The California Consumer Privacy Act – What Hoteliers Need to Know Now

02 January 2020

Click here for the latest articles on Data Technology, Privacy & Security.

My partner, Bob Braun, senior member of JMBM’s Global Hospitality Group® and Co-Chair of the Firm’s Cybersecurity & Privacy Group, has written extensively about the California Consumer Privacy Act that became effective January 1, 2010. In his excellent article below, he describes how the CCPA will impact the hotel industry.

— Jim

CCPA: Loyalty Programs, Data Retention and the Brave New World of Privacy
by Robert E. Braun

This article first appeared in the Hotel Business Review and is reprinted with permission from www.HotelExecutive.com.

The California Consumer Privacy Act (the “CCPA” or the “Act”) is a piece of consumer privacy legislation which was signed by California Governor Jerry Brown on June 28, 2018, and goes into effect on January 1, 2020. The Act is, far and away, the strongest privacy legislation enacted in the United States at the moment (although there are a number of contenders for that honor), giving more power to consumers to control the collection and use of their private data, and is poised to have far-reaching effects on data privacy.

What is the CCPA?

It is estimated that more than 500,000 companies are directly subject to the CCPA, many of them smaller and mid-size business, where the detailed requirements of the Act – disclosure and notice procedures, opt-out rights, updating privacy policies, and revising vendor agreements – is daunting. As discussed below, many hotels and hotel companies will be directly impacted by the Act, either because their qualify as a “business” as defined in the CCPA, or because they are associated with companies – brands and management companies – that are subject to the Act. Hotel owners, managers and brands that have not grappled with the requirements of the CCPA need to move quickly to do so, or risk potential liability under the penalty provisions of the Act.

Where did the Act Come From?

In early 2018, Alistair McTaggart, a California real estate developer, led an effort to include a new privacy law – the Consumer Right to Privacy Act of 2018 – on the November 2018 California ballot. By June 2018, supporters of the initiative had gathered enough signatures to earn a place on the November ballot. In response, California legislators, working with California businesses and other interest groups, negotiated and passed a substitute bill – the CCPA – in exchange for an agreement to drop the more restrictive text in the Consumer Right to Privacy Act from the November ballot.
The Act is aggressive, and cites the March 2018 disclosure of the misuse of personal data by Cambridge Analytica, as well as the congressional hearings that followed which highlighted the fact that any personal information shared on the internet can be subject to considerable misuse and theft. This prompted the California legislature to move rapidly to protect Californians’ right to privacy by giving consumers much more control of their personal information.

Because the Act was adopted so quickly, and because it was driven by the original proposition, the Act, as entered into law, does not have the kind of guidance that helps us understand how to implement the concepts in the Act. The California Attorney General has, as required under the Act, submitted proposed regulations that assist in complying with the Act, but much more needs to be done for businesses to feel comfortable in plotting a means of compliance. It is likely that our understanding of the Act, and how businesses can comply with the Act, will evolve over the coming years.

The Act as Part of a Broader Shift in Consumer Preferences

In order to understand the impact of the Act, and how to address its many changes, businesses need to understand how it reflects an evolution in consumer attitude toward the ownership and use of personal information.

In the United States, there have been few limitations on the collection or use of personal data. There are some exceptions – financial information is regulated under the Gramm-Leach-Bliley Act, health information is governed under the Health Insurance Portability and Accountability Act, and children’s information is addressed under the Children’s Online Personal Privacy Act. But in general, personal information – names, addresses, and other identifying information – may be collected and used without significant restriction, and consumers did not typically object.

The advent of computers and the increased ability to collect, store, process and monetize information, has changed consumers’ attitudes. Companies increasingly base their business models on the ability to collect and utilize information. This is not limited to firms like Facebook and Google; a variety of firms monetize the information they collect, both by direct marketing and by sharing, or selling, the data to others. Along with the “legitimate” use, came less savory forms, like credit card fraud and identity theft. As a result, individual consumers are increasingly concerned about how their personal data is shared.

Hotels should be particularly aware of this shift, since hotels are among the businesses most targeted by bad actors, and reports of data theft are regularly reported.

Behind these changes is a significant shift in the treatment of personal information. Increasingly, the belief is that an individual should have control over his or her identifying data, and not just a limited selection of financial data, but a broad array of information – essentially, anything that could be used to identify an individual. This would include not just names, addresses and other obvious data points, but also biometric and location data, of which many of us are unaware are being collected.

Do Hotels Need to Comply with the Act?

The Act is applicable to many businesses, whether located inside or outside California. The Act applies to for-profit entities that both collect and process the personal information (as defined in the Act) of California residents and do
business in the State of California – a physical presence in California is not a requirement to becoming subject to the Act. Additionally, the business must meet at least one of the following criteria:

- Generate annual gross revenue in excess of $25 million
- Receive or share personal information of more than 50,000 California residents annually
- Derive at least 50 percent of its annual revenue by selling the personal information of California residents.

Moreover, the Act defines a business as entities with shared control, who use common trademarks or identifiers. It is thus likely that a wide variety of hotels, hotel managers and hotel brands will have to comply with the Act.

In addition, the Act requires covered businesses to impose obligations on their vendors and service providers, and businesses that are required to comply with the Act cannot do so without the active participation of their business partners. Just as brands and management companies that became subject to the European Union’s General Data Protection Regulation (the “GDPR”) require hotel owners to assume burdens under the GDPR, they will require their owners to comply with the CCPA – even if the hotel itself might not fall within the purview of the Act.

Beyond the direct application of the law, the hotel industry needs to address its privacy and security concerns. This is a tall order – every major hotel company has been the victim of significant information breaches, and many have been victimized multiple times. At the same time, hotel companies rely heavily on the trust and loyalty of their guests. The drumbeat of negative publicity regarding the ability of hotels to maintain the security and privacy of guest information has a negative impact on the reputation of individual hotels and hotel industry generally, even while one of the main commodities that hotels sell is trust – if guests do not believe they, or their personal information, are safe with a hotel, they will simply not patronize it. The issue goes beyond individual properties – it is an industry imperative.

Key Elements of the Act

**Personal Information.** The Act defines personal information broadly, to include any information that can be used to identify an individual, whether alone, or together with other information, or which can reasonably be derived from the information at hand. It specifically includes information like:

- Typical personal identifiers such as name, address, email address, social security number, and the like
- “Unique personal identifiers” as defined by the Act as “a persistent identifier that can be used to recognize a consumer, a family, or a device… over time and across different services”; including, e.g., an Internet Protocol address, cookies, user alias, or other “probabilistic identifiers
- “Personal information” as defined in California breach notification laws
- Characteristics relevant to protected classifications (e.g., race, gender, sexual orientation)
- Commercial information such as purchase or consuming histories
- Biometric information
- Internet activity, such as browsing history, search history, etc.
- Geolocation data
- Audio, electronic, visual, thermal, olfactory, or similar information
- Professional or employment-related information
- Education information
Inferences drawn from any of the foregoing information to create a consumer profile

**Consumer Protections under the CCPA.** The CCPA provides four key rights to consumers:

- **Right to Know:** Consumers have the right to know at or before the point of collection what personal information a business collects and for what purposes—such information would typically be provided through a public facing privacy policy.
- **Right to Opt Out:** Consumers have the right, at any time, to direct a business not to sell their personal information to third parties. For consumers who are under 13- to 16-years-old, businesses may not sell their personal information without an affirmative opt in by the consumer (for consumers 13 to 16 years old) or by the consumer’s parent or guardian.
- **Right to Delete:** Consumers have the right to request that a business delete any personal information the business has collected, with certain exceptions.
- **Right of Non-Discrimination:** A business may not discriminate against a consumer because the consumer exercises any of the consumer’s rights under this title. The Act gives, as examples, charging different prices or rates for goods or services, or providing a different level or quality of goods or services. For hotels, this means that loyalty programs will be under scrutiny, and to pass muster, their sponsors must identify the value associated with the right to use personal information, and how that was determined.

**Potential Liability Under the CCPA**

The Act authorizes the California Attorney General to bring a civil action against a business found to be in violation of any provision of the CCPA that is not cured within 30 days of notice of the alleged noncompliance. The business may be subject to an injunction and a fine of $2,500 for each violation, or $7,500 for each intentional violation.

In addition to the Attorney General, the Act gives consumers a limited right of action under the CCPA, if the consumer’s non-encrypted or nonredacted personal information (as that term is defined in the Act, and which is a narrower and more typical definition of personal information found in California’s pre-existing breach notification law) is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures. In such a case, the consumer may recover damages in an amount not less than $100 and not greater than $750 per incident, or actual damages, whichever is greater.

**Complying with the CCPA**

Hotels that are subject to the requirements of the CCPA will need to implement new systems and procedures to comply with the statute. Among those steps are the following:

**Data Mapping:** Businesses need to identify all of the personal information pertaining to California residents and households that they collect, where they obtain it, where it is located, who uses it, and for what purpose. Data mapping is an essential part of allowing a business to determine the information needed to add the newly required disclosures to its privacy policies, to prepare for data access, deletion, and portability requests, to secure prior consent for data sharing from parents or minors, and to comply with opt-out requests from consumers.
Privacy Policy: The CCPA includes specific requirements for applicable public facing privacy policies, including requirements to:

- Notify consumers of the categories of personal information to be collected and/or sold, the purposes for which the information shall be used, and an identification of any third parties to whom personal information will be disclosed or sold
- Provide notice of the intention to sell any California consumers’ personal information
- Describe California consumers’ rights, including the rights of access and deletion, and the right to opt-out
- Provide a separate link to the “Do Not Sell” web page

Do Not Sell: The Act requires each business to provide a clear and conspicuous “Do Not Sell My Personal Information” link on the business’ Internet homepage, as well as its privacy statement and wherever it collects data, directing users to a web page enabling them to opt out of the sale of their personal information. If a business does not sell personal information, it must say so explicitly.

Access Requests: The Act requires each business to designate at least two methods for consumers to submit data access requests, one of which must be a toll-free telephone number. The business must respond to request for data access, deletion, and portability within 45 days, so will need to develop procedures for tracking and responding to requests, and for applying accepted verification procedures.

Verification: A business may only respond to verified requests, so it must establish procedures for properly verifying the identity and authorization of persons who make requests for data access, deletion, or portability, and to opt-out or opt-back-in to data monetization.

Parting Thoughts

Hotels and hotel companies that are subject to the CCPA and that have not started to implement compliance procedures should begin the compliance process without delay. There have been rumors of preemptive federal privacy legislation, but it is clear that nothing will be adopted before the CCPA goes into effect in 2020. Moreover, even if federal legislation is enacted, it will inevitably include many of the same fundamental provisions as those found in the CCPA, such as requirements for transparency, rights of access and deletion, opt-out of selling and/or marketing use of consumer data, and potentially some form of non-discrimination clause.

Hotels should consider finding ways to use the CCPA, and compliance with the CCPA, to their advantage. Privacy, particularly when imposed by statute, is often seen solely as an expense, as a cost of doing business. Hotels can embrace privacy as a means of separating themselves from their competitors. In an environment where privacy is increasingly seen as an important asset, hotels can emphasize their commitment to the same values as their guests.
Bob Braun is a Senior Member of JMBM’s Global Hospitality Group® and is Co-Chair of the Firm’s Cybersecurity & Privacy Group. Bob has more than 20 years experience in representing hotel owners and developers in their contracts, relationships and disputes with hotel managers, licensor, franchisor and brands, and has negotiated hundreds of hotel management and franchise agreements. His practice includes experience with virtually every significant hotel brand and manager. Bob also advises clients on condo hotel securities issues and many transactional matters, including entity formation, financing, and joint ventures, and works with companies on their data technology, privacy and security matters. These include software licensing, cloud computing, e-commerce, data processing and outsourcing agreements for the hospitality industry.

In addition, Bob is a frequent lecturer as an expert in technology, privacy and data security issues, and is one of only two attorneys in the 2015 listing of SuperLawyers to be recognized for expertise in Information Technology. Bob is on the Advisory Board of the Information Systems Security Association, Los Angeles chapter, and a member of the International Association of Privacy Professionals. Contact Bob Braun at 310.785.5331 or rbraun@jmbm.com.

This is Jim Butler, author of www.HotelLawBlog.com and hotel lawyer, signing off. Please contact us if you would like to discuss any issues or development that affect your hotel interests. We would like to see if our experience might help you create value or avoid unnecessary pitfalls. Who’s your hotel lawyer?

Jim Butler is a founding partner of JMBM and JMBM’s Global Hospitality Group® which provides business and legal advice to hotel owners, developers, independent operators and investors. This advice covers hotel purchase, sale, development, financing, franchise, management, labor & employment, litigation, ADA, IP, EB-5 matters and many other areas. Click here for a more detailed listing of how we might help you.

Jim is recognized as one of the top hotel lawyers in the world and has led the Global Hospitality Group® in more than $87 billion of hotel transactions and more than 3,900 hotel properties located around the globe.

Contact Jim at +1-310-201-3526 or JButler@jmbm.com

Hotels we have worked on over the years. Visit our hotel photo gallery to see some of the more than 3,900 properties around the globe that the hotel lawyers of the Global Hospitality Group® have been involved with, on behalf of our clients. For a more comprehensive list of hotels properties and projects we have worked on, see our Credentials.