philosophical beliefs, trade union membership, sex life or orientation, criminal convictions or offenses, and health as well as genetic or biometric information used to identify an individual. According to the GDPR's drafters, even an employee's performance evaluation, disciplinary records, or photo could be considered personal data for purposes of GDPR compliance.

Year one of enforcement

GDPR enforcement decisions were limited during the first year as supervisory authorities concluded investigations related to infringements under the GDPR's predecessor, the EU Data Protection Directive, and initiated new investigations for infringements of the GDPR. As early GDPR investigations wound down, enforcement decisions began to trickle out this summer. Businesses can expect to see a continued increase in these decisions, particularly as individuals develop a greater understanding of their rights.

During the first nine months of the GDPR, approximately 31 percent of enforcement activity stemmed from supervisory authority investigations into self-reported data breaches. These investigations typically found not only violations of security principles but other principles as well.

Various decisions have related to employee, consumer, and client personal data in electronic, paper, and video form. Several examples of recent decisions include:

- Failing to remove information about a former employee from the company's social media page, despite the former employee's request;
- Providing an incomplete and untimely response to an employee's request to see his personal data;
- Inadvertently disclosing the name of a whistleblower to his employer, resulting in his termination;
- Failing to institute security measures to protect the usernames and passwords of primary school employees;
- Recording employees on closed-circuit television without providing the employees with information about the company's data processing;
- The publishing on-line of a printed paper list of customers that included personal data, photographed by an unauthorized individual;
- Processing customer personal data for a period

GDPR continued on page 10

GDPR **continued from page 9**

longer than necessary for the purpose for which it was originally collected and processed; failure to have deadlines for deletion of personal data in the CRM system; and failure to document data deletion procedures; and

- Processing more customer data than necessary for the purpose of payment processing.

Recent enforcement activity against U.S. companies include a U.K. notice of intention to fine a hotel chain for failing to undertake sufficient due diligence when acquiring another hotel and resort company and failing to implement appropriate security measures for its systems. This decision stemmed from a security incident Starwood experienced prior to the acquisition but which was not discovered until after the acquisition. In other activity, Greece fined an employer for using the incorrect "legal basis" for processing employee data under the GDPR, in this case, consent. This resulted in employees being misled as to the legal basis, a violation of the transparency principle. Since the employer was unable to demonstrate that it had conducted a prior assessment to determine the appropriate legal basis for processing employee personal data, it was also in violation of the accountability principle.

U.S. data protection laws post-GDPR

The GDPR's passage has spurred increased discussion about data protection in the United States. In March 2019, the Senate Committee on Commerce, Science, and Transportation held a hearing to discuss the development of a federal data protection law. While Congress has not passed a comprehensive measure yet, many key issues were raised at the hearing, such as whether a federal law would preempt existing state data privacy laws; how broad the Federal Trade Commission's regulatory authority should be; and whether the law should be sector- and technology-neutral, signaling the key points of contention likely to emerge as legislative efforts unfold. Going a step further, the U.S. Chamber of Commerce has drafted a proposed national data privacy bill.

Moreover, data protections laws are expected to continue to proliferate at the state level, particularly following the CCPA's enactment.

▶ For a more detailed discussion of the GDPR and its impact on privacy laws in the U.S., see The GDPR—One Year and Counting, in Jackson Lewis' Workplace Privacy, Data Management & Security Report blog. ■

State consumer privacy and security laws likely to proliferate

All 50 U.S. states (and the District of Columbia and Puerto Rico) have enacted data breach notification laws that require private and/or public entities to notify individuals when a security breach occurs involving their personal information. These laws typically require prompt notification to affected individuals and, in some cases, relevant government agencies. Many jurisdictions also have enacted laws creating affirmative obligations to safeguard personal information, dispose of data properly when no longer needed, and contractually obligate service providers to protect personal information.

Several states, however, have gone even further, taking the lead to expand their data privacy and protection laws to cover more than just breach notification. In 2010, Massachusetts was the first state to issue a comprehensive set of generally applicable regulations setting out specific requirements for safeguarding personal information. States such as California, Colorado, and Oregon followed. More recently, New York enacted the SHIELD Act which sets out a comprehensive set of safeguard requirements applicable to businesses in the state.

▶ For more information about the New York statute, see New York Enacts the SHIELD Act in Jackson Lewis' Workplace Privacy, Data Management & Security Report blog.

In response to the privacy protections enacted under the CCPA, since the beginning of 2019, at least 14 state legislatures have introduced privacy laws mirrored largely on CCPA and GDPR principles. Some of these bills are much more limited than the CCPA. For example,

STATE CONSUMER PRIVACY, SECURITY LAWS continued on page 11

STATE CONSUMER PRIVACY, SECURITY LAWS **continued from page 10**

Maine recently passed An Act to Protect the Privacy of Online Consumer Information, which applies only to internet service providers. Similarly, Nevada's law is aimed at operators of internet websites or online services that collect "personally identifiable information" from consumers in order to sell it to a third party without consent.

Conversely, other bills propose more stringent requirements than the CCPA. A bill introduced in Maryland, for example, would provide a more extensive "right of deletion" (popularly known as the "right to be forgotten") than under the CCPA, and prohibits discrimination against a consumer for exercising his or her rights and financial incentives for processing personal information. Massachusetts legislation, if passed, would grant a private right of action if a consumer's personal information is improperly collected; consumers may not have to demonstrate actual harm to seek damages.

Both public and private businesses must adopt measures to ensure that they are compliant with the various privacy and security laws that may apply to them.

▶ The Massachusetts bill is discussed in detail in Proposed Legislation in Massachusetts Would Create Private Right of Action for Improper Collection of Personal or Biometric Information in Jackson Lewis' Workplace Privacy, Data Management & Security Report blog.

It is important to note that while over a dozen state legislatures are considering consumer data protection laws, most are still in early stages of the legislative process, will continue to be amended, and not all will be enacted into law.

New York considers a stiffer measure

It was only a matter of time before New York introduced its own law. The New York Privacy Act (NYPA) is a more expansive version of its California counterpart and is distinct from the CCPA in significant ways. For example, while the CCPA applies only to businesses with a threshold of $25 million annual revenue, the NYPA applies broadly to "legal entities that conduct business in New York" or that produce products or services that "intentionally target" New York residents. That means small-to-medium size businesses are more likely to be covered, and potentially even non-profit organizations will be subject to the law's privacy and security obligations. The New York measure also includes a right to rectification in the event of a breach, unlike the California law. The right to rectification provides the consumer with the right to have personal data about him or her corrected if it is inaccurate or incomplete.

The state's attorney general may bring an action in the name of the state or on behalf of its residents. A private right of action is also available to any person injured by a violation of the law—promising a surge of litigation if passed, including class actions. This is arguably the most significant difference from the CCPA, which provides for a private right of action only in cases where there has been a data breach. The NYPA is still very early in the legislative process—it is currently in the Senate's Consumer Protection Committee, and will not be considered, if at all, until the 2020 Legislative Session. Regardless of how the New York measure fares as it makes its way through the legislative process, such an aggressive bill signifies the seriousness with which New York is considering privacy and security matters.

A patchwork of compliance requirements

This surge in legislative activity, combined with the growing public awareness of data privacy rights and data security obligations, makes development of a meaningful data protection program an essential component of business operations. Moreover, the varied coverage standards and data protection requirements from state to state presents a challenge to organizations that conduct business or employ individuals in multiple jurisdictions. Both public and private businesses must adopt measures to ensure that they are compliant with the various privacy and security laws that may apply to them.

The compliance challenges for affected organizations will only increase as more states enact their own privacy

STATE CONSUMER PRIVACY, SECURITY LAWS **continued on page 12**

STATE CONSUMER PRIVACY, SECURITY LAWS **continued from page 11**
and security laws—laws that are inconsistent and often include mutually exclusive requirements. With the passage of each state law, it is increasingly apparent how complicated this patchwork of state legislation will become for covered businesses.

This state-level activity could prompt Congress to move more quickly with one of its own proposed federal bills. The latest is the Data Care Act, which proposes to hold large tech companies (*i.e.*, "online service providers") responsible for the protection of personal information. A federal approach to consumer privacy, particularly legislation with preemptive reach, would likely ease the compliance challenge for U.S. businesses seeking to ensure the personal information in their possession or under their control is protected while avoiding legal liability in an increasingly complex legal landscape. ■

Prevention pointer: Avoiding data breaches

While states currently appear focused on consumer privacy measures, an earlier surge of legislative activity took aim at a sharp rise in data breaches. As a result, there are data breach laws already on the books in every U.S. jurisdiction. Data breaches are more than a growing liability concern—although they are certainly that, especially given that such incidents often wreak havoc in a manner that invites class litigation—they also pose a significant threat to an organization's operations, exposing businesses to significant business interruption losses. Businesses must implement rigorous data security measures both to avoid legal risk and to safeguard a company's own data and systems.

"The challenge is trying to adapt to the lightning-fast demands of the business world, where everything has to be done instantly," noted Jeffrey M. Schlossberg, Principal in the Long Island office of Jackson Lewis and a Certified Information Privacy Professional (CIPP). "You're trying to give your employees as much access as possible on a 24-7 basis, but sometimes employers don't have the proper protocols in place to protect the data that could be accessed when employees are using their remote devices."

The compliance challenge is exacerbated by a confusing web of data breach laws. "These laws can vary in significant ways—such as how personal information and breach is defined, whether there are exceptions to notification, whether identify theft resolution services should be provided, does a state agency have to be notified, and requirements for notice content and the deadline for providing same" Schlossberg explained. "So for breaches affecting residents in multiple states, businesses have to understand which laws apply and the specific provisions of each."

Small and medium-size businesses may assume that hackers would rather set their sights on large national companies with valuable credit card data and other sensitive information to poach. "But *every* business has data that a hacker would be interested in getting," according to Mary Costigan, another CIPP-certified member of Jackson Lewis' Privacy, Data and Cybersecurity Practice Group. "Every business has personal information of individuals, even it only pertains to the businesses employees and their social security numbers."

To help minimize the risk of a data breach, Schlossberg recommends the following preventive measures:

- Implement protocols to protect data and develop a written data security program. Effective baseline policies and practices include prohibiting employees from logging on to the organization's business network from unsecured networks, such as free wifi at the local coffee shop. Company systems should be accessed through a secure remote app.
- Many employers have a bring-your-own-device (BYOD) policy which enables employees to access company

PREVENTION POINTER continued on page 13

Other class action developments

Courts, not arbitrators, decide availability of class arbitration. Agreeing with its sister circuits, the Fifth Circuit Court of Appeals held in a matter of first impression that class arbitration is a gateway issue that must be decided by the courts, not by an arbitrator, *unless* an arbitration agreement contains clear and unmistakable language to the contrary. The Fourth, Sixth, Seventh, Eighth, Ninth, and Eleventh Circuits have held that class arbitrability is a gateway issue for courts, not arbitrators. Agreeing with the other circuits, the Fifth Circuit concluded that class arbitration substantially changes the nature of an arbitration, and thus it is an issue of arbitrability. Specifically, class arbitration jeopardizes some of the perceived benefits of arbitration—cost, efficiency, and privacy—because of the due process requirements to notify unnamed class members and allow them an opportunity to be heard. The court then addressed whether the arbitration agreement at issue in this case "clearly and unmistakably" allowed the arbitrator to decide whether the employees could proceed as a class. Finding no such language, the court reversed and remanded one lower court decision, and vacated and remanded another, in a ruling on consolidated appeals.

OTHER CLASS ACTION DEVELOPMENTS continued on page 14

PREVENTION POINTER continued from page 12

information on their own smart phones and laptops. The organization's IT department must retain the ability to control information even on an employee's personal phone, zip drives, and the like, including the right to swipe data in the event the employee's phone is lost.

- Train employees on data security: how to recognize phony emails (phishing attempts); what to do if they lose their mobile phones; and the importance of robust passwords in deterring inadvertent or purposeful attacks.
- Conduct regular, thorough data security assessments, evaluating physical risks such as where the company's back-up systems are located; administrative protocols regarding who has access to data; and password protection policies. For example, back-up data storage should be located at a different site, to guard against total loss in a natural disaster. Risk assessments should be customized to the company and their specific systems.
- Carefully consider which employees need access to highly confidential information, and provide access only to those individuals.
- Ensure collaboration between the business unit, IT, and human resources. "Everybody has a role," Schlossberg said. "HR needs to ensure the employer has the right policies in place and that employees are properly trained."
- Draft a data breach plan in the event the organization's data is compromised. Be prepared to respond immediately and comply with applicable breach notification laws. Prepare data breach notification templates in advance of any breach.

▶ See Schlossberg's discussion of data breaches and strategies for avoiding them at JL Live: Privacy Issues and Data Breaches.

The aftermath of a data breach

A prompt response is critical when a data breach occurs. The Jackson Lewis Privacy, Data and Cybersecurity Practice Group's 24/7 Data Incident Response Team assists employers in effectively responding following a breach incident.

The team will assess the level of the breach and how expansive it was; identify the kind of information that has been compromised; and help employers meet their obligations under the applicable federal and state laws, such as who must be notified and the required timeframe for notification.

OTHER CLASS ACTION DEVELOPMENTS continued from page 13

Courts can't review settled attorneys' fees. In a 2018 decision, the Eighth Circuit Court of Appeals addressed the standard for reviewing attorneys' fees in negotiated Fair Labor Standards Act (FLSA) settlements "under the assumption that district courts have authority to review them." Picking up where it left off, the appeals court recently held that courts have *no* authority to review settled attorneys' fees under FLSA Section 216(b). While there may be sound policy reasons for judicial oversight of the amount employees stand to recover in a wage-hour settlement, "the amount the employer pays to the employees' counsel has no bearing on whether the employer has adequately paid its employees in a settlement," said the appeals court. The ruling was issued in a proposed overtime collective action under the FLSA and class action under the Arkansas Minimum Wage Act. In reviewing the parties' proposed settlement, the district court had erroneously modified the attorneys' fee provision.

A coalition of 50 attorneys general has reached the largest data breach settlement in history with a consumer credit reporting agency following an investigation into a massive 2017 data breach that exposed the personal information ... of more than 147 million consumers, or 56 percent of U.S. adults.

Federal *de minimis* doctrine does not apply in California. Non-exempt retail employees can no longer be required to undergo "off the clock" exit inspections without compensation for such time, ruled the Ninth Circuit Court of Appeals in reversing and remanding a contrary ruling by a district court in a class action wage suit under California law. The appeals court concluded that the 10-minute threshold for a *de minimis* finding under federal law is inconsistent with the state's labor laws in light of a California Supreme Court ruling that the federal *de minimis* doctrine does not apply to claims for unpaid wages under California Labor Code Sections 510, 1194, and 1197. Following this decision, an employer that requires its employees to work minutes off the clock on a regular basis or as a regular feature of the job may not avoid the obligation to compensate the employee for that time by invoking the *de minimis* doctrine.

RIFs are subject to disparate impact review. A divided panel of the District of Columbia Circuit Court of Appeals held that a Title VII discrimination claim arising from a reduction in force (RIF) is subject to disparate impact review. The plaintiffs in the case had alleged that their municipal employer, in implementing a RIF in the face of a budget shortfall, eliminated the job categories in which African Americans were most densely concentrated. The employer argued that the RIF decisions were not subject to scrutiny under Title VII for disparate racial impact because the employees failed to identify a specific employment practice that was actionable under a disparate impact theory. The layoff decisions did not involve an objective "test or requirement," according to the employer but, rather, a series of individual subjective, contextual judgments. The district court agreed that a RIF is not a "particular employment practice" for purposes of analyzing disparate impact. However, the D.C. Circuit explained that "an employer's assertion that the firings were a 'RIF' required by budget cuts does not somehow immunize them from Title VII scrutiny." The appeals court reversed a grant of summary judgment in the employer's favor on a class action race discrimination suit alleging both disparate treatment and disparate impact discrimination.

State AGs obtain $600M data breach settlement. A coalition of 50 attorneys general has reached the largest data breach settlement in history with a consumer credit reporting agency following an investigation into a massive 2017 data breach that exposed the personal information (Social Security numbers, names, dates of birth, addresses, credit card numbers, and, in some cases, driver's license numbers) of more than 147 million consumers, or 56 percent of U.S. adults. The deal includes a consumer restitution fund of up to $425 million, a $175 million payment to the states as a fine, and significant injunctive relief for consumers, including free credit-monitoring services for up to 10 years and identity theft insurance available (at no deductible) to

OTHER CLASS ACTION DEVELOPMENTS continued on page 15

OTHER CLASS ACTION DEVELOPMENTS **continued from page 14**
cover identity recovery expenses and legal costs. The settlement requires court approval.

$102M for California wage violations. A federal court in California awarded nearly $102 million in a class action suit alleging a global retail chain violated the California Labor Code's wage statement and meal period provisions. The court had certified three classes: (1) a meal period class of workers who received meal period premiums that did not factor in nondiscretionary compensation, including incentive pay earned; (2) an overtime/incentive wage statement class of workers who claimed their quarterly incentive bonuses should have been factored into the calculation of their regular rate; and (3) a final wage statement class of former employees. The retailer was assessed $70,000 in PAGA penalties for the meal period violations; statutory damages of $48,046,000 for violations of California's itemized wage statement requirement, an additional $48,046,000 in PAGA penalties for those; and an additional $5.8 million in PAGA penalties for violating the final wage statement provisions. In the end, of the damages awarded, more than half are PAGA penalties.

A federal court in California awarded nearly $102 million in a class action suit alleging a global retail chain violated the California Labor Code's wage statement and meal period provisions.

Hourly bank employees to get $35 million. A class of non-exempt bank employees will share in a $35 million settlement after a federal court in New Jersey signed off on the parties' deal to resolve their collective and class action overtime claims. In addition to the FLSA collective action, the court certified seven subclasses of bank tellers alleging that the defendant, a national banking industry giant, also violated state wage laws by forcing personal bankers at branches nationwide to work off-the-clock outside of regular bank branch business hours, soliciting new accounts at family gatherings, social events, the gym and through personal contacts in order to meet their quarterly quotas. Several plaintiffs alleged that they also were forced to work at the branch during lunch hours, and after hours, without pay, including participating in mandatory "call nights" at least one night per week soliciting new accounts and selling financial products such as credit cards by phone. The plaintiffs contended that the bank had a nationwide policy of knowingly requiring unpaid overtime work and instructing employees not to record their overtime hours.

Tech giant to pay $11 million to end ADEA action. A technology company would pay $11 million to resolve allegations that it engaged in systemic age discrimination against a class of applicants age 40 and older for jobs as site reliability engineers, software engineers, and systems engineers. A settlement reached between the parties also provides programmatic relief, including manager training on age discrimination; creation of a subcommittee in recruiting to focus on diversity in the positions at issue; ensuring that marketing materials reflect age diversity; ensuring adequate investigations of age bias complaints; and surveying departing employees about discrimination. The court certified an Age Discrimination in Employment Act (ADEA) collective in 2016, and 262 individuals opted in. Of the remaining 234 class members, 227 signed off on the agreement. The average gross recovery is said to be more than 80 percent of the estimated actual damages suffered during the relevant timeframe, not including potential liquidated damages. Plaintiffs' counsel will receive 25 percent of the $11 million settlement in fees ($2.75 million) and out-of-pocket expenses, if the agreement wins court approval.

$7.4M deal resolves suit over ACA mandate dodge. In one of the first lawsuits of its kind alleging that an employer cut employee work hours in order to skirt Affordable Care Act (ACA) health coverage requirements, a federal court in New York gave final approval to a $7.425 million settlement resolving a nationwide ERISA class action against a national restaurant chain. The plaintiffs alleged that the employer drastically cut their work hours in order to reduce them from full-time to part-time status and avoid having to provide them with

OTHER CLASS ACTION DEVELOPMENTS **continued on page 16**

OTHER CLASS ACTION DEVELOPMENTS continued from page 15

health insurance under the looming ACA employer mandate (which requires covered employers to offer health coverage to full-time employees). The suit was brought by a long-term employee whose schedule was reduced to an average of 17.43 hours per week pursuant to a companywide "Position to Win" program, and who was formally notified that she was now on part-time status, meaning her insurance coverage would be terminated. (At her location, the full-time workforce was cut from 100 employees to 40.) More than 2,000 current and former employees nationwide will recover from the settlement fund proportionally based upon their documented losses as a consequence of having their hours cut and their health benefits eliminated. In addition, the settlement includes injunctive relief barring management from reducing employees' hours or discharging them for the purpose of denying health coverage.

More than 2,000 current and former employees nationwide will recover from the settlement fund proportionally based upon their documented losses as a consequence of having their hours cut and their health benefits eliminated.

Settlement awards $6.2 million to female sales reps. A class of 671 current and former female sales representatives of a drug manufacturer will share a $6.2-million settlement after a federal court in New Jersey approved a deal to resolve their gender discrimination claims under Title VII, the Equal Pay Act, Family and Medical Leave Act, ERISA, and New Jersey law. According to the employees, the employer tried to force pregnant employees to quit outright rather than take maternity leave, and instituted an incentive plan that connected sales reps' compensation to the sales of their colleagues. They alleged that this discouraged employees from working with women who might become pregnant and take maternity leave and led to women being excluded from social and networking events, creating a "boys' club" atmosphere.

Automaker must defend ADEA collective action. A federal court in Tennessee has conditionally certified a collective action under the ADEA on behalf of workers 50 years of age or older at an auto manufacturer's plant in Chattanooga, Tennessee. The plaintiff, a 54-year-old manager, was transferred and demoted three days after the company unveiled its new efficiency program, "Pact for the Future." The program aimed to eliminate 30,000 jobs worldwide, partly through attrition and retirements. A press release from the CEO discussed early retirements, stated that the changes would affect operations worldwide, and appeared to imply that the company had a new focus on younger workers, stating: "We are expecting our management levels to become younger and slimmer." The employer argued that the plaintiff failed to show the putative class members were similarly situated because he proffered nothing more than discrete employment actions against four declarants without a "common unifying nexus" or "unified policy tying individual claims together." But the court concluded that the Pact for the Future was just such a policy. In a subsequent ruling, the court denied the employer's motion for partial judgment on the pleadings as to the plaintiff's class claims under the Tennessee Human Rights Act, finding it was not clear from the face of the complaint that he would be unable to satisfy Rule 23's requirements. ■

On the JL docket

Mark your calendars for these timely and informative Jackson Lewis events:

September 17-18, 2019	2019 SAHRA Conference (McClellan, CA)
September 17, 2019	Colorado's New Equal Pay for Equal Work Act—Are You Ready? (Colorado Springs, CO)
September 18, 2019	What to Expect When Your Employee is Expecting: The New Pregnancy Rules (Reston, VA)
September 19, 2019	Cybersecurity Risks and Fears for Retirement Plan Sponsors (Warren, NJ)
September 23-24, 2019	Remaining Union Free: A Counter-Organizing Simulation Preparing Your Team in 2019 (Las Vegas, NV)
September 24, 2019	Taking Control of the Workplace Law Landscape: Minnesota Conference Series (Bloomington, MN)
September 25, 2019	Colorado's New Equal Pay for Equal Work Act – Are You Ready? (Denver, CO)
September 26, 2019	Third Avenue Breakfast Briefing (New York, NY)
September 26, 2019	Conducting Effective Workplace Investigations (Cleveland, OH)
October 15-16, 2019	Remaining Union Free A Counter-Organizing Simulation Preparing Your Team in 2019 (Chicago, IL)
October 16, 2019	Taking Control of the Workplace Law Landscape: Minnesota Conference Series (Mankato, MN)
October 21-22, 2019	Restoring the Balance: Bargaining to Win for Unionized Employers (Chicago, IL)
October 23, 2019	Focus on Connecticut: Harassment Education and Training (Hartford, CT)

*Watch for news on important developments affecting class litigation on Jackson Lewis' **Employment Class and Collective Action Update** blog!*