Locke Lord LLP

PRIVACY & CYBERSECURITY NEWSLETTER

AUGUST 2019

IN THIS ISSUE

Practical Wisdom, Trusted Advice.

www.lockelord.com

GDPR Enforcement - The Experience So Far

by Andrew Shindler

Introduction

In 2018, GDPR compliance was a main focus for many organisations around the world. GDPR enforcement is likely to continue to grab the headlines in 2019 and beyond.

At the end of January, the EU Commission reported that over 95,000 data protection complaints had been filed with data protection authorities in the first eight months of GDPR. During that same period, organisations self-notified over 40,000 personal data breaches, a massive increase compared to the pre-GDPR figures.

As is probably well known by now, the penalties for breaching the GDPR, which apply to any organisation with an establishment within the EU or which markets to or monitors individuals in the EU from outside it, can be enormous. The maximum being a fine of €20 million and 4% of world-wide group turnover, whichever is higher.

Enforcement Action - Penalties

Inevitably there is a material time-lag between the GDPR having come into force, complaints having been made and investigated and penalties issued to organisations. Indeed, since GDPR, most of the penalties which have been issued by authorities have been under the previous law, such as the UK ICO's record fine of £500,000 issued to Facebook in October for data protection breaches which took place between 2007 and 2014.

CCPA CORNER

Our Privacy & Cybersecurity Practice Group has organized a CCPA Initiative of lawyers in various offices throughout our Firm to work with clients on CCPA compliance. We are developing templates and checklists that will be available for a fixed fee in the coming weeks. If you would like to talk with a member of our CCPA Initiative, and to learn more about our CCPA templates and checklists, please contact:

Theodore P. Augustinos ted.augustinos@lockelord.com or 860-541-7710

Molly McGinnis Stine mmstine@lockelord.com or 312-443-0327

Owing to this time-lag, the first GDPR penalties have only recently started to emerge. The first major penalty was issued by the Portuguese DPA, which fined a hospital €400,000 for breaching the GDPR's data security requirements. The German DPA followed closely, issuing a fine of €20,000 for a similar breach – the significant difference being the level of co-operation between the organisation and the authority.

A recent report calculated total GDPR fines at around €239 million to date. The French Authority, CNIL imposed €50 million fine on Google LLC, resulting from a finding that Google had breached GDPR by providing insufficient transparency and inadequate information as to its data processing, and not obtaining valid consent regarding personalized advertising. In July, British Airways and Marriott were notified of potential fines following security breaches. Click here for more.

CNIL levied the fine against Google despite recognition of Google's efforts to put appropriate policies and notices in place – this was not a case of Google ignoring GDPR, but rather of CNIL finding that Google's compliance steps were insufficient. Google has not accepted this and has appealed.

GDPR fines must be proportionate, so it is worth looking at why CNIL imposed such a large penalty. It considered that Google had violated some of the basic data protection principles; that the violations were continued and, given the massive and intrusive collection of personal data, that they were severe. In addition, Google's model is based on the value of users' personal data from which it obtains benefit and it occupies an important position on the operating system market.

Looking Forward

With limited experience of GDPR enforcement so far, we remain at the early stages. The issues to be monitored going forward include:

- How strictly data protection authorities will interpret the GDPR's provisions where there are grey areas?
- What types of non-compliance will be regarded as most serious?
- How much will a business's good faith efforts to comply be taken into consideration in assessing penalties?
- How large will fines be?
- Will there be a consistent approach across data protection authorities in different EU countries?
- Will data subjects bring private claims for compensation, as opposed to complaints to the authorities?

GDPR – Extra-Territoriality Revisited

By Andrew Shindler

Introduction

Although seemingly simple on its face, the test for determining whether an organization is subject to the European Union's stringent data protection laws, the GDPR, continues to confound.

In this article, we examine the situation of insurance companies and universities based in the United States with no European presence that wish to communicate with their customers and alumni now residing in Europe. Is this communication enough to subject them to the rigorous standards of GDPR?

The GDPR's Territorial Test

Article 3 of the GDPR sets out a deceptively simple-sounding territorial test. Broadly, it applies to organizations by one of two criteria:

the "**establishment criterion**" - where the organization is "established" in the EU and processes personal data in relation to that establishment, regardless of where the individuals are located and where the processing takes place; or

the "**targeting criterion**" - where the organization is not established in the EU, but processes personal data of individuals physically located in the EU in relation to intentionally offering them goods or services or monitoring their behavior in the EU.

Establishment

Where an insurance company has an "establishment" in the EU, such as a subsidiary, branch or office, or where a university has a campus other physical presence in the EU, one can see the clear logic of GDPR applying to the personal data processing activities of that establishment. This, the establishment criterion, is not the subject of this article, although it is worth noting that where GDPR applies, this criterion is not limited to the processing carried out by the EU establishment - the GDPR is also likely to extend to at least some the processing activities of the U.S. parent.[1]

Targeting

Under the targeting criterion, there is a sound rationale for the GDPR to apply to cases where a U.S. company proactively offers its goods or services to EU residents to grow an international market or where the U.S. company monitors the behavior of EU residents to monetize advertising to be targeted at them.

However, what of the case of an insurance company based solely in the U.S. that markets solely within the U.S. for customers? There is a chance that some percentage of its insureds may later move to the EU. There is also the chance that the insurer may not be aware of such moves, and may continue to retain only an electronic address to contact customers about renewals and offers of new products. Likewise, offers to customers may also available on the insurer's website, hosted in the U.S. but accessible globally.

Similarly, consider a U.S.-based university with no European campus or office, which does not actively solicit applications for students from outside North America. Universities may also keep in touch with its many thousands of alumni, primarily by email and its website, offering them overseas trips, branded leisure-ware and other merchandise. Some of the alumni may move to the EU where they continue to receive these offers.

The question, in both cases, is whether GDPR applies to the organisations processing of the personal data of these EU based individuals.

These Individuals Are Not EU Citizens Or Residents, So How Can GDPR Apply?

One of the first myths to dispel is that GDPR only protects EU citizens and residents. As the European Data Protection Board (EDPB), which is comprised of representatives of the national data protection authorities, points out in its recent guidelines on territorial scope,[2] the targeting criterion refers to "*data subjects who are in the EU*". Therefore, the application of GDPR "*is not limited by the citizenship, residence or other type of legal status of the data subject*".

The determining factor under the targeting criterion is the data subject's actual physical location. This is assessed at the moment the trigger activity takes place, being the moment the goods or services are offered.

This seems to apply GDPR to the examples above: the relevant customers and alumni are located in the EU when the offers are made. In fact, on this basis it will even apply to customers and alumni who just happen to be in Europe on vacation or a short business trip when an email or text containing an offer is sent to them.

Website Offers

In the examples above, various customer and alumni offers are available on the insurer's or the university's U.S.-based websites, which are readily accessible from the EU.

Here, the position is relatively clear, the mere accessibility of a U.S.-based website from the EU does not trigger GDPR. GDPR is only triggered where the U.S.-based website's features or content show that there is an intent to offer goods or services to EU individuals, such as by quoting prices in an EU currency, making it possible for users to order in an EU language other than English, providing a dedicated address or phone number to be reached from an EU country, offering delivery to an EU country or mentioning customers in the EU. This is specifically stated in Recital 23 of GDPR.

Therefore, so long as there is no content on the websites clearly aimed at the EU, U.S.-based insurers and universities can operate their websites without being subject to GDPR, even though EU-located customers and alumni may access and place orders on the site.

Individual Offers

The test for websites, referred to above, is the only example the GDPR gives of whether "*it is apparent that the controller … envisages offering services to data subjects …in the Union.*" The GDPR says nothing on this point about offers made other than via websites.

So the position is less clear for offers targeted to individuals. In our examples, the customers and alumni are physically located in the EU when they receive an offer by email, mail or other means. This offer has been intentionally and actively sent to the individuals concerned, unlike a website which is mainly passive, only

1 If the activities of the local EU establishment are "inextricably linked" to the U.S. parent's data processing, that processing will be covered by GDPR.

2 Draft guidelines 3/2018 on the territorial scope of GDPR (article 3) adopted 16 November 2018

receiving orders. Is this not targeting of individuals in the EU where they are so located?

Recent guidelines of the EDPB, which carry much weight, have attempted to provide clarity. The guidelines underscore that mere data processing of EU individuals is not enough to trigger GDPR, there must also be "targeting. But this was already stated in the GDPR. So the question remains as to what this means in practice. The guidelines give one relevant example:

> *A U.S. citizen travels through Europe during his holidays. While in Europe, he downloads and uses a news app that is offered by a U.S. company. The app is exclusively directed at the U.S. market. The collection of the U.S. tourist's personal data via the app by the U.S. company is not subject to the GDPR.*

In this example, the news app is "exclusively directed at the U.S market". Presumably this mean that it was only sent to people the U.S. company believed were located in the US or it only intended to send it to such persons. The question therefore comes back to intention: did the conduct of the data controller demonstrate an intention to offer goods or services to individuals in the EU?

In answering this question for U.S.-based insurers and universities, it must be strongly arguable that, where an offer of products or services is sent to all or whole categories of customers or alumni, then the fact that a minority of them may be located in the EU does not invoke the application of GDPR, because there was no intention to send the offer to people in the EU – a subset of the recipients merely happened to be there. The argument is strongest when there is no actual knowledge that the individuals are in the EU, for example where the only record is an email address without an EU-specific Top Level Doman (TLD) such as "co.uk".

The argument is weaker where the offer is sent to an EU-specific TLD or to a physical EU mailing address. Nevertheless, a U.S.-based insurer or university might still succeed to avoid triggering GDPR on the basis that the mailing is on an automated mass basis with no intention to direct the offer to those located in the EU, but that sending the communication to the EU-located recipient was simply an oversight. The question then becomes how much due diligence was or should have been done to identify individuals in the EU.

It seems that the greater the knowledge of the U.S.-based entity that particular customers or alumni are located in the EU, the more likely it is to trigger GDPR if it sends them offers. Where the U.S.-based insurer or university knows or reasonably believes it likely that is has some customers or alumni in the EU – other than those who might merely pass through on vacation – it has a number of options, such as:

- undertaking a GDPR compliance exercise;
- removing from its mailing list for offers any customers or alumni which have EU email or mailing addresses or which it otherwise knows are living in the EU;
- inviting customers and alumni to notify it whether they are in the EU and, if so, to remove them from the relevant mailing list as above; or
- taking the view that while there will always be some recipients of its communications in the EU, it is not targeting the EU deliberately so GDPR does not apply - and then wait to see if any enforcement action is taken.

The last option carries the most risk. If a complaint is made and GDPR found to apply, the sanctions could include heavy fines. If taking that approach, it is therefore highly advisable to take advice on and respect the key principles of GDPR when dealing with EU individuals' data in order to reduce exposure. This will include keeping the data secure, not transferring it to third parties or using it for any purpose which could harm the individual.

No Sale! Nevada Consumers May Opt Out of Personal Data Sales

By: Laura L. Ferguson and Sean Kilian

With the recent passage of SB 220, Nevada has become the latest state to regulate consumer privacy online by allowing individuals to opt-out of certain sales of their information. Although SB 220 is not a comprehensive data privacy law similar to the California Consumer Privacy Act (CCPA), it creates important new consumer rights and business obligations. Covered businesses may need to undertake a substantial effort to comply with the law prior to its October 1, 2019 effective date. However, as stated below, businesses should review the law carefully, because the rights and obligations it creates apply to a fairly limited set of transactions.

Who does the new law apply to?

SB 220 imposes new obligations on "operators" of websites. In sum, under existing law (NRS 603A.330), an "operator" is a person who:

1. Owns or operates a website or online service for commercial purposes; and
2. Collects and maintains "covered information" from consumers who reside in Nevada and who use or visit the website or online service.

SB 220 narrows the definition of an operator by excluding: (a) financial institutions that are subject to the Gramm-Leach-Bliley Act; (b) entities that are subject to HIPAA; and (c) certain manufacturers and repairers of motor vehicles.

What information does the new law cover?

The rights and obligations created by SB 220 pertain to "covered information" collected by operators, which is also defined by existing Nevada law. NRS 603A.320. "Covered information" includes:

1. A first and last name;
2. A home or other physical address which includes the name of a street and the name of a city or town;
3. An electronic mail address;
4. A telephone number;
5. A Social Security number;
6. An identifier that allows a specific person to be contacted either physically or online; and
7. Any other information concerning a person collected from the person through an operator's website or online service and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable.

What consumer rights does the law create?

SB 220 allows consumers to direct operators not to make any "sale," as defined, of any covered information the operator has collected or will collect about the consumer. Operators might be familiar with the existing Nevada requirement to provide notice to consumers of the categories of covered information the operator collects through its website or service. NRS 603A.340. SB 220 expands on this requirement by allowing consumers to opt out "sales" of such information.

A potential challenge for operators is determining what activities count as sales. SB 220 defines a "sale" as the "exchange of covered information for monetary consideration by the operator to a person for the person to license or sell the covered information to additional persons." This definition, which is fairly narrow relative to other data privacy laws, is also subject to several exceptions. The term "sale" does not include an operator's disclosure of covered information to:

1. A person who processes covered information on behalf of the operator;
2. A person with whom the consumer has a direct business relationship for the purposes of providing a product or service requested by the consumer;
3. A person for purposes which are consistent with the reasonable expectations of a consumer considering the context in which the consumer provided the covered information to the operator;
4. An affiliate of the operator; or
5. A person, where the covered information is an asset that is part of a transaction where the person assumes control of the assets of the operator.

What obligations does the new law create for businesses?

SB 220 creates three new obligations for covered businesses.

First, operators must establish a "designated request address," through which a consumer may submit an opt-out request. The designated request address must be either an email address, a toll-free phone number, or a website.

Second, operators who receive opt-out requests from consumers must cease making sales of any covered information that the operator has collected, or will collect, about the consumer. Operators need act only on "verified requests," which are requests submitted to the designated request address, and for which the operator can reasonably verify the authenticity of the request and the identity of the consumer.

Third, operators must respond to verified requests within 60 days of receipt. When reasonably necessary, the operator may extend the 60-day response deadline for up to 30 days by notifying the consumer.

What mechanisms are available to enforce the new law?

Notably, SB 220 does not create a private right of action against an operator. Instead, it extends the current remedies available under existing Nevada law related to the enforcement of the consumer notice requirement described above. The Attorney General may enforce the law by seeking either a civil penalty of up to $5,000 per violation, or injunctive relief.

What should I do now?

Businesses that are covered by SB 220 should first create and study their data inventories and determine what data transfers might constitute a "sale" from which a consumer may opt-out. If a business is selling data within the meaning of SB 220, it should review and update its privacy policies to address how the business will review and respond to opt-out requests, create a designated request address, and prepare to process consumers' verified opt-out requests beginning October 1, 2019.

Biometrics: Illinois Supreme Court Allows No-Injury Biometric Information Privacy Act Claims in Complete Victory for Plaintiffs' Bar

By: P. Russell Perdew and Michael McGivney

On January 25, 2019, the Illinois Supreme Court held that plaintiffs can assert claims and recover statutory damages under Illinois's Biometric Information Privacy Act (BIPA) based on a bare violation of the statute without any showing of consequential harm. *Rosenbach v. Six Flags*, 2019 IL 123186. This question had split Illinois appellate courts over the last two years. The Court's decision will likely prompt filing of even more BIPA class actions; over a hundred have already been filed over the last two years in Illinois and elsewhere. And, because at least some federal courts have held that no-injury BIPA claims do not create the "case or controversy" required for federal-court jurisdiction, defendants may be required to litigate such claims in state court.

BIPA regulates private entities' collection, storage, and use of biometric information.

BIPA prohibits private entities from obtaining or using an individual's biometric information without first providing defined notices and obtaining written consent to do so. 740 ILCS 14/15(a), (b). BIPA allows any "person aggrieved" by a statutory violation to sue for either actual damages or "liquidated damages" of between $1,000 and $5,000, plus attorneys' fees and injunctive relief. 740 ILCS 14/20.

"Person aggrieved" is not defined in the statute, which led to conflicting decisions in Illinois appellate courts about whether a tangible injury—beyond a mere statutory violation—is required for a plaintiff to have statutory standing to sue. *Compare Rosenbach v. Six Flags Entertainment Corp.*, 2017 IL App (2d) 170317 (plaintiff must have tangible injury to sue); *Sekura v. Krishna Schaumburg Tab, Inc.*, 2018 IL App (1st) 180175 (plaintiff can sue based solely on statutory violation).

Plaintiff sued based on a violation of BIPA without a tangible injury.

The plaintiff in Rosenbach—a minor represented by his mother—had his fingerprints taken by defendant for a season pass when he visited a Six Flags amusement park. 2019 IL 123186, ¶¶ 4–6. Plaintiff's mother alleged that defendant created a biometric profile for her son without providing the notice and obtaining the consent required by BIPA. *Id.* ¶ 8. She did not allege that she or her son had been damaged by the alleged statutory violation, such as through a theft or other disclosure of his biometric information or through any kind of identity theft. *Id.* ¶ 22.

Defendant moved to dismiss the complaint, arguing that the lack of any tangible injury meant plaintiff was not "aggrieved" and thus had no right of action under the statute. *Id.* ¶ 12. The trial court denied the motion, but on interlocutory appeal, the appellate court reversed and held that a plaintiff could only be aggrieved under the statute if they could show some tangible harm beyond a mere statutory violation. *Id.* ¶ 15. The Illinois Supreme Court then granted leave to appeal that decision.

In *Rosenbach*, the Illinois Supreme Court allowed BIPA claims to proceed based solely on statutory violations.

The Supreme Court in *Rosenbach* gave a clear and final answer that will be binding on all courts that consider BIPA claims: plaintiffs need only allege a statutory violation to have a private right of action and an ability to collect statutory damages. 2019 IL 123186, ¶ 40 ("an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act.").

In reaching its conclusion, the Supreme Court relied on both statutory text and legislative intent. Looking at the text, the Court noted that a dictionary defines "aggrieved" as including an invasion of a legal right. *Id.* ¶ 32. The Court also noted that other Illinois statutes that use the word "aggrieved" in similar fashion have been interpreted to authorize a private right of action, and that Illinois statutes that require a tangible injury to sue explicitly express that requirement. *Id.* ¶¶ 25–27.

Regarding policy, the Court noted the Illinois legislature's desire to both require companies handling biometric information to safeguard that information and to deter violations of the Act. The Court believed that significantly limiting a plaintiff's ability to sue to enforce the statute's requirements would undercut the legislature's purpose. *Id.* ¶ 37 ("To require individuals to wait until they have sustained some compensable injury beyond violation of their statutory rights before they may seek recourse, as defendants urge, would be completely antithetical to the Act's preventative and deterrent purposes.").

Impact: More BIPA cases will be filed, and Defendants may be stuck in state court.

Over a hundred BIPA class actions have been filed over the last two years. Filings seemed to slow after the appellate court decided *Rosenbach* and held that plaintiffs must have a tangible injury to have a viable BIPA claim. Now that the Illinois Supreme Court has conclusively held that claims can be stated based solely on statutory violations, BIPA class actions will undoubtedly increase.

Further, defendants may be precluded, in at least some jurisdictions, from removing no-injury BIPA cases to federal court. Federal district courts in Illinois, and the 2nd Circuit Court of Appeals, have all held that bare violations of BIPA without a tangible injury do not create a case or controversy as required under Article III for federal subject-matter jurisdiction. *Santana v. Take-Two Interactive Software*, 717 Fed. App'x. 12 (2nd Cir. Nov. 17, 2017); *McGinnis v. U.S. Cold Storage*, No. 17 C 08054, 2019 WL 95154 (N.D. Ill. Jan. 3, 2019); *Rivera v. Google, Inc.*, No. 16 C 02714, 2018 WL 6830332 (N.D. Ill. Dec. 29, 2018). All of these decisions relied on the U.S. Supreme Court's 2016 decision in *Spokeo v. Robins*, 136 S. Ct. 1540 (2016). *But see, Patel v. Facebook, Inc.*, 290 F. Supp. 3d 948 (N.D. Cal. 2018) (finding Article III standing in BIPA case despite lack of injury).

Thus, defendants caught up in the new wave of BIPA cases may find themselves in the odd position of arguing that a plaintiff's bare statutory violation is sufficiently tangible to support federal-court jurisdiction. Otherwise those defendants will be forced to defend in plaintiff's oft-preferred forum: state court.

Cybersecurity Update: NYDFS, NAIC, and What's Going on in SC, OH, MI, and MS?

By Theodore P. Augustinos and Ben Frazzini-Kendrick

On March 1, 2017 the cybersecurity regulation of the New York Department of Financial Services (the DFS Regulation) took effect, requiring subject financial institutions (Covered Entities), including insurance companies, to, among other things, adopt written information security programs to address the protection of nonpublic information and information systems. *See* 23 NYCRR Part 500. The National Association of Insurance Commissioners (NAIC), which had separately been preparing a model cybersecurity law, adopted a model law that closely resembled the DFS Regulation.[1] A version of the NAIC model law was first enacted in South Carolina, with Ohio, Michigan, and Mississippi following suit.[2] A similar bill in Alabama passed both chambers of the state legislature,[3] and additional bills are pending in Connecticut, New Hampshire, and Nevada.[4] However, none of the laws as enacted were exactly the same as each other, and none precisely followed the NAIC model.

So what's going on?

In concept, the laws are substantially similar. Each requires Covered Entities to adopt cybersecurity programs and policies to protect information systems and nonpublic information. Further, they require each Covered Entity to perform a risk assessment and base its programs and policies thereon, to develop an incident response plan, and to investigate and report data breaches to regulatory authorities in their respective states. Finally, the laws provide for some limited exemptions from having to comply with their requirements based on compliance with, for example, the Health Insurance Portability and Accountability Act (HIPAA), or based on the size of the licensee.

Each law differs in some respects. For example, the DFS Regulation and NAIC model law differ as to their definitions of what constitutes a cybersecurity event and what triggers a cybersecurity event notification requirement. Ohio adopted a cybersecurity event definition based on, but slightly different from, the NAIC model law. Further, the laws differ as to their deadlines for providing notification of cybersecurity events. The DFS Regulation and the NAIC model law both require notification within 72 hours. Michigan requires notification within 10 days, and Ohio and Mississippi require notification "as promptly as possible," but no later than three business days. The laws also differ with respect to the nature and scope of exemptions and particular requirements for written policies. Covered Entities should be attuned to these differences when developing compliance programs. Click HERE for a summary of some of these differences.

1 Click here for prior coverage of the NY DFS cybersecurity regulation and the NAIC model law.
2 Mississippi (Senate Bill No. 2831) approved by Governor Phil Bryant on April 3, and scheduled to take effect July 1, 2019.
3 Alabama Senate Bill 54, assigned Act No. 2019-98.
4 Similar laws are now pending in other states, including Connecticut (Raised Bill 903), New Hampshire (Senate Bill 194-FN), and Nevada (Senate Bill 21).

Data Privacy and Security for the HR Suite

By Laura L. Ferguson and Sean Killian

On two fronts, the Human Resources department has an increasingly important role in the privacy and security of an organization's data. On the one hand, HR collects, uses, retains, stores, and disposes of personal information related to the organization's applicants, employees, and former employees. Employee personal information is valued by hackers and has been targeted specifically, and it could be exposed by hackers even when not targeted. On the other hand, as a liaison between management and employees, HR typically conducts training and administers personnel policies meant to enhance the security of all the organization's data, whether employee data, consumer data, or company data. This article discusses the legal obligations and best practices HR should consider in its dual role.

Data privacy for HR starts with minimizing the collection of personal information of applicants and employees. This is not to say that HR should collect less information than it needs, but HR should review the types of personal information it collects, and when the information is collected. A prime example is job applications, which too often collect sensitive personal information (such as Social Security numbers or driver's license numbers) that should not be collected until the background check or identity verification stages. HR should also be wary of using job applications to collect information that is subject to use restrictions, such as arrest and conviction information, protected characteristics or their proxies, and, in some jurisdictions, past salary information.

Job applications are only the first of many points at which HR collects personal information, and the issue becomes how such information must be preserved. Other categories of personal information collected or created by HR include contact information, bank account numbers, background checks, drug test results, physical exams, health and genetic information, employee benefits information, biometric information, personnel action records, payroll records, and more. HR might also administer employee wellness programs or flu shot clinics, or it might be on the HIPAA team for the company's group health plans. HR should consider conducting a data inventory to understand each of the ways it collects personal information, and the types of personal information it collects, so that it can determine how such information should be stored, and how long it should be retained.

To complicate matters further, nearly all of the categories of information named above are subject to one or more specific federal or state record retention statutes. For example, the FMLA requires retention of leave-related records for at least three years; the FLSA requires retention of certain payroll records for at least three years (and state laws often require longer); and federal law requires retention of personnel action records for at least one year.[1] Other statutes, such as the Texas biometric privacy statute, take the opposite approach by mandating destruction after a maximum length of time.[2]

Because employers have to collect personal information and they have to retain it, the issue becomes how to retain it securely. For practical reasons, employers often store the information above in a single personnel file for each employee.[3] At least *some* of the information in the file is likely entitled to special protection under applicable law. For example, under Texas law, companies that store "sensitive personal information" are required to implement and maintain reasonable procedures to prevent it from being unlawfully disclosed.[4] At the outset, HR can help lessen the burden of maintaining information by developing an approach to retaining data consistent with the applicable retention laws.

Although there are industry-standard security frameworks, there is not a "one size fits all" approach to what constitutes a "reasonable procedure" for secure data

1 29 C.F.R. § 825.500 (FMLA records); 29 C.F.R. § 516.5 (FLSA records); 29 C.F.R. § 1602.14.
2 Tex. Bus. & Com. Code § 503.001 (c)(3) (mandating destruction of biometric identifiers within a reasonable time not later than one year after the purpose for collecting the biometric identifier expires).
3 An important exception is employee medical information, which should be stored in a separate file.
4 Tex. Bus. & Com. Code § 521.052 (a) (requiring implementation of reasonable procedures to protect "sensitive personal information"). "Sensitive personal information" is generally defined as an individual's name in combination with his or her Social Security number, identification card number, or account number and access code. Tex. Bus. & Com. Code § 521.002 (a)(2).

retention.[5] Some of the common technical measures – such as controls on access to electronic data, or encryption in transit and at rest – fall in the domain of IT. Many companies, such as those with obligations under HIPAA or the Gramm-Leach-Bliley Act, already have data security programs in place, and they can consider extending those programs to HR data. HR has a role here, too, by implementing personnel policies that control employees' access to company information. HR should also work with IT to train employees on information security awareness. Implementing these measures can serve the dual purposes of securing employee data and other company data, such as consumer data.

HR's role does not end when employee data is securely stored, because there is still the privacy issue of how the stored employee data can be used. In what might be an example of an emerging trend, California has enacted the California Consumer Privacy Act (CCPA), a comprehensive data privacy law that gives employees a variety of rights to their employee data.[6] As currently drafted,[7] the CCPA will give employees the rights to request access to their personal information, request deletion of their personal information, request disclosure of the business purpose for which their personal information is used, request disclosure of the third parties with whom the employers shares their personal information, and receive certain notices, among others.[8] The emergence of comprehensive data privacy laws underscores the importance of having a data inventory that will enable compliance with obligations to employees.

Lastly, HR should understand how to dispose of data securely. Secure disposal is not only a good practice, it is a legal requirement as to certain types of data.[9] When the data's retention period expires, HR should train employees to identify and securely destroy documents and digital files containing employee personal information.

For any company meeting the ongoing challenge of data privacy and security, HR has important roles to play, specifically as to employee data, but also as to all data stored by the company. HR must be prepared to collect, use, store, retain, and dispose of personal information consistent with company practice and applicable law, and to equip employees to do the same.

Privacy Law Update: Texas To Study Entering The Fray

By: Laura L. Ferguson and Sean Kilian

The 2019 Texas legislative session recently passed a new bill on the consumer privacy front that strengthens the breach notification obligations under the Texas Identity Theft Enforcement and Protection Act (TITEPA, located in Section 521.053 of the Texas Business and Commerce Code) and creates the Texas Privacy Protection Advisory Council (TPPAC). HB 4390 has been signed by Governor Abbott and will become effective on January 1, 2020.

HB 4390 provides for two amendments to TITEPA that bring it more in line with many other states' data breach notification laws. First, HB 4390 adds a deadline for the notification of individuals after discovery of a breach. Businesses must notify individuals whose sensitive personal information was breached without unreasonable delay and no later than 60 days after determination that a breach occurred, subject to the existing exception allowing for delayed notice at the request of a law enforcement agency. Second, HB 4390 adds a new Attorney General notification requirement for breaches in which at least 250 Texas residents were affected. The notification to the Texas Attorney General must include, among other things, a description of the breach, the number of affected residents, and the measures taken regarding the breach.

The newly created TPPAC will be a 15-member council that is charged with studying current data privacy laws and making statutory recommendations regarding the

5 Some state laws are more specific than Texas on this point. For example, as we have previously written, Ohio law specifically recognizes that certain industry norms constitute reasonable security.
6 Please see page 13 herein for more information about the CCPA's effects on employee data.
7 The California legislature is currently considering an amendment to the CCPA (Assembly Bill 25) that, in its current form, would delay most obligations related to employee data until January 1, 2021.
8 Less dramatic regulation of use of employee data exists in other areas of the law. For example, by statute, employee genetic information cannot be used in making employment decisions. 42 U.S.C. § 2000ff–1(a). Other employee data, such as background check information, should only be used consistent with the scope of the employee's authorization. 15 U.S.C. § 1681b. In some jurisdictions, state laws simply give employees the right to access their personnel files. See, e.g., 820 Ill. Comp. Stat. 40/2 (Illinois statute granting employees right to inspect personnel documents).
9 *See, e.g.*, 16 C.F.R. § 682.3 (requiring secure disposal of background checks); Tex. Bus. & Com. Code § 521.052 (a) (requiring implementation of reasonable procedures to protect "sensitive personal information").

privacy and protection of information. The council will be appointed and will consist mostly of representatives of specified industries, including medical, retail, banking, and several internet-related industries. HB 4390's creation of the TPPAC is a significant signal that Texas is focused on consumer privacy and more onerous legislation may come in the future. The TPPAC will be getting to work with a first official reporting deadline of September 1, 2020.

Another bill that had businesses concerned this year was HB 4518 (also known as the Texas Consumer Privacy Act), which was essentially a copy and paste version of the California Consumer Privacy Act (CCPA), the comprehensive data privacy statute that will soon become effective in California. HB 4518 was left pending in committee, but it would have given consumers a number of new individual rights with respect to businesses that collect their personal information, including: the rights to disclosure and deletion of personal information collected; the right to disclosure of personal information sold or disclosed; the right to opt out of the sale of personal information; and the right to receive notice when personal information will be collected and used. Although HB 4518 ultimately failed, that type of bill may be the direction the TPPAC will be heading. Since the passing of the CCPA, a number of state legislatures – including Massachusetts, Nevada, New Mexico, New York, and more – have considered comprehensive data privacy bills that would grant consumers individual rights similar to those granted by the CCPA.

Prior to January 1, 2020, businesses that maintain sensitive personal information of Texas residents (such as Social Security numbers, drivers' license numbers, credit/debit card numbers, or health care related information) should review their incident response plans and update as needed to reflect the changes to TITEPA.

CCPA Guide: Are You Covered by the CCPA?

By Laura L. Ferguson and Theodore P. Augustinos

Beginning on January 1, 2020, the California Consumer Privacy Act of 2018 (CCPA) will impose new privacy obligations on certain businesses that collect personal information of California consumers and are (or are jointly with others) responsible for determining the purposes and means of the processing of such information. This summary will assist U.S. businesses in making an initial determination of whether they might be subject to the CCPA once effective.

Is your business subject to the CCPA?

The CCPA applies to businesses — not nonprofits or governmental entities — that meet the following criteria:

1. For-profit entity doing business in the State of California; and
   (a) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), subject to adjustment;
   (b) Handles data of more than 50,000 people or devices; or
   (c) Has 50% or more of revenue coming from selling personal information.
2. Businesses that "control" or are "controlled by" or have "common branding" with a business that satisfies the above.

What is a Business for purposes of the CCPA?

Any sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is not considered a nonprofit entity under the California Nonprofit Corporation Law.[1]

What does "doing business" in the State of California mean?

Although the CCPA does not define "doing business", the typical analysis begins with looking at the California Revenue and Taxation Code (the "R&TC").[2] A business is doing business in California if it actively engages in any transaction for the purpose of financial or pecuniary gain or profit in California or if any of the following conditions are satisfied:

- The business is organized or commercially domiciled in California.
- Sales, as defined in subdivision (e) or (f) of R&TC section 25120, of the business in California, including sales by the agents and independent contractors of the business, exceed the lesser of $500,000 or 25% of the business's total sales. For purposes of R&TC Section 23101, sales in California are determined using the rules for assigning sales under R&TC 25135, R&TC 25136(b) and the regulations thereunder, as modified by regulations under Section 25137.
- Real and tangible personal property of the business in California exceed the lesser of $50,000 or 25% of the business's total real and tangible personal property.

1 The California Nonprofit Corporation Law (Division 2 of the Title 1 of the California Corporations Code) provides that nonprofit entities can incorporate as Nonprofit Public Benefit Corporations, Nonprofit Mutual Benefit Corporations, or Nonprofit Religious Corporations. The law further provides that an unincorporated nonprofit association must contain language in its creating document that the association is not allowed to keep the proceeds from business activities and the proceeds must be used for nonprofit purposes.

2 R&TC Section 23101.

- The amount paid in California by the business for compensation, as defined in subdivision (c) of R&TC 25120, exceeds the lesser of $50,000 or 25% of the total compensation paid by the business.
- For the conditions above, the sales, property, and payroll of the taxpayer include the business's pro rata or distributive share of pass-through entities. "Pass-through entities" means partnerships, LLCs treated as partnerships, or S corporations.[3]

How is annual gross revenues calculated?

There is currently no guidance that explains whether a business must take into consideration worldwide revenue or revenue from California operations. Conservatively, absent further guidance on this issue, a business doing business in California with annual gross revenue exceeding the $25 million threshold should begin preparing for the implementation of the CCPA.

What is "control"?

A business that controls or is controlled by a business covered by the CCPA is also considered to be covered by the CCPA. For purposes of this determination, the CCPA follows typical indicia of control: (i) common ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a business; (ii) control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or (iii) the power to exercise a controlling influence over the management of a company.

What is "common branding"?

A business that shares common branding with a business covered by the CCPA is also considered to be covered by the CCPA. For purposes of this determination, the CCPA provides that common branding includes a shared name, servicemark, or trademark.

What exemptions might apply?

There are various partial exemptions available for certain types of information collected by entities that are also subject to federal privacy laws. It is important to note that the most important and potentially relevant exemptions apply to certain information processed pursuant to the protections of certain federal regimes. It is important to note that the exemptions do not apply to the businesses covered by these regimes. For example, HIPAA-covered entities (and business associates) are not exempt from the CCPA, but protected health information collected by a covered entity or business associate governed by the privacy, security and breach notification rules promulgated pursuant to HIPAA is exempt.[4] Note, however, that not all information collected by HIPAA covered entities and business associates is "governed by" these rules. Therefore, IP addresses, for example, collected by a HIPAA covered entity appear to be subject to the requirements and protections of the CCPA, even though protected health information collected by the same entity would be exempt.

Similarly, nonpublic personal information processed by a financial institution subject to the privacy, security and breach notification rules promulgated pursuant to the Gramm-Leach-Bliley Act would be exempt, but the financial institution would be required to comply with the CCPA with respect to other information (such as information collected when tracking website visitors or providing targeted online advertisements) collected by the financial institution.[5] In addition, this exemption does not apply to the consumer's right of to sue for statutory damages as a result of data breach.[6]

What if my business is subject to the CCPA?

The CCPA has several onerous requirements that will require significant preparation in advance of the CCPA effective date of January 1, 2020. Therefore, businesses subject to the CCPA will need to plan and start their compliance efforts immediately

Notice Requirement: At or before the time of collecting personal information, the business must provide notice of the categories of personal information to be collected, and the purposes for which they will be used.

Disclosure Requirements: Upon request of a consumer, the business must disclose the following:

- categories and specific pieces of the consumer's personal information the business has collected;
- categories of sources from which personal information is collected;
- business or commercial purpose for collecting or selling personal information; and
- categories of third parties with whom the business shares personal information.

Delivery of Personal Information: Upon request of a consumer, up to twice in a 12-month period, the business must deliver to the consumer all of the consumer's personal information collected.

Right to be Forgotten: Each business must notify consumers of their right to request the business to delete all of the consumer's personal information. Certain exceptions permit the business to retain personal information for specific purposes.

3 Revenue and Taxation Code (R&TC) Section 23101.
4 CCPA Section (c)(1)(A).
5 CCPA Section 1798.145(e).
6 CCPA Section 1798.145(f).

Non-Discrimination: With limited exceptions, businesses are prohibited from discriminating against a consumer because the consumer exercised any of the consumer's rights under the Act, including denying goods or services, charging different prices, providing a different level of quality of goods or services, or suggesting that the consumer will receive a different price or level of quality of goods or services.

What should businesses be doing between now and January 1, 2020?

In order to be in a position to satisfy these requirements by the effective date, businesses subject to the CCPA will need to take the following actions, starting now:

- Understand the data. What personal information does the business collect?
- Understand how personal information is processed, including to whom it is transmitted or made accessible, and where it is stored.
- Draft the required notices and disclosures.
- Build a process for responding to consumer demands, including protocols for deleting data.
- Review and, as necessary, amend contracts with third party service providers to ensure the business can compel its vendors to comply with CCPA requirements.

CCPA Guide: We Are Covered, So Now What Do We Do? Create a Project Plan!

By: Theodore P. Augustinos and Laura L. Ferguson

Effective January 1, 2020, the California Consumer Privacy Act of 2018 (CCPA) will impose new privacy obligations on certain businesses that collect personal information of residents of California and are responsible for (or jointly with others) determining the purposes and means of the processing of such information. As a companion to our articles in this Newsletter, Are You Covered by the CCPA?, and Does Personal Information Include Employee and Employee Benefit Plan Data?, below is a list of action items, key deliverables, and target dates to create a compliance program in time for the CCPA's effective date.

As this timeline indicates, it is imperative that a business begins its compliance efforts immediately in order to be prepared for the onerous requirements in advance of the CCPA effective date of January 1, 2020. Even though the CCPA enforcement date is the earlier of July 1, 2020 or six months following the date that the California Attorney General issues regulations under the CCPA, businesses must comply with the CCPA requirements beginning January 1, 2020.

ACTION ITEM	KEY DELIVERABLES	TARGET DELIVERABLE DATE
Data Mapping	Review what type of personal information is collected by the business and how it is processed, including to whom it is transmitted or made accessible, and where it is stored. Create a data map.	August 31, 2019
Draft Policies and Procedures	Draft policies and procedures that document how the business intends to comply with its responsibilities under the CCPA. For example, develop a policy and procedure to review data and systems periodically, verify the validity of consumer requests, respond to consumer requests (including protocols for deleting data), and manage vendor contracts.	September 30, 2019
Draft Disclosure Notices	Draft required notices: (i) consumer's rights under CCPA (such as the right to request what categories and specific data is held by business, right to be forgotten, right to opt out of sale of personal information) and (ii) business' collection of personal information and the purposes for which such information will be used.	September 30, 2019
Review and Amend Vendor Contracts	Review and, as necessary, amend contracts with third party service providers to ensure the business can compel its vendors to comply with CCPA requirements. For example, if a vendor maintains data that is required to be disclosed to a consumer or deleted upon request, the vendor must be obligated to do so in the service agreement.	November 30, 2019
Draft form request and response letters	Draft forms for consumers to use in exercising their various rights under the CCPA and draft form response letters for the business. For example, draft a consumer request for categories and specific data collected by a business, as well as a response letter, including a form for when the response is to not disclose the information (such as when the consumer has submitted more than 2 requests within a 12-month period).	December 31, 2019

CCPA Guide: Does Personal Information Include Employee and Employee Benefit Plan Data?

By: Theodore P. Augustinos, Laura L. Ferguson, Emily Holpert and Sean Killian

Beginning on January 1, 2020, the California Consumer Privacy Act of 2018 (CCPA) will impose new privacy obligations on certain businesses that collect personal information of California consumers. Employers with employees in California are trying to navigate how the CCPA applies to the employment relationship, including information related to employee benefit plans. Below is a summary of the potential implications for employers that are a "business" covered by the CCPA. To determine if your business is subject to the CCPA, please see our companion articles in this newsletter, Are You Covered by the CCPA? For guidance on developing your CCPA compliance project plan, please see our companion article in this newsletter, We Are Covered, So Now What Do We Do? Create A Project Plan!

Are my employees covered by the CCPA?

The definition of "consumer" is very broad, providing that any natural person who is a California resident is a "consumer" for purposes of the CCPA. Currently, this broad definition extends to cover employees who are resident in California. The fact that their relationship with the business is as an employee, and not a consumer of the goods and services of the business, is irrelevant for this purpose. Residency is determined using an analysis of whether an individual is (i) in California for other than a temporary or transitory purpose; or (ii) domiciled in California but temporarily or transitorily outside of California.[1] Therefore, your employees who are domiciled in California, including those who are temporarily outside of California on business, are consumers under the CCPA. However, your employees who travel to California to do business periodically, but are not considered resident there, are not "consumers" under the CCPA.

Whether the CCPA will apply to consumers in their capacities as employees is in flux right now due to a pending amendment to the CCPA by AB 25, which has itself been revised since it was first introduced. A previous version of AB 25 would have modified the definition of "consumer" to exclude employees from the definition. The July 11, 2019 version of AB 25 would leave the definition of "consumer" unchanged, but it would provide a temporary respite for employers. AB 25 states that the CCPA does not apply to:

> Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.

However, AB 25 also states that the foregoing paragraph "shall become inoperative on January 1, 2021." As such, if the July 11, 2019 version of AB 25 passes, the CCPA generally would not cover employees on January 1, 2020, but it would cover employees – and any employment-related and employee benefit plan data held by an employer – on January 1, 2021. Reportedly, the exemption for employees may be made permanent by later amendment, but the temporary reprieve was the result of a political compromise. We cannot currently assess the likelihood of any future amendment to extend this exemption or make it permanent.

Lastly, note that under the July 11, 2019 version of AB 25, two key provisions affecting employees will come into effect with the rest of the CCPA on January 1, 2020: (1) employees can sue for data breaches; and (2) the notice regarding categories of information collected, used and disclosed by the employer must be given to the employees. Once January 1, 2021 arrives, the exemption language described above would go away and the CCPA would fully apply to consumers in their capacities as employees. The rest of this article discusses the current text of the CCPA and the implications for employment-related and employee benefit plan data.

Is employment-related data considered "personal information"?

Yes. As the definition of "consumer" is very broad, so is the definition of "personal information." Employment-related information is clearly "personal information"

1 California Code of Regulations, Title 18, Section 17014.

under the CCPA.[2] There is no exemption for employment-related personal information stored and maintained by an employer, unlike the privacy laws of other states, such as Texas.[3]

"Personal information" means "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[4] Various examples applicable to the employment relationship are listed in the definition, including: name (real or alias), address, email address, Social Security number, driver's license number, insurance policy number, education, employment, employment history, bank account number, credit card number, or any other financial information, medical information, health insurance information, biometric information, Internet or other electronic network activity information.

Notwithstanding this definition, to the extent employment-related information is collected or used in connection with an ERISA-covered employee benefit plan, such data *may* be exempted from the CCPA due to ERISA preemption, as discussed below under "Is employee benefit plan data covered by the CCPA?"

From an employer perspective, consider the following common types of data that would be "personal information" for purposes of the CCPA:

- New hire/onboarding paperwork, including resumes, employee applications (typically including Social Security Number, drivers' license, mailing address, and other personal information), background checks, IRS Forms W-4 (withholding), etc.
- Payroll information, including employee bank account numbers for direct deposit.
- Credit card information provided in connection with expense reports.
- Random drug testing paperwork and results.
- Documenting of various types of leave, such as sick leave, vacation, paid time off, FMLA leave, USERRA leave, maternity/paternity leave, etc.
- Employee benefit plans (to the extent not exempt from the CCPA).
- Employee's online activity on a work computer/system, such as browsing history, search history, and information regarding the employee's interaction with an Internet Web site, application, or advertisement.

Is employee benefit plan data covered by the CCPA?

Generally, yes. Employee benefit plans collect and use personal information as the plans require various types of personal information in operation, such as name, address, Social Security Number, and insurance policy information. However, compliance obligations of certain benefit plans may be: (1) limited by the CCPA's HIPAA exemption; and (2) potentially preempted by ERISA.

1. **HIPAA Exemption.** The CCPA does not apply to "protected health information" (PHI) of a group health plan that is a "covered entity" subject to HIPAA or to other personal information maintained by the covered entity in the same fashion as PHI. Employer sponsored HIPAA-covered benefit plans typically include a major medical plan, dental, vision, health flexible spending account, and certain wellness or employee assistance programs. It is important to note that some information collected by a plan may be personal information under the CCPA, but not PHI under HIPAA, and there may be compliance obligations with respect to that information.
2. **ERISA Preemption.** ERISA-covered benefit plans that are not HIPAA-covered (such as retirement, long term disability, life and AD&D) may be able to successfully argue that personal information collected and used in connection with such plans are not subject to the requirements of the CCPA. ERISA supersedes all "state laws" (including state law causes of action) that "relate to" employee benefit plans that are covered by Title I of ERISA.[5] ERISA preempts a state law if (1) the state law imposes requirements explicitly with reference to ERISA plans, or (2) if the state law governs central matters of plan administration or that interferes with nationally uniform plan administration.[6] Although the CCPA does not explicitly reference ERISA plans, the CCPA is likely to have a direct impact on the ability of an employer to have a nationally uniform plan administration for its benefits when operating in multiple states. The CCPA would require the employer to subject the ERISA plan to employee/participant requests for access and deletion that would be likely to significantly increase the cost of operating plans with respect to California employees/participants. Unfortunately, absent guidance that may be provided by the California Attorney General, in order to find out if the CCPA is in fact preempted so compliance is not required a company may need to bear enforcement risk, and be willing to spend time and money to litigate the issue.

2 CCPA Section 1798.140(o)(1)(I).
3 For example, in Texas, the medical records privacy law provides an exemption for employers, except with respect to a limited provision on the prohibition on re-identification of PHI. Texas Health and Safety Code Section 181.051.
4 CCPA Section 1798.140(o)(1). Note that "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
5 ERISA Section 514(a).
6 *Shaw v. Delta Air Lines, Inc., 463 US 85 (1983).*

Most employers likely maintain non-ERISA benefit plans that would be required to comply with the CCPA, such as short-term disability (if designed as a pay practice), various types of leave/vacation/paid time off, dependent care flexible spending accounts, and voluntary insurance (such as Aflac). Therefore, employers will need to consider whether claiming ERISA preemption is worthwhile, given that some of the employer's plans may and others may not be subject to the preemption argument. In addition, many ERISA plans are administered by third party vendors that may otherwise be preparing to comply with the CCPA, which could reduce some of the challenges with compliance at least with respect to the benefit plan data held by the third party vendor.

What rights do my employees get under the CCPA?

The CCPA gives consumers, including your employees who are residents of California, various rights related to their personal information held by your business if your business is subject to the CCPA. For employees, here is what that currently means:

- Right to Data Access. Employees may request categories of, and specific pieces of personal information that the employer has collected about them. The employer must promptly provide the employee with that data, upon verification of the employee's identity.
- Right to Deletion. Employees may request that an employer delete any personal information the employer has collected about the employee. An employer is not, however, required to comply with the request to delete when it is necessary for the employer to maintain the personal information in certain situations.[7]
- Disclosure Requirements: Upon verified request, the employer must provide to an employee the:
- categories of personal information collected;
- categories of sources from which personal information is collected;
- purpose for collecting such information;
- categories of third parties with access to the personal information; and
- specific pieces of personal information collected about the employee.[8]
- Right to Opt-Out. Although a consumer has the right to opt out of a businesses' sale of the consumer's personal information to third parties, this is unlikely to come up in the context of the employment relationship as employers typically do not "sell" employees' personal information.[9]

What key steps should employers take?

An employer subject to the CCPA should apply the same steps it is applying to "personal information" it collects from customers and other consumers to employee data and employee benefit plan data that may be subject to the CCPA. However, as a practical matter, the notices provided and the processes involved may be communicated and operated differently for the employee population versus external "consumers". A few key issues for employers developing a CCPA compliance project include:

- *Determine which employees are residents of California or whether to extend the California consumer rights to all employees.*
- *Determine whether employee benefit plan data is personal information that is not exempt from the CCPA.*
- *If your business is a "covered entity" under HIPAA and/or the CMIA,[10] determine whether employee data is subject to the same privacy and security protections as patient information.*
- *Determine which systems and third party service providers hold the employee information.*
- *Develop a streamlined method by which employees can make personal information access and deletion requests.*
- *Develop processes to identify and isolate an individual's information.*
- *Train a team of employees to handle and respond to CCPA requests from employees.*

Employers subject to the CCPA should begin compliance efforts immediately in order to be prepared for the onerous requirements in advance of the CCPA effective date of January 1, 2020.

7 CCPA Section 1798.105.
8 There are additional disclosure requirements if an employer sells employee information for a business purpose; however, a typical employer would not be selling employee information and such disclosure requirements are not discussed herein. CCPA Section 1798.115.
9 CCPA Section 1798.145(c)(1)(B).
10 CCPA Section 1798.120.

Verifying the Verifiable – Considering a "Verifiable Consumer Request" Under the CCPA

By: Molly McGinnis Stine and Paul B. Sudentas

You can't hear it often enough: the California Consumer Privacy Act of 2018 (CCPA) – Cal. Civ. Code § 1798.100 *et seq.* – comes into effect on January 1, 2020 with enforcement by the Attorney General beginning on July 1, 2020 (6 months after the effective date). Yes, really. This broad-sweeping Act does many things, including permitting California consumers[1] to request information from covered businesses about the California consumers' personal information collected by said businesses.

Under the CCPA, a California consumer may submit two kinds of verifiable consumer requests to a covered business. The first type requests that the business provide, for example, the types of personal information collected by the business; the personal information specifically collected by the business; and the identity of entities with which the business shared and/or sold the personal information. The second type requests that the business delete the consumer's personal information. Upon receipt of either kind of request and verification of the identity of the requestor, the business must promptly respond.

Despite giving considerable detail about what may be requested, the CCPA does not provide much explanation of what constitutes a verifiable consumer request or how a business is to verify such a request. The CCPA defines "verifiable consumer request" as:

> [A] request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information.

Cal. Civ. Code. § 1798.140(y). Notably, however, the CCPA identifies only one mechanism for "reasonably verify[ing]" that the request was made by the consumer or by someone authorized to submit such request on the consumer's behalf, and leaves it to the Attorney General to provide further guidance:

On or before January 1, 2020, the Attorney General shall solicit broad public participation to adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

> Establishing rules and procedures . . . to govern a business' determination that a request for information received by a consumer is a verifiable request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business' authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

Cal. Civ. Code. § 1798.185(a)(7).

Covered businesses cannot afford to take a "wait and see" approach to developing internal policies on how to "reasonably verify" a request from a California consumer. While awaiting specific guidance from the Attorney General, considerations should include, for example:

- types of information to request in order to verify a consumer's request;
- mode of communication with a consumer regarding the request;
- templates for a consumer to use to make a request based on whether or not the consumer has an online account with the business;
- whether to verify requests in-house or through a third party vendor (and the potential implications of sharing personal information with such a third party); and
- possible guidance from how requests are already verified for other purposes, including, for example, under the European Union's General Data Protection Regulation (GDPR).

We also note that the CCPA allows for up to two requests within a 12-month period to seek identification of information collected over the 12 prior months for which a covered business is required to respond and provide personal information.

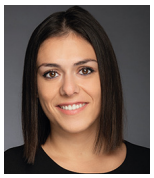
1 Under the CCPA, a "consumer" is "a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier." Cal. Civ. Code 1798.140(g).

OUR AUTHORS:

Theodore P. Augustinos
Partner
Hartford
860-541-7710
ted.augustinos@lockelord.com

Laura L. Ferguson
Partner
Houston
713-226-1590
lferguson@lockelord.com

Ben FrazziniKendrick
Associate
Hartford
860-541-7763
benjamin.frazzinikendrick@lockelord.com



Emily Holpert
Associate
Chicago
312-443-0264
emily.holpert@lockelord.com

Sean Kilian
Counsel
Dallas
214-740-8560
skilian@lockelord.com

Michael McGivney
Associate
Chicago
312-443-0208
michael.mcgivney@lockelord.com

Matthew Murphy, Editor
Associate
Providence
401-276-6497
matthew.murphy@lockelord.com

P. Russell Perdew
Partner
Chicago
312-443-1712
rperdew@lockelord.com

Andrew Shindler
Partner
London
+44 (0) 20 7861 9077
andrew.shindler@lockelord.com

Molly McGinnis Stine
Partner
Chicago
312-443-0327
mmstine@lockelord.com

Paul B. Sudentas
Senior Counsel
New York
646-217-7716
psudentas@lockelord.com

Practical Wisdom, Trusted Advice.

www.lockelord.com

Atlanta | Austin | Boston | Chicago | Cincinnati | Dallas | Hartford | Hong Kong | Houston | London | Los Angeles
Miami | New Orleans | New York | Princeton | Providence | San Francisco | Stamford | Washington DC | West Palm Beach

Locke Lord LLP disclaims all liability whatsoever in relation to any materials or information provided. This piece is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. If you wish to secure legal advice specific to your enterprise and circumstances in connection with any of the topics addressed, we encourage you to engage counsel of your choice. (081519)

Attorney Advertising © 2019 Locke Lord LLP