GAMING & HOSPITALITY LEGAL NEWS

THE CALIFORNIA CONSUMER PRIVACY ACT COULD BE EXPENSIVE FOR THE GAMING AND HOSPITALITY INDUSTRY

by Sara Jodka

Today's gaming and hospitality companies are complex businesses with data driven processes and systems that collect significant and various types of customer information to provide unsurpassed customer service. However, the collection, processing, and storage of such information will now be more complex as regulatory bodies globally and governments in the U.S. impose tighter controls on the collection, use, selling, and disclosure of such information.

While the national focus has been largely on compliance with the General Data Protection Regulation ("GDPR") imposed by the European Union, the principles embedded in the GDPR are making their way state-side. Recently, a number of states, including Nevada (see article on Nevada's new privacy law here) have passed their own data privacy laws that have applicability outside their state boundaries but none are more far-reaching or impactful than the California Consumer Privacy Act ("CCPA"), which goes into effect January 1, 2020.

Although the CCPA is a California law, the fact that more than 10 million visitors to Nevada each year are California residents means the CCPA is relevant to the gaming and hospitality industry in Nevada. The CCPA is expressly designed to protect the personal information of California residents regardless of the location of the data collector. Additionally, since Nevada's primary industry is a highly regulated industry with a focus on legal compliance, becoming compliant with the CCPA is a current focus for many Nevada-based businesses. Finally, although the CCPA is the first state-side comprehensive law to embrace the core principles of the GDPR, it is unlikely to be the last. And while global businesses are looking to the CCPA to provide standardization and harmonization as data-driven business and cloud-computing technology business expand, the scope of the CCPA is fairly broad meaning many companies outside California, including many in Nevada, will be subject to compliance.

This article will provide a basic understanding of the CCPA as businesses evaluate their data compliance plans and actions.

December 5, 2019 | Volume 12, Number 6

GAMING & HOSPITALITY LEGAL NEWS

To What Businesses Does the CCPA Apply?

The reach of the law cannot be understated as its scope stretches to businesses that may not consider themselves within the purview of California law. Specifically, the CCPA will apply to for-profit business that collect California consumer/household information, if they meet any one of the following three thresholds:

1. Has $25 million or more in gross annual revenue;

2. Buys, receives, sells, shares or collects for commercial purposes the personal information of 50,000 or more California consumers; or

3. The business earns more than half of its annual revenue from selling consumer personal data.

The $25 million or more in gross annual revenue threshold is the one that is catching the most businesses within the CCPA's crosshairs. Although the CCPA is limited in its application to California consumers, due to the size of the California population and the scope of its economy, the CCPA will apply to a significant number of businesses in the gaming and hospitality industry. For example, with approximately 20% of all visitors to Las Vegas coming from California, this is a major development for Nevada casino resort properties.

What Is "Personal Information" Under the CCPA?

It's hard to imagine any customer-facing gaming and hospitality company – be it a land-based casino resort or an online company – that does not collect and/or sell "Personal Information" as that term is defined under the CCPA.

"Personal information" or "PI" is defined under the CCPA as any "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

For more clarity, the CCPA provides that PI will include any of the following categories if they are reasonably capable of being associated with a particular consumer or household. Some of the categories are familiar as they are used in most state data breach laws' definitions of PI. However, many are not and further demonstrate another layer of broadness not otherwise seen in US privacy law. These categories of PI include:

- Real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;

- 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 and other electronic network activity information, including 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;

- Education information; and

- Inference drawn from any of the above mentioned information.

Section 1978.140(o).

What Type of Activity Triggers a Business's Obligations under the CCPA?

There are two types of broad activity that trigger compliance obligations under the CCPA. The first activity is if the business collects PI which is fairly broad and includes "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means." Section 1978.140(e).

The other activity that triggers CCPA obligations is the "sale" or "selling" of PI, which means selling, renting, releasing, disclosing,

disseminating, making available, transferring, or otherwise communicating" Personal Information for a "monetary or other valuable consideration." Section 1978.140(t).

The difference between the two functions, collecting v. selling, however, is significant because the selling of PI by a business will trigger far more compliance requirements under the CCPA, as discussed more fully below.

What Are a Business's Compliance Obligations?

Notice

Whether a business is collecting or selling information, prior to the collection of that information for whatever purpose, the business must provide the individual notice of the categories and specific pieces of PI that the business is collecting and has collected in the preceding 12 months. Section 1978.100(b). The business must identify the purposes for collecting the PI and specifically reference both the business purposes, i.e., the business's internal operations as well as any commercial, i.e., pecuniary purposes. Section 1978.140.

It should also identify the categories of PI that the business has sold in the prior 12 months and to whom. If the business has not sold PI in the last 12 months, that is to be disclosed as well.

Data Subject Rights

The CCPA provides a number of rights to consumers regarding their PI held by a business, which in turn, provides eight compliance obligation on businesses as follows:

1. The Right to Know. Provides a consumer the right to request the business disclose the categories and specific pieces of PI collected about them, the sources from which the PI is collected, the business or commercial purpose of collection (meaning that there are two types of interests to be identified), and with whom the collected PI is shared.

   The right to know also provides consumers the right to request the business disclose the following for the previous 12 months, the categories of PI collected and sold, the categories of third parties to whom data is sold, and the categories of PI disclosed about the consumer for a business purpose. Consumers have the right to receive specific notice of the business's PI collection practices, as well as notice of these rights within the business's general privacy policy.

   Due to the fact that disclosures of information have to be provided directly to the consumer, including in readily-accessible format so that it is portable, the right to know is also a right of access.

2. The Right to Opt Out of the Sale of Data. This gives consumers or their authorized agent the ability to direct businesses to stop selling their PI to third parties. Consumers have the right to receive notice of these rights within the business's general privacy policy, as well as a clear and conspicuous link on the business's internet homepage titled "Do Not Sell My Personal Information," leading to an internet webpage that enables a consumer to opt out of the sale of the consumer's PI.

3. The Right to Opt In for Children; Obligation Not to Sell Children's PI without Affirmative Authorization. This consumer right provides that a business must obtain the opt-in consent from a child (between ages 13 and 16) or the child's parent or guardian (if the child is under the age of 13) before selling the child's PI.

4. The Right to Delete. This right gives consumers the right to request that the business delete their PI after receipt of a verifiable request. In support of this right, consumers have the right to receive notice of their right to deletion within the business's general privacy policy.

5. The Right Not to Be Discriminated Against for Exercising Any Consumer Right. This right gives consumers the right to not be discriminated against for exercising their rights under the CCPA.

Consumer Rights

A business is required to take certain steps to assist individual consumers in exercising their rights under the CCPA.

First, the business must provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number, and, if the business operates a website, an interactive web form accessible through

the business's website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail. If not via the business's app, notice must be on either (1) the mobile app's platform page or download page; or (2) accessed through a link within the mobile app in the "About," "Information," or "Settings" page.

Verification Process

Second, because the right to know and the right to delete require the business to first verify the identity of the customer, businesses will also need to have a functioning verification in place to effect consumer requests.

Whenever possible, businesses should verify consumers using PI collected *from the consumer* or use a third-party identification service that complies with the same requirement. Businesses should use reasonable security measures to detect fraudulent identity verification procedures and prevent the unauthorized access to, or deletion of, a consumer's PI.

For password-protected accounts, business are to verify the consumer's identity through its existing authentication practices if they are consistent with the CCPA. Businesses must also require consumers making requests through password-protected accounts re-authenticate their identities before responding to a deletion or right to know request.

There is also a two-tier verification process allowed for non-password protected accounts, which requires businesses verify requests to know categories of PI to a "reasonable degree of certainty." To do so, a business can match two pieces of consumer-provided PI with PI maintained by the business. For requests to know specific pieces of information, however, a business must verify to a reasonably higher degree of certainty, which can be done by matching three pieces of consumer-provided PI with PI maintained by the business.

Specific Response Obligations

Upon receipt of a verified consumer request to delete personal information, the business must delete that consumer's personal information within 45 days. While extensions of up to an additional 45 days can be asserted under unusual circumstances, businesses should develop a process for responding to consumer rights requests.

Special Requirements for Businesses that Sell PI

As mentioned earlier, there are additional requirements for businesses that sell PI. The most significant of those is that the business must provide on its business homepage titled "Do Not Sell My Personal Information" and a separate landing page for the same.

In addition, a business must update its privacy policy (or policies), or a California-specific portion of the privacy policy, to include a separate link to the new "Do Not Sell My Personal Information" page.

Upon receipt of a verified consumer request for information about the sale of that consumer's personal information, a business must provide the consumer with a report within 45 days that includes the following information from the preceding 12 months:

- Categories of personal information that the business has collected about the consumer;
- Categories of personal information that the business has sold about the consumer;
- Categories of third parties to whom the business has sold the consumer's personal information; and
- The categories of personal information about the consumer that the business disclosed to a third party (or parties) for a business purpose.

Interdependent Business Obligations

In addition to the aforementioned obligations, the CCPA also requires businesses to engage in the following independent business obligations.

Employee Training

The CCPA requires businesses to train employees handling consumer inquiries on the requirements related to CCPA-provided consumer rights and business obligations. Businesses are obligated to ensure that employees know how to direct

consumers to exercise their rights under the law.

Execute Vendor Contracts Containing Specific Criteria

Businesses that engage vendors to handle PI must execute written contracts with specific criteria with those vendors if they want to shift liability to the vendor for any violations of the CCPA caused by the vendor. If the vendor is defined as a "service provider" under the CCPA, it must have a written contract that limits processing to the business purpose of the contract.

If the vendor is defined as a "person" under the statute, among other requirements, the contract should prohibit vendors from selling, retaining, using or disclosing the PI outside of the direct business relationship with the business. The contract must also include a certification from the vendor that it understands the restrictions and will comply with them.

What Are Implications for B2B Customer Contact Data?

AB-135, which was signed into law, will exempt B2B contact data from a number of the CCPA's provisions for "personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit or government agency." Section 1978.145(h).

The exemption is a limited 1-year exemption, which means that, if the legislature does not take action by January 1, 2021, the exemption will be lifted and all B2B data will be subject to all provisions of the CCPA.

The exemption applies to the following specific provisions:

- Section 1798.100 (Abbreviated right to know);
- Section 1798.105 (Right to deletion);
- Section 1778.110 (Expanded right of disclosure);
- Section 1798.115 (Right to know of sale);
- Section 1778.130 (Data subject request rights); and
- Section 1798.135 (Website link to opt-out of sale).

The CCPA will still apply to the following provisions:

- Section 1798.120 (Opt-out of the sale of personal information or the disclosure of personal information for a business purpose);
- Section 1798.125 (Non-discrimination); and
- Section 1798.150 (Private right of action).

What this means in application is that for the next year, B2B businesses will largely not have to comply with the CCPA, but, to the extent they sell personal information or disclose personal information for a business purposes, they will have to afford consumers opt-out rights. They will also have to afford consumers rights to non-discrimination if they are providing discounts on goods or services in exchange for B2B data.

Lastly, B2B contacts will have a private right of action. In application, this merely means that if B2B contact data is breached through the business's negligence, the B2B contact could sue individually under the CCPA.

What Are the Implications for Employee Information Gathered for Employment Purposes?

The same limited 1-year exemption applies to employee data, which excludes from the CCPA information collected about a person by a business while the person is acting as a job applicant, employee, owner, officer, director, or contractor of the business, to the extent that information is collected and used exclusively in the employment context.

What Are the Penalties under the CCPA?

Violations of the CCPA are enforced by the California Attorney General's office, which can issue civil monetary fines of up to $2,500 per violation, or $7,500 for each intentional violation. Currently, the California AG's office must provide notice of any alleged violation and allow for a 30-day cure period before issuing any fine.

There are a number of exceptions. First, the CCPA is pre-empted by a number of federal laws, including HIPAA, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and information subject to the Driver's Privacy Protection Act.

There are also a number of potential defenses a business may be able to use in response to data subject requests. Some of the defenses apply to all data subject requests, such as: (1) the business is not a covered entity under the CCPA; (2) the

business is not processing PI as defined by the CCPA; (3) the PI is needed to comply with federal, state or local law, investigations or subpoenas or to cooperate with law enforcement; (4) the PI is needed to defend a legal claim; (5) the business processes de-identified or aggregated data; and many others.

Similarly, there are a number of specific defenses that are only applicable in response to certain data subject requests. For example, a defense to the expanded right to know is if compliance by a business would violate an evidentiary privilege under California law and/or would prevent the business from providing the PI of a consumer to a person covered by an evidentiary privilege.

Key Takeaways

The above summary of the CCPA is just that – a summary. The CCPA is highly complex and contains many different compliance requirements that require detailed and thoughtful planning across many departments.

For a gaming and hospitality company, preparation for compliance with the CCPA will require a coordinated effort across multiple departments, including IT, legal, marketing, security, and reservations, and coordination across multiple systems where customer data is collected and tracked. For many of these companies, the data is not only kept in house, but is also collected and stored by third-party partners and vendors. The task of understanding what data resides where, who can access and process the data, and how data is replicated across internal and external systems are essential to getting a handle on CCPA compliance. If your business needs assistance in preparing for CCPA compliance, please do not hesitate to contact us.

Sara Jodka is an attorney in Dickinson Wright's Columbus office.

COALITION OF CALIFORNIA GAMING TRIBES SEEK 2020 SPORTS WAGERING BALLOT INITIATIVE

by Patrick Sullivan

Eighteen tribes from across the State of California, led by the Pechanga Band of Luiseño Indians in Southern California's Riverside County, are pursuing legalized sports wagering through a statewide voter ballot initiative on the 2020 ballot. The initiative would allow in-person, on-site sports wagering at tribal casinos and licensed racetracks – but not internet or mobile wagering.

The initiative would amend the California Constitution to add "roulette, games played with dice, and sports wagering" to those games authorized in tribal compacts, allow sports wagering at licensed racetracks, and add statutory provisions regulating such wagering to the California code. The statute would prohibit betting on high school athletics, California college team events, or greyhound racing. Sports wagering would be limited to those 21 years and older, taxed at 10% with proceeds to public safety, mental health programs, education, and the costs of regulating the industry.

The Tribes and other supporters will need to collect 997,139 valid signatures (8% of the most recent gubernatorial vote total) by June 25, 2020 to ensure the initiative is placed on the November ballot.

The effort comes in the wake of a failed non-tribal initiative in 2018 by a group called "Californians for Sports Betting," which filed a petition with the state but never collected any signatures, and a legislative initiative which failed to gain tribal support and is therefore likely to fail to reach the 2020 ballot.

With sports wagering now legal in 13 states and under consideration in a majority of states, high popular support for sports wagering, and the support of California's largest gaming tribes, the initiative has a significant chance of success.

Patrick Sullivan is an attorney in Dickinson Wright's Washington, D.C. office.