CARLTON FIELDS

California Consumer Privacy Act:
A Reference Guide for Compliance

California Consumer Privacy Act:
A Reference Guide for Compliance

Table of Contents

Dates reflect the date of original publication. For additional updates, please consult your Carlton Fields lawyer.

California Passes Stringent Privacy Law Akin to GDPR

July 9, 2019

Barry Leigh Weissman

Steven Blickensderfer

Last month, California passed a sweeping new privacy law that will impact many businesses. The California Consumer Privacy Act of 2018, AB 375 (CCPA) is the first U.S. law to grant consumers extensive rights as to their personal information and how businesses handle it. Similar to the European Union's newly-minted GDPR, the CCPA is intended to further the right of privacy, which is constitutional in nature in California. The law requires companies to be transparent with consumers regarding the categories of personal information being collected and how that information is disclosed and shared. Specifically, the law will grant consumers increased access to their personal information, the option to direct businesses to delete that information, and additional control concerning the sale and sharing of their personal information. Should any consumer exercise these rights, the CCPA prohibits businesses from discriminating against them by charging a different price or providing a different service in response.

This alert informs U.S. companies about the rights and obligations the CCPA creates, as well as the scope of its application. Although the current version of the law is expected to be modified by amendments prior to its January 1, 2020 enactment, businesses should begin to prepare for the change. California continues to set the bar in terms of U.S. privacy law, and this landmark development will undoubtedly spur the enactment of similar data privacy laws in other states.

New Rights and Obligations under the CCPA: Key Takeaways

The CCPA grants "consumers," defined as California residents, more power and control over their personal information held by businesses than ever before. Under the new law, California consumers will have the power to direct businesses to delete or refrain from selling their personal information under certain circumstances. The CCPA also completely prohibits businesses from selling the personal information of a consumer between 13 and 16 years of age unless the sale is affirmatively authorized by the consumer or their parent or guardian. In the case of consumers under the age of 13, the authorization must be by the parent or guardian.

The CCPA grants rights that will give consumers access to information about the data collection and processing practices of businesses, including information concerning:

1. the categories and specific pieces of personal information businesses are collecting and processing about the consumer;
2. whether personal information is being sold;
3. the purpose for which the personal information is being collected or processed; and
4. the categories of third parties with whom the business shares or sells the personal information.

The CCPA also contains detailed requirements regarding consumer requests. First, businesses must make available to consumers two or more designated methods for submitting requests for information, including a toll-free telephone number and website if the company maintains one. Second, businesses must disclose and deliver the requested information to consumers free of charge within 45 calendar days. Businesses will also be expected to comply with the Act's specific instructions regarding the content of their websites and online privacy policies. Websites must contain clear and conspicuous links that enable customers to opt out of the sale of their personal information, although the law allows for some flexibility on how to implement certain of these new changes.

Businesses will be prohibited from discriminating against consumers who exercise their privacy rights by denying them goods or services, providing a different level of quality of those

goods or services, or charging different prices or rates. Businesses will even be prohibited from ***suggesting*** that they may deny services or charge a different price if consumers exercise these privacy rights. However, the law allows businesses to charge a different price, or offer a different quality of goods or services if the difference "is directly related to the value provided to the consumer by the consumer's data." Despite these restrictions, the new law does authorize businesses to offer financial incentives for the collection of personal information, including payments to consumers.

The Scope of the New Law

Similar to the GDPR's definition of personal data, the CCPA applies to "personal information" that is broadly defined to include IP addresses, browsing history, and even inferences drawn from any of the identified information that creates a profile reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

As for whom the law will impact, the CCPA specifies that it will only apply to certain types of businesses that collect and process the personal information of California consumers. Specifically, the law defines "business" to mean one that is either a sole proprietorship, partnership, LLC, corporation, association or other legal entity organized or operated for the financial benefit of its shareholders or other owners, that (1) collects consumers' personal information, (2) determines the purposes and means of the processing of consumers' personal information, and (3) does business in California. The business must also satisfy one of the following conditions:

1. have annual gross revenues in excess of $25 million;
2. alone or in combination, annually buy, sell, or receive or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or
3. derive 50 percent or more of annual revenues from selling consumers' personal information.

The CCPA will also apply to any entity that controls or is controlled by a qualifying business and that shares common branding with that business. While the definition of "business" makes clear that bigger businesses like Google and Facebook will fall within the scope of the CCPA, even small startups could be subject to CCPA requirements if they are in the business of buying, selling, receiving, or sharing the personal information of California consumers.

Importantly, the law will not apply to protected health information that is already subject to regulation under HIPAA or personal information covered by the Fair Credit Reporting Act. However, the same sweeping exemption does not apply to personal information subject to regulation by the Driver's Privacy Protection Act and the Gramm-Leach Bliley Act (GLBA). In those cases, the CCPA would only apply to the extent it does not conflict with those laws. Applying these different laws in practice may prove complex for businesses. Because the exemptions apply specifically to *information* that is subject to regulation, and not entire entities, businesses will need to pay close attention to the particular information at issue in each instance.

The CCPA also includes an extraterritorial limitation which states that the law will not restrict a business's ability to collect or sell consumer personal information so long as "every aspect of that commercial conduct" occurs outside California. This means that the consumer must be outside of California while their data is being collected and processed, and the collection and processing must take place outside of the state as well.

Consequences of Non-Compliance

The statutory damages allowed for under the CCPA could be staggering, as they can range between $100 and $750 "per incident or actual damages, whichever is greater." In determining the amount of damages, courts may consider the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct and length of time over which it occurred, the willfulness of the misconduct, and the defendant's assets, liabilities, and net worth. After certain requirements are met, the law allows consumers to bring a private right of action in the event their personal information is subject to unauthorized access or disclosure. Prior to suit, businesses must be given notice and the opportunity to cure any alleged noncompliance within 30 days. However, no notice is required before an individual consumer initiates an action "solely for actual pecuniary

damages suffered as a result of the alleged violations" of the law. The Attorney General may also institute a civil action, and can seek up to $7,500 for each intentional violation. The law will create a new Consumer Privacy Fund to offset costs incurred by the Attorney General and the courts in these efforts.

What Prompted the New Legislation?

A brief history of the CCPA's passage helps to contextualize the new law. The bill was passed swiftly in a last-minute effort to evade a ballot measure initiated by a real estate mogul. The ballot initiative was the first attempt at this sweeping privacy law, albeit a stricter version, and would have been voted on in November 2018. However, an initiative passed by the people would be much more difficult to amend in the future than a law passed by the legislature. The technology industry and the legislature negotiated with the ballot initiative campaign, which ultimately agreed to withdraw the proposal if the CCPA, in its current form, was passed. The legislature fast-tracked the bill and it was passed in a matter of days. Because the current form of the CCPA was drafted so hastily, it is expected to undergo some change between now and its January 1, 2020 effective date.

The CCPA's 50,000 California Resident Requirement - Easier to Meet Than It Might Seem

August 6, 2019

Gregory A. Gidus

When the California Consumer Privacy Act (CCPA) takes effect in January 2020, it will grant California residents new rights regarding their personal information and will impose new and significant obligations on businesses that collect this information. The CCPA applies to all types of for-profit business entities — from sole proprietorships to corporations — that meet one of three criteria: (1) the business has gross revenues in excess of $25 million; (2) the business annually buys, receives, sells, or shares the personal information of 50,000 or more California residents; or (3) the business derives 50% or more of its annual revenues from selling California residents' personal information. Cal. Civ. Code § 1798.140(c).

At first blush, it might appear that the CCPA will not apply to many businesses, especially small businesses outside California that are not involved in brokering data. But a deeper dive into the CCPA demonstrates that the 50,000-consumer threshold is rather easy to overcome and could apply to many U.S. and foreign businesses.

First, even if a business is not based in California and does not have a physical location in California, the CCPA still applies if the business annually collects the data of 50,000 or more California residents. Moreover, the CCPA broadly defines personal information to encompass "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." Cal. Civ. Code § 1798.140(o)(1). This includes not only the usual personal information categories such as names, addresses, Social Security numbers, and driver's license numbers, but also additional categories such as IP addresses, purchasing or consuming histories, browsing history, and information regarding a consumer's interaction with a website. Cal. Civ. Code § 1798.140(o)(1)A–J.

Consequently, if a business's website collects IP addresses, like most do, amassing the personal information of 50,000 California consumers could happen quickly. In fact, this threshold would be met if the website were visited by an average of just 137 California residents per day over the course of the year. This could also be a concern for bloggers and other individuals realizing profits from social media, whose websites may collect personal information from more than 50,000 Californians every year.

Businesses should also be aware that they could be subject to the CCPA if their parent or subsidiary company annually collects the personal information of 50,000 or more California residents. Under section 1798.140(c)(2), "business" is defined to include any entity that controls or is controlled by a business and that shares "common branding," meaning a shared name, service mark, or trademark.

In this digital age in which sales are conducted online and internet advertising is ubiquitous, the CCPA has the potential to affect many more businesses than it would seem at first glance. In order to avoid potential fines and penalties, businesses should carefully assess if the CCPA applies and, if so, ensure that they are in compliance.

It's 3 a.m., Do You Know Where Your Data Is? The Importance of Data Mapping and the California Consumer Privacy Act

July 29, 2019

Joseph W. Swanson

The California Consumer Privacy Act (CCPA) takes effect in January and imposes a number of requirements on how businesses collect, use, and transfer personal information. Among other things, a business subject to the CCPA must be able to respond to consumers' requests for information about what personal information the business collects and whether the business sells that information. Businesses must also provide the consumer's personal information to that individual and delete it if requested to do so.

The California attorney general is authorized to enforce the CCPA. In addition, the CCPA provides a private right of action — with statutory damages of $100 up to $750 per consumer per incident — for data breaches caused by a business's failure to implement reasonable security measures.

Given those stakes, organizations that do business in California and that collect personal information relating to California residents need to prepare for the law's onset. The myriad obligations created by the CCPA, and the fact that those obligations do not neatly align with those created by the EU's GDPR and other privacy regulations, may seem overwhelming to businesses.

But those organizations can attack compliance in a disciplined manner by asking themselves some threshold questions: *What personal information do we collect, where is it stored, and what do we do with it?* These questions are part of a process called "data mapping," in which an organization evaluates the data it collects, where it is stored, and how (if at all) it is shared with third parties. This process is essential for an organization to be able to act on a consumer's request related to his or her personal information under the CCPA.

A business that has previously engaged in data mapping can and should leverage that earlier work, but the organization should be mindful of some unique aspects of the CCPA. First, the CCPA defines "personal information" to include some relatively novel items, such as biometric information, education information, geolocation information, and household information. And, second, the CCPA defines the "sale" of personal information to include selling, transferring, or communicating that information to a third party for money or "other valuable consideration." Given the breadth of these definitions, a business engaged in data mapping for the CCPA should consider whether to supplement previous data mapping that may not have incorporated these concepts. And, some organizations may find themselves data mapping for the first time.

A business can deploy its own resources and/or work with third-party service providers to complete data mapping. If using a third party to assist, the business may want that third party retained by counsel so as to better protect the work under the attorney-client privilege. The business should document its data mapping so that there is a defensible record of its attempts to comply with the law. That record will also be helpful when updating the data mapping in the future, as other jurisdictions will inevitably pass additional CCPA-like provisions.

Is Your Organization Ready for the CCPA? The Importance of an Incident Response Guide

July 3, 2019

Joseph W. Swanson

With the California Consumer Privacy Act (CCPA) set to take effect in January 2020, organizations should be hard at work preparing. That work includes data mapping, understanding the extent to which the organization sells personal information, reviewing and revising vendor contracts, and establishing mechanisms to handle data requests. For many organizations, that is a daunting "to-do" list with little time to get it all done. The good news is that one item on an organization's CCPA punch list should already be in place: the incident response guide.

An incident response guide is the organization's playbook for how to investigate, respond to, and remediate a data security incident or breach. The best guides are short, easy to follow, and clearly lay out roles and responsibilities — and contact information — for the organization's incident response team. The team should be familiar with the guide from conducting tabletop exercises and revising the document periodically.

The benefits of a functional and well-tested guide are widely known. As an initial matter, the process of drafting a guide prompts an organization to evaluate its cybersecurity posture, identify risks, and marshal resources to be ready for an incident. When there is an incident, the guide should help the organization identify and respond in a more timely and disciplined manner, which can dramatically cut down on response costs. In fact, the Ponemon Institute's annual survey of data breach costs routinely notes that response costs are lower when data breaches are identified and contained as quickly as possible.

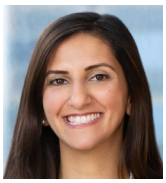
The CCPA's looming effective date underscores the need for an incident response guide. Among other things, the CCPA confers a private right of action — with statutory damages ranging from $100 to $750 per consumer per incident — for breaches involving personal information that result from an organization's failure to "maintain reasonable security procedures and practices." This private right of action, which explicitly permits class actions, means that organizations subject to the CCPA must assess their cybersecurity posture as part of their preparations. That assessment includes ensuring that an incident response guide is in place. The guide will help the organization detect and respond to a potential incident, possibly preventing that incident from amounting to a breach that could give rise to a claim. And if there is litigation, the presence of an incident response guide will be among the features that defense counsel will tout in defending the organization's "reasonable security procedures and practices."

The CCPA heralds a new era for cybersecurity and privacy in the United States, and getting ready for the law is no small task. Organizations would be well-served to update and test their incident response guides now so that they can focus on other, more labor-intensive aspects of their CCPA preparations.

How Broad Is the Scope of the CCPA's Standing Provision Under Section 1798.150(a)(1)?

July 18, 2019

Steven B. Weisburd



Farah Z. Alkayed

Once the California Consumer Privacy Act (CCPA) takes effect on January 1, 2020, the California courts will be inundated with a litany of interpretive questions. One that will no doubt surface concerns the proper interpretation and scope of the standing provision in the CCPA's private right of action for statutory and actual damages under Section 1798.150(a)(1). The California Legislature granted standing under this provision to "[a]ny consumer whose nonencrypted or nonredacted personal information ... is subject to an 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 and practices appropriate to the nature of the information to protect the personal information."

By its terms, this provision certainly would afford standing to a person who is a "consumer" in California and who is a victim of "an unauthorized access and exfiltration, theft, or disclosure" of his or her protected "personal information" that is caused by a "business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." But is the scope of the statutory standing provision limited to those who are actual victims of identity theft or other harm caused by an actual unauthorized disclosure, access, or exfiltration? Is the statutory language susceptible to a broader construction by the California courts?

Proponents of a broader construction can be expected to advocate that any consumer who is merely *subject* to the risk of possibly having some unauthorized access or theft or disclosure occur "as a result of" any "business's violation of the duty to implement and maintain reasonable security procedures and practices" should also have standing to sue under Section 1798.150(a)(1). The plaintiffs' bar may be expected to contend that any consumer "subject to" such a risk should have standing to sue — *before* the occurrence of any data breach or identity theft or other tangible harm — because the CCPA mandates that all businesses comply with their "duty to implement and maintain reasonable security procedures and practices" that are appropriate in light of the nature of the personal information at issue.

If courts were to entertain such an open-ended construction of Section 1798.150(a)(1)'s standing provision, that would open the proverbial floodgates of litigation against virtually any company, where the plaintiffs' bar will likely contend that the reasonableness of any business's security procedures and practices should be a triable issue of disputed fact. When coupled with the CCPA's statutory damages provisions, litigation concerning the proper scope of the CCPA's statutory standing provision may take on monumental significance for all affected businesses.

As courts are called upon to interpret the CCPA's standing provision, they will apply familiar rules of statutory interpretation — focusing on the plain meaning of the statutory text, and any relevant portions of the legislative history. *See, e.g., Horwich v. Superior Court*, 21 Cal. 4th 272, 276-77 (1999). And "[w]hen attempting to ascertain the ordinary, usual meaning of a word, courts appropriately refer to the dictionary definition of that word." *Wasatch Prop. Mgmt. v. Degrate*, 35 Cal. 4th 1111, 1121-22 (2005). So, here, one can expect the proponents of a broad standing analysis to point to Merriam-Webster's definition of "subject to" as meaning "affected by or *possibly affected by* (something)." (Emphasis added). This could be used to argue that a mere *possible risk* of disclosure or theft due to a company's violation of its duty to implement and maintain reasonable security procedures and practices should be enough for any individual consumer to have standing to sue under the CCPA.

But could the California Legislature possibly have intended such a dangerously overbroad interpretation of standing under Section 1798.150(a)(1)? Likely not. Indeed, there is no support for such a broad construction of the standing provision in either the legislative

history or preamble to the bill. Nor is there any reference to standing being afforded to those who are merely subject to the possible risk of having their personal information compromised. Quite the opposite.

The Senate Judiciary Committee's report on AB 375 (June 25, 2018) recites the text of the statutory standing provision, including its "subject to" language, but then specifically explains at page 21 that "[t]his would create a private right of action for *those whose personal information has been compromised* through the failure of a business to properly maintain that information." (Emphasis added). Likewise, the CCPA's preamble indicates that the statute "would provide a private right of action in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal information," without any mention of a mere risk of such access or theft. Similarly, in its discussion of the Legislature's "intent" and what "rights" the CCPA is designed to ensure, Section 2 is entirely silent as to any supposed "right" to be free from a mere risk of disclosure. *See* CCPA, Section 2(i) ("[I]t is the intent of the Legislature to further Californians' right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights: (1) The right of Californians to know what personal information is being collected about them. (2) The right of Californians to know whether their personal information is sold or disclosed and to whom. (3) The right of Californians to say no to the sale of personal information. (4) The right of Californians to access their personal information. (5) The right of Californians to equal service and price, even if they exercise their privacy rights.").

Accordingly, even if the statutory language might be susceptible of an overbroad interpretation that affords immediate statutory standing to any consumer who is merely subject to a possible risk of having his or her personal information stolen or accessed as a result of a business's failure to implement and maintain reasonable security procedures and practices, the absence of any support for such a broad interpretation in the legislative history or full statutory regime should derail such efforts from the plaintiffs' bar. As the California Supreme Court has held, "[t]he fundamental purpose of statutory construction is to ascertain the intent of the lawmakers so as to effectuate the purpose of the law. In order to determine this intent, we begin by examining the language of the statute. But it is a settled principle of statutory interpretation that language of a statute should not be given a literal meaning if doing so would result in absurd consequences which the Legislature did not intend. Thus, the intent prevails over the letter, and the letter will, if possible, be so read as to conform to the spirit of the act." *Horwich*, 21 Cal. 4th at 276 (citations and internal quotations omitted).

Show Me the Money: How the CCPA Provides a Mechanism for Consumers to Monetize Their Personal Data

August 4, 2019

Joshua L. Gutter

Under section 1798.125(b) of the California Consumer Privacy Act of 2018 (CCPA), "[a] business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data." Accordingly, this provision of the CCPA offers consumers a mechanism to monetize their personal data, and time will tell regarding how this provision will work in application once the statute becomes effective on January 1, 2020. Nevertheless, in an era that continues to emphasize privacy rights, the CCPA attempts to give bargaining power to consumers and align their economic interests with the businesses that collect such personal information.

Historically speaking, companies have monetized personal data in a number of ways. Per the MIT Sloan Management Review, "There are two primary paths to data monetization. The first is internal and focuses on leveraging data to improve a company's operations, productivity, and products and services, and also enable ongoing, personalized dialogs with customers. The second path is external and involves creating new revenue streams by making data available to customers and partners." With respect to the former, it is not uncommon to see privacy policies whereby the users of an application or website consent to their personal data being analyzed to improve a platform or enhance a user experience. But with respect to the latter, companies also sell such personal data to a variety of third parties, including other businesses, marketing firms, and data brokers.

As stated by Tim Sparapani, former director of public policy at Facebook and former privacy lawyer with the American Civil Liberties Union, "Most retailers are finding out that they have a secondary source of income, which is that the data about their customers is probably just about as valuable, maybe even more so, than the actual product or service that they're selling to the individual. So, there's a whole new revenue stream that many companies have found." As a result of this, a variety of marketplaces have been created for businesses to buy and sell data, which can exclude any type of financial remuneration for the consumer (and on a related note, because of this booming industry with little oversight, Vermont is an example of a state that has begun regulating data brokers, and the public can see a list of companies that are transacting with consumers' personal information).

Refocusing on California, until the CCPA goes live, it is hard to envision how section 1798.125(b) will be used by consumers and whether it will actually incentivize them to sell their personal data. Last year, the BBC investigated this very question of "Can you make money selling your data?" and the economic returns did not seem significant from the methods that were deployed. Notwithstanding those efforts, it is possible that future technology platforms and shifting regulatory environments (as well as the overall evolution of the internet) will change that. If such change happens, consumers might be able to sell their personal data for higher returns and cut into the revenue streams that are currently being dominated by businesses, data brokers, and other third parties.

The CCPA's Contractual Requirements Between Covered Businesses and Service Providers

July 23, 2019

Steven Blickensderfer

There are many facets to California's new data privacy law, the California Consumer Privacy Act of 2018 (CCPA), that are generating a lot of buzz — such as the new rights afforded to California consumers and the broad definition of personal information. There is an equally impactful, yet often forgotten, obligation required by the CCPA that warrants attention. That is the need to make certain representations in written contracts between covered businesses and service providers.

The CCPA generally impacts three types of entities: (1) covered businesses; (2) service providers; and (3) third parties. There are certain advantages to being considered a service provider over a third party. For instance, if a business shares personal information with a third party, that can trigger certain disclosures that must be made to the consumer. *See* Cal. Civ. Code § 1798.110(a)(4). Likewise, third parties must provide notice to consumers before "selling" personal information they receive to others (as that word is broadly defined in the CCPA), as well as a mechanism by which consumers can exercise their newfound right to opt out. *See* Cal. Civ. Code §§ 1798.115(d), 1798.120(a). Any one of these obligations could prove costly for an entity to implement in practice depending on the circumstances.

Transferring personal information to a service provider, by contrast, does not necessarily trigger those additional obligations. But an entity cannot simply call itself a service provider. There are certain thresholds that must be met as set forth in the statute.

First, there must be a written contract in place between the covered business and the service provider, such as a service agreement. *See* Cal. Civ. Code § 1798.140(v). The absence of any agreement or written contract is a strong indication, if not concrete proof, that the entity receiving the personal information is a third party.

Second, the written contract must include certain representations. The CCPA requires the written contract to state that the service provider will not retain, use, or disclose the personal information for any purpose other than for the specific purpose of performing the services set forth in the contract. *See* Cal. Civ. Code § 1798.140(v). The parties must further agree to limit the collection, sale, or use of the personal information disclosed except as necessary to perform the "business purpose" for which the service provider was retained. *See* Cal. Civ. Code § 1798.140(w)(2). The CCPA anticipates that the "business purpose" will relate to a covered business's "operational" needs, such as auditing, detecting security incidents, fulfilling orders and transactions, processing payments, etc. *See* Cal. Civ. Code § 1798.140(d). Finally, the parties must represent that they have read and understand the CCPA's requirements. *See* Cal. Civ. Code § 1798.140(w)(2).

Third, those representations must be accurate. A company that receives and uses personal information for reasons beyond the operational needs of the covered business will likely be considered a third party, regardless of the representations in the written contract. Where that is unavoidable, the company must be sure to weigh the benefits of processing the personal information against the risks of being considered a third party and the costs of additional CCPA compliance.

In situations where these representations can be made and are accurate, they are simple enough to implement and could be low-hanging fruit for a business looking to demonstrate CCPA compliance by January 1, 2020. Following the passage of the European Union's General Data Protection Regulation (GDPR), many U.S.-based businesses have been forced to enter into data processing agreements (DPAs) to supplement existing service agreements. While the CCPA does not necessarily require a DPA, more and more companies' global privacy compliance programs are requiring one to do business. In those instances, it may make the most sense to include these representations in the DPA itself. Otherwise, a business could include them in a stand-alone addendum to its existing written service contracts.

The CCPA's Impact on Businesses Processing Personal Data of Minors and Children

August 6, 2019

Steven Blickensderfer

Businesses that offer services or have websites used by minors in California will have a new law to worry about come January 1, 2020 — the California Consumer Privacy Act of 2018 (CCPA). Businesses offering such services are already impacted by the FTC's Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-6506, and California's "Online Eraser Law," Cal. Bus. & Prof. Code §§ 22580-22582. These laws aim to protect minors and children in certain jurisdictions. Precisely how they function, however, varies in material ways, resulting in a complex set of questions as to which law applies, when, and to whom.

COPPA protects children anywhere in the United States and defines a child as an individual under the age of 13. *See* 16 C.F.R. § 312.2. COPPA operates by, among other things, requiring verifiable parental consent before collecting personal information from children under 13, and giving parents the ability to access and delete that data. California's Online Eraser Law protects minors, defined as individuals under the age of 18, Cal. Bus. & Prof. Code § 22580(d), by allowing them to request, and obtain removal of, content or information posted by them on a website, online service, or mobile application. Businesses, wherever located, must comply with these laws if their website or service is directed to minors, or if the business has actual knowledge that a minor is using its website or service.

The CCPA falls somewhere in the middle of this regulatory trifecta. It prohibits the "selling" of personal information (as that term is broadly defined) of California consumers under the age of 16, absent consent. Cal. Civ. Code § 1798.120(c). If the individual is between 13 and 16 years of age, the minor can "affirmatively authorize[]" the sale of the data. But if the minor is less than 13 years of age, the consumer's parent or guardian must give the consent. While the CCPA does not elaborate on the requirements for consent, use of the word "affirmatively" seemingly rules out consent through opt-out methods, such as pre-checked boxes.

Consistent with the other two statutes, a business must comply with the CCPA's consent obligations if it has actual knowledge of the minor's age. A business will be held to have actual knowledge if it willfully disregards the consumer's age. The CCPA does not define what it means to willfully disregard a minor's age. Nevertheless, one could envision that a regulator would equate a minor-oriented website or online service — such as a video game or mobile application appealing to that target audience — that fails to screen the user's age prior to use as willfully disregarding the consumer's age.

Going forward, businesses with products or services online that collect and process data from minors should be aware of the variations between these laws, including the new two-tiered consent obligation of the CCPA. Privacy policies and online notices should be revisited to account for the varying requirements of obtaining consent depending on the user's age. Does that mean the age for consent to access a particular website or play a video game should be 18? 16? 13? The answer will depend on the circumstances. Passage of the CCPA nevertheless serves as a reminder that businesses must be mindful of the data they collect, especially data belonging to minors.

This article was co-authored by Carlton Fields Law Innovation Technology Clerk Talia Boiangin.

The CCPA Has Placed a Mandatory Link on Your Company's Homepage

July 26, 2019

John E. Clabby

If a company sells personal information of California consumers, then the California Legislature has claimed real estate on its homepage. This article summarizes this new requirement of a "Do Not Sell My Personal Information" link and provides some practical guidance.

The California Consumer Privacy Act of 2018 (CCPA) in certain instances requires a business to "[p]rovide a clear and conspicuous link on the business' Internet homepage, titled 'Do Not Sell My Personal Information,' to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer's personal information." Sec. 1798.135(a)(1).

This requirement applies only to businesses that "sell" personal information about California consumers to third parties. Sec. 1798.120(a). "Sell" in the world of the CCPA does not really mean "sell" — it means share for any benefit at all. Sec. 1798.140(t). What this homepage requirement does is make operational the CCPA's much-discussed "right to opt out," that is, a consumer's right to demand that a company stop transferring his or her personal data for value to others. Sec. 1790.120(a).

Compliance requires more than a cosmetic website tweak. By January 1, 2020, the effective date of the CCPA, the company must also:

- Construct a back-end system that takes opt-out requests from the webpage and turns it into a reality. Sec. 1798.135(a)(4).
- Train individuals responsible for "handling consumer inquiries" on how to direct consumers to exercise the right to opt out. Sec. 1798.135(a)(3).
- Figure out a system so that the company refrains from soliciting the sale data of an opting-out customer for 12 months from the date of opting out. Sec. 1798.135(a)(5).

A website's landing page is not the only place where this "Do Not Sell My Personal Information" link must appear. A company must also install it in the company's (i) online privacy policy or policies if the business has one; and (ii) any California-specific description of consumers' privacy rights. Sec. 1798.135(a)(2). The CCPA also defines "homepage" to include "any Internet Web page where personal information is collected," suggesting that some may interpret the statute to require that the link be included on other parts of the website where the user inputs data or user data is tracked or collected. Sec. 1798.140(l).

We have already observed a number of websites adopting a separate "California privacy rights" link from its general "privacy rights" link for residents of every other state, accessible from the homepage. Such a strategy does not deploy the actual language that the statute requires for the "do not sell" link and may face compliance challenges.

A more certain way to avoid having this "do not sell" link on the common homepage, other than not selling California residents' data, is both an engineering and advertising challenge. That is, the law allows an entirely separate homepage for California residents (with the link) and one for everyone else (without the link). Sec. 1798.135(b). If a company takes California up on that challenge, it must further "take[] reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally." *Id.* We look forward to seeing enterprising web engineers experiment with what "reasonable steps" might work here.

Can You Write the California AG with Questions About CCPA Compliance?

July 11, 2019

John E. Clabby

If a company has questions about how to comply with California's new data privacy law, it may, under a remarkable provision of that law, request an opinion from California's attorney general (AG). This article analyzes that provision, notes the AG's objection to it, and discusses one proposal to change that provision before the law's January 1, 2020, effective date.

The California Consumer Privacy Act of 2018 (CCPA) raises a lot of questions about what companies must do to comply and, thankfully, provides a mechanism by which those companies can get some answers: "Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title." Sec. 1798.155(a).

That single sentence raises a host of possible issues. First, the word "opinion" has quite a different legal definition than does "guidance," but the provision uses both terms. "Opinion" usually means that the person receiving it can rely on it to some extent, including perhaps, in this context, in defense to an enforcement action.

Second, while this provision permits a business to seek an opinion, it does not by its terms require the AG to provide an answer, although one could reasonably infer that the statute did not provide California's businesses a meaningless right.

Third, the provision refers to a business "or third party," which would seem to allow pretty much anyone to solicit the AG's guidance. The CCPA gives "third party" an inverse definition, as any individual or entity *except* (i) any "business" under the CCPA; or (ii) any individual or entity to whom personal information is sent for a business purpose pursuant to a written contract that contains certain promises and provisions. Sec. 1798.140(w). The provisions working together would embrace entities beyond those regulated by the CCPA as being proper requesters to the AG and could include consumer advocates, industry groups, and even privacy lawyers. This interpretation is reinforced by Section 1798.155(a) not requiring an actual controversy as the predicate to guidance.

Fourth, the provision does not explain how the AG's response will be delivered, including whether it would be made public immediately, such as posting to the AG's website. Under California's Public Records Act and the California Constitution, businesses availing themselves of this "opinion" should anticipate, absent an exception, that the initial correspondence and the AG's response will be public.

The California AG, Xavier Becerra, had questions of his own upon reading this provision. The AG made his displeasure with the provision clear, sending a letter on August 22, 2018, to the two co-sponsors of the CCPA, likening the provision to conscripting his office into giving unlimited, free legal advice:

> Requiring the AGO to provide legal counsel at taxpayers' expense to all inquiring businesses creates the unprecedented obligation of using public funds to provide unlimited legal advice to private parties. This provision also creates a potential conflict of interest by having the AGO provide legal advice to parties who may be violating the privacy rights of Californians, the very people that the AGO is sworn to protect. What could be more unfair and unconscionable than to advantage violators of consumers' privacy by providing them with legal counsel at taxpayer expense but leaving the victims of the privacy violation on their own? I do not see how the AGO can comply with these requirements. I urge you to swiftly correct this.

The AG takes a dim view of the requesters in describing them as those who may be "violating the privacy rights of Californians." As such, he does not leave much room for what will likely be the bulk of the inquirers — those who are attempting in good faith to comply with the statute and just need some guidance on how the AG will be interpreting unclear or contested provisions.

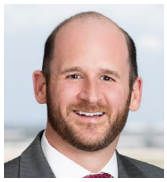
Additionally, it takes little effort to brainstorm myriad things that are "more unfair and unconscionable" than allowing businesses facing a complex, new regulation to ask the government that is imposing it for advice on how to comply. Frankly, the IRS and the SEC provide such guidance all the time. The IRS even has a hotline.

Nonetheless, there is a bill pending that would address the AG's concerns and take substantial responsibilities off of his office. Senate Bill 561, currently in committee, would change the language of Section 1798.155(a) to: "The Attorney General may publish materials that provide businesses and others with general guidance on how to comply with the provisions of this title." This is more consistent with how the European Union's GDPR operates.

The proposed text differs greatly from the current language and presents a range of issues of its own, including whether those published materials will have the force of law. The term "general guidance," at least, would belie such authority, as the California Legislature knows how to confer rulemaking authority and this is not it. But that may not stop courts from deferring, explicitly or otherwise, to those published materials in interpreting the CCPA. This would be particularly a problem for businesses if the AG's "general guidance" increases the compliance burdens that the CCPA otherwise imposes or makes specific a means or method of compliance that the CCPA left open.

Are Banks and Other Lenders Subject to the CCPA?

August 29, 2019



John E. Clabby

Michael L. Yaeger

California's new privacy statute imposes a number of new requirements on businesses that touch the personal information of California consumers. Its reach includes banks and financial services companies.

But the California Consumer Privacy Act of 2018 (CCPA) recognizes what financial institutions know all too well — those institutions are already regulated at the federal level. In recognition of this, the CCPA exempts certain types of personal financial information that is subject to federal regulation. However, because the exemption is designed for types of data, not types of companies, financial institutions are not fully exempt from the law and should attend to its details.

The key federal law is the Gramm-Leach-Bliley Act (GLBA) and its implementing regulations, which impose substantial requirements on financial institutions to protect customer data. 15 U.S.C. § 6801–6809; 16 C.F.R. § 314.1–5. In general, "financial institutions" are companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance. 15 U.S.C. § 6801(a), 6809(3); 12 U.S.C. § 1843(k). This definition covers most banks, securities brokers, and insurance companies.

The GLBA requires these companies to assess and implement controls for risks to customer information, with a focus on areas that are particularly important to information security, including: (1) employee training and management; (2) information systems (including network and software design and information processing and storage); and (3) detecting, preventing, and responding to attacks and system failures. 16 C.F.R. § 314.4(b). These are meaningful obligations; noncompliance can lead to enforcement action by the SEC, the FTC, or state regulators, and companies and consumers alike have litigated its provisions for years.

Into this regime comes the CCPA, which becomes effective January 1, 2020, and upends in many ways the default state data breach notification and privacy protection laws, in ways that we have discussed in several other places. Critically for financial institutions, the CCPA exempts "personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act, and implementing regulations. …" Cal. Civ. Code § 1798.145(e).

The key question is the extent of the exemption. The exemption does not do much for financial institutions as a category, as it would had it exempted all "financial institutions" under the GLBA. Instead, it exempts the information that the GLBA covers. In effect, the CCPA declares that it begins where the GLBA ends.

The trouble is that the CCPA covers a wider range of information than does the GLBA, and financial institutions are likely to possess such data. The CCPA covers "personal information" through an open-ended, default definition that focuses not on how the information was gathered but on its ability to identify its subject: "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." Cal. Civ. Code § 1798.140(o)(1).

By contrast, the GLBA, when coupled with its implementing regulations, applies to the narrower category of "personally identifiable financial information." That term is defined as "any information":

> (i) A consumer provides to you to obtain a financial product or service from you;
>
> (ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or
>
> (iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

12 C.F.R. § 1016.3(q)(1). Examples include information on a loan application, account balance information, and information from an internet "cookie." *Id.* § 1016.3(q)(2)(i).

Accordingly, because it is covered by the GLBA, the CCPA likely exempts transaction or account information, as well as information collected to provide a customer with financial products or services. Such information can include IP addresses when they are obtained in connection with the provision of a financial product or service. The CCPA likely does not exempt personal information, including an IP address that is collected from marketing activities or a financial institution's website, when the collection is not connected to the actual provision of a product or service. Likewise, because the GLBA does not apply to information shared with an institution's affiliate when that affiliate is not providing a joint product or service with the institution, the CCPA is unlikely to exempt such data.

It will be a complex task to sort through, in any given set of facts, what information is gathered in a way that means it is covered by the GLBA versus what information a financial institution holds that otherwise would be subject to the default CCPA definition.

The upshot is that financial institutions should review their data inventories and reassess their privacy practices to account for this interaction between the GLBA and the CCPA. Depending on how and why a data element is collected, the same element, such as an IP address, could receive different treatment in different instances. If it had been collected in connection with the provision of a financial service it would likely be exempt from the CCPA, but if it had been collected through general marketing efforts that never led to the provision of any service it would likely be covered by the CCPA. Financial institutions will have to get in the weeds and make fine distinctions.

Applying the CCPA to Health Care: The HIPAA Exemption, Exercise Apps, and Marketing Data

September 20, 2019

Michael L. Yaeger

Joshua L. Gutter

Despite its breadth, California's new privacy law, the California Consumer Privacy Act (CCPA), creates an exemption designed around the federal Health Insurance Portability and Accountability Act (HIPAA). That exemption is codified at section 1798.145(c)(1) of the California Civil Code. An organization that is otherwise subject to the CCPA—such as a for-profit entity "operating" in California that collects personal information and has either the information of 50,000 consumers or else annual gross revenues in excess of $25 million—may therefore find shelter under HIPAA. The problem is in determining the actual scope of the CCPA's HIPAA exemption and applying it. Here we provide some guidance for doing so.

The first part of the HIPAA exemption is relatively clear. Subsection (c)(1)(A) exempts a certain kind of information: "protected health information" (PHI) collected by a "covered entity" or "business associate" as those terms are defined in HIPAA. HIPAA, in turn, defines PHI as information relating to the physical or mental health or condition of an individual, or the provision of or payment for health care to an individual, for which there is a reasonable basis to believe it can be used to identify the individual.[1]

Accordingly, an organization's status under HIPAA, and the purpose for which the organization collects data, will affect whether the data will qualify for the CCPA's HIPAA exemption. Assume that an athletic sportswear company that sells product in California has developed a pedometer app that consumers can download to their phone via the Apple App Store or Google Play. The app tracks the number of steps a person takes each day and captures additional information, including the user's name, weight, birthday, calories burned, geolocation, and average pace. That company is probably not a covered entity or business associate under HIPAA and would not be able to avail itself of the CCPA's HIPAA exemption.

But consider a health care system "operating" in California that created an app with the exact same functions, yet made the app available only to its patients in order to monitor their health and treat medical conditions. That organization is a covered entity under HIPAA, the data is probably PHI, and the HIPAA exemption probably applies.

On the other hand, it is less clear if the HIPAA exemption covers a health care provider's marketing data, data from mobile apps, or customer service or call center data that is not also PHI. Such data could include internet "cookies," IP addresses collected from an organization's website, mobile device IDs, recorded phone calls, and email addresses. While the actual text of subsection (c)(1)(B) would seem to cover such information, health care organizations should nevertheless proceed with caution because a regulator may reject that reading in favor of one that creates more protection of consumers.

On its face, the text of section 1798.145(c)(1)(B) appears to exempt not only certain kinds of *information* regulated by HIPAA, but also a certain kind of *organization*, namely, a "covered entity" who maintains patient information in a certain way: "This title shall not apply to any of the following: ... (B) ... a covered entity governed by [HIPAA] ... to the extent the ... covered entity maintains patient information in the same manner as ... [PHI]." In other words, the CCPA exempts an organization that "maintains patient information in the same manner" as PHI under HIPAA. The consequence of this reading is that a health care provider might be exempt as a whole; all of its *non*-health care information might qualify for the CCPA's HIPAA exemption so long as the health care provider protects "patient information" in the right way.

But this reading of the CCPA's HIPAA exemption might not be received well by a judge or assistant state attorney general reviewing a data incident after it has occurred. Hindsight might tempt

an unsympathetic reader into limiting the exemption in subsection (B) to "patient information." Perhaps a judge would invoke the purpose of the statute, or the findings and declarations at the beginning of the bill. And while the broader category of "patient information" might include information that is not PHI, there is a lot it would not include. For example, IP addresses, cookies, or marketing data regarding people who have not become patients. In that case, such data would not fall under the HIPAA exemption and would instead be regulated by the CCPA.

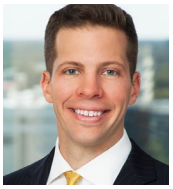
The most prudent course may be to assume that the HIPAA exemption will cover only the PHI and patient information of HIPAA-regulated organizations, and to design privacy policies and practices accordingly. Then, if an incident occurs that leads to discussions with regulators or litigation, a health care organization might seek additional shelter under the broader exemption suggested by the actual text. In any event, organizations in the health care sector should review their data inventories carefully and reassess their privacy practices to account for the interaction between HIPAA and the CCPA.

[1] *Exempt, too, are aggregate consumer information or de-identified information, 'medical information" already covered by California's Confidentiality of Medical Information Act, and certain information collected as part of clinical trials. See Cal. Civ. Code § 1798.145(c)(1)(A), (C). (Note, however, that the definitions of deidentified information in the CCPA and HIPAA are not the same.)*

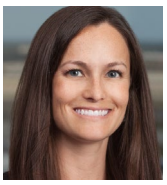
CF on Cyber: Cybersecurity Due Diligence in M&A Deals Under the CCPA and GDPR

February 20, 2019

John E. Clabby



Joseph W. Swanson



Jacqueline Pace Swigler

Sophisticated due diligence in corporate mergers and acquisitions has long included an assessment of the cybersecurity posture and privacy protocols of the target company. But the new California Consumer Privacy Act (CCPA) and the European Union's General Data Privacy Regulation (GDPR) have raised the stakes for compliance, particularly for target companies that process or collect personal information or otherwise earn a living from consumer data. In this podcast, cybersecurity attorneys Jack Clabby and Joe Swanson and M&A attorney Jackie Swigler offer their top five inquiries for cyber due diligence in this enhanced landscape. The discussion is of use both to those looking to invest in or acquire companies subject to the CCPA or the GDPR and to such companies or owners who are preparing for a sale or strategic partner. After a helpful overview of the applicable regulations and their impact generally, the podcast turns to a discussion of their top five tips.

Transcript:

Jack: Welcome to CF on Cyber. We have a topic today that came out of conversations with some of our clients and friends about what impact the new California privacy statute is going to have on investments that private equity and other entities might be making in businesses that process or collect consumer data, and we thought through some of our talking points for that and said, you know what, this would be a good podcast. We have Jackie Swigler here, who is an M&A and corporate transactions attorney in our Tampa office. She works with companies that are both up for sale and companies that are making investments or purchases so Jackie, thank you for joining us on the podcast today. And as always, we've got Joe Swanson who's the head of our national cybersecurity and data privacy practice and me, Jack Clabby, a shareholder here in the Tampa office of Carlton Fields. So let's get into it. Joe, we've been on a couple of these phone calls where our friends or our clients are asking us about not just compliance with the new California data protection statute but if they're looking at making an investment or acquiring a company that processes data, how it affects them. What's happening here in this cyber due diligence space?

Joe: Thanks, Jack. So the cyber due diligence space has really picked up and it's due in part, I think, to some mega breaches that have hit the news over the last couple of years and what that has meant for a couple of M&A deals – most notably, the Yahoo and Verizon merger that had a significant data breach occur in the midst of it and it resulted in a significant decrease in the price. And then more recently, the Marriott data breach, which as it turns out spanned the period of time during which they were conducting due diligence for the Starwood acquisition. So that's why there's a lot of attention in this space and it's not just on M&A deals. We have been called quite frequently in recent months to assist our partners, for example, in negotiating reps and warranties for a commercial lease or other types of transactional documents that the parties to those deals now want assurances that their cyber house is in order.

Jack: Alright, so one of the lawyers who calls us from time to time to help out is here. Jackie, can you tell us a little bit about, let's put aside the GDPR and the special problems from the California Consumer Privacy Act, what is usual in cyber due diligence?

Jackie: Right. So in cyber due diligence you would want to know what laws and regulations are applicable to the company that you're investigating. If you're buying a company then it would be the target company or if you are putting your company up for sale, ideally you are looking into these kinds of questions before you go through the process of putting up your company for sale. So you would want to know the laws and regulations that are applicable and how the company is doing in terms of complying with those laws and regulations. And in order to do that, you would want to look at, for example, policies that are in place whether they are privacy policies, terms of use for online operations or policies just internally for

employees to be operating under. A lot of companies have vendor contracts that they outsource to third parties to help them with the compliance. So you would want to know what vendor contracts they have and if they're complying with their vendor contracts and how they're using third parties to help them with their compliance. You would want to know if there have been any incidents related to cyber and data security and data protection, large incidents but also small incidents where they're having troubles with people complying with their policies. Insurance coverage is an important part of this as well, whether the company has proper insurance coverage to cover for any sort of these breaches.

Jack: Joe, could you talk to us about why the GDPR and the CCPA have changed this a bit.

Joe: Sure. Jackie talked about looking at applicable laws and regulations, and increasingly for businesses that is the GDPR and will be the CCPA. The GDPR took effect in May of last year; the CCPA was passed last year and will take effect in January of this coming year. And each of them imposes significant obligations on organizations around the world. They have extra-territorial reach and for that reason a number of our clients are interested in how they apply and what their impact might be on these types of deals.

Jack: Alright. So these privacy issues that are raised by the GDPR and the California Consumer Privacy Act, the CCPA, am I getting that right?

Joe: You are.

Jack: Alright. They're particularly acute when the company that's being put up for sale or contemplating a merger or investment is a business that earns its revenue from the collection and the processing of personal data, right? So the average retail company has its own risks from consumer lawsuits, for example, but a company whose business is buying, selling, processing or earns revenue from the buying, selling or processing of that data, has special considerations and could essentially be wiped out if the wrong calls are made under compliance with these statutes. We have top five hits that we want to talk about today. So let's get through these top five suggested inquiries from parties to transactions or M&A deals that might involve these kinds of companies. Joe, could you walk us through the first of these inquiries.

Joe: Sure, the first inquiry would be just basically where does the data come from? And by that I mean, how much of a target company's business model relies on data that is collected from public sources versus data that is purchased from other data aggregators versus data that's collected from the consumers directly.

Jackie: And where the data comes from matters. That's one of the key establishing questions in your due diligence investigation. As a deal lawyer on either side of the transaction, knowing the answer to these questions helps me locate the right vendor contracts that I mentioned earlier, to see how the rest has shifted. It also helps me understand what specialized cyber advice I might need and to advise my client whether it should invest in that specialized cyber advice.

Jack: Right, and that's because the GDPR and the CCPA do a lot more than state data breach notification.

Joe: They do. They govern how organizations collect, store and use data and what those organizations promise and disclose to the individuals. These would be their use of data and their rights and that's what has made it such a paradigm shift.

Jack: So that's why you want to start these specialized inquiries with where is this data coming from? It might be treated differently, or the incident might be treated differently under the regulations depending on what originates that data. And it also flows through to the questions that are followed. The second inquiry is how is that data used for each individual? And critical here is this idea of profiles. Does the company set up profiles for individual people to track that person across time, across their spending habits or across other behavior, and then does the company segregate the data within that individual profile by where it came from? The answers to these questions, I think, can help the potential investor in the target company know, again, where the cascading risk arises.

Joe: Profiles are really a double-edged sword on the one hand. You know, the downside of them is that if a company keeps profiles, that may trigger a number of reporting and compliance obligations if GDPR and CCPA come into play. On the other hand, the good news is that if the company is keeping profiles it's more likely to be able to comply with a customer request to surrender, delete or transfer data, all of which at a high level are the rights that are conferred by the

GDPR, the CCPA and surely in what will be other statutes like them and active in the coming months. So the bottom line is, if all of this information is one place and the company has a good handle on that, they have a higher regulatory risk profile but their ability to comply is going to be that much greater.

Jack: And there's a big difference between companies that track consumer data in individual files in individual folders essentially for those consumers, and those that simply are aggregators that separate that consumer data from identifying whose it is. So our first inquiry then is *where* does the data come from, our second is *how* is the data used for each individual and our third inquiry is, *what* is in the privacy policies that the target entity has in place? And are the things that the entity says it's doing in the privacy policy in fact being done? Alright, so if a company is collecting data from the individuals directly, what does it tell those individuals and how does it inform them of what it's collecting, why it's collecting it and what their rights are with respect to that data? And can the potential investor, maybe the private equity firm or the larger company, can they get copies of those privacy policies? Are they readily available? And critical to this is getting the privacy policies that actually exist at the point of collection.

Jackie: Like any due diligence, the target company's willingness to share the information tells us as much, if not more, than the actual information itself. Willingness or ability. This is why when we're helping companies sell themselves, ideally we would spend a little bit of time helping them clean up their contracts in their books and records. We'll often suggest changes to the privacy policies and their procedures if data collection and processing is integral to the company value.

Joe: And I would add one other thing to this discussion and that is if collection of the data is done through a proxy-vendor or some third party, it's important to consider what review does the target company do for those point of collection disclosures and does the vendor, the third party, comply with those disclosures strictly, because liability here for the target company is not just what it promises to do about its consumers or its employees and information it collects about those individuals but also what these third parties are promising on their behalf with regard to collection, storage and processing of data that could ultimately cause problems for the target company.

Jack: A lot of the work that companies are doing now in the run-up to the California statute is cleaning up their privacy policies for exactly this purpose. And Jackie, you were saying, if a company is getting ready for a sale, it's a pretty easy thing for a company to do to rewrite the policy – the hard part is determining whether the company is actually doing the things it's promising in the policy.

Jackie: Yes.

Jack: And inquiry four is based around the new requirements of the statute we see in California that may be adopted in other states. Inquiry four is, can an individual actually see his or her data and can they delete it? So if a particular individual has requested to the company, "I want to see all my personal data that you have on me and if I don't like what you have, I want you to destroy it," can the company comply with this? And if so, how quickly and how completely can they comply? This at the heart of the GDPR's right to be forgotten which we've talked about on other podcasts, and also part of what's essential to the CCPA's structure, right? Can the company destroy all data on an individual on demand and if not, why not? That's the question that I would want to know if I was planning on making an investment. And if they can't do it, that's not fatal while we're in this run-up period, but how soon can the company get its compliance structures in place and what resources would it need from me and my investment firm in order to get there?

Jackie: Right, and that will certainly be one of the stumbling blocks to compliance with the GDPR and the CCPA – how can the target company comply with a consumer's request to see, delete and transfer all of the data on that individual.

Joe: So that brings us to the fifth of the inquiries that we wanted to cover today and that is, what is in the vendor contracts and are they being followed? Will the target company allow you to review all contracts or just a few example contracts that it has in place with its third parties from which it receives personal data, for which it holds personal data, or to which the company transfers personal data either for processing or storage?

Jack: And Joe, that's particularly true about those profiles that we were talking about a moment ago, right?

Joe: Yes.

Jack: Is the target company selling its profiles? It's making these profiles but does it actually profit from the fact that the data is segregated by individuals? If that's the case, then all sorts of risk arises and the due diligence needs to dig in a little bit more.

Joe: That's right.

Jackie: Right. And what we really want to know when we see these contracts is how they spread the risk of data security and compliance. What are the companies promising to each other as far as legal compliance is concerned? Separately, if the target company has made a number of commitments in these contracts, is it actually following them? Does it have the ability to track what its employees are doing? And are the employees following the commitments that are being made?

Joe: The bottom line here within this inquiry is that it's important to know how many vendors there are, where they are located, and do they do business in Europe or in particular United States jurisdictions such as California that would pose a heightened risk because of the CCPA. Frankly, California is probably not going to be the only statute, or the only state with a law like it, and so any target company should have its house in order so to speak with a view to these issues.

Jack: Alright, so in sum, there are these five inquiries that we use in connection with M&A due diligence as to cybersecurity and privacy that takes into account the GDPR and the new California statute. First, where does the personal data come from? Second, how is that personal data used by the company to support revenue, that is, how does the money get made by the use of this personal data? Third, what are the privacy policies and is the company following them? Fourth, can an individual see the data that the company has on her and successfully request its deletion? And fifth, and finally, what is in these vendor contracts and are they being followed by the target company and its vendors?

Jackie: And remember, it's a cliché, but a hard compliance environment is an opportunity for competitive advantage. For a company that's preparing for sale and particularly one that believes it has significant growth ahead, compliance with these emerging privacy standards will be immediately apparent and it will stand out in the sale process.

Joe: Thanks for joining us and special thanks to Jack and Jackie. Thanks to everyone for listening and we hope you'll join us again soon.

This is a transript of a CF on Cyber podcast. Listen to the podcast at https://youtu.be/NUBLio44qpo or on iTunes, Google, and Spotify.

The Research Exception to the CCPA's Right to Deletion — Will It Ever Apply?

July 17, 2019

Gregory A. Gidus

Following in the footsteps of the GDPR, the California Consumer Privacy Act of 2018 (CCPA) grants California consumers the so-called right to deletion when it goes into effect January 1, 2020. Section 1798.105(a) provides that "[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."

This right to deletion, however, is not without its limitations. *See* § 1798.105(d)(1)–(9). One such limitation is the exception for "scientific, historical, or statistical research," which provides:

> (d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:
>
> * * *
>
> (6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

§ 1798.105(d)(6).

While seemingly useful at first glance, this exception will likely prove difficult for most businesses to use in practice. First, the research to which the exception applies must be "public," "peer-reviewed," and in the "public interest." In addition, the definition of "research" in section 1798.140(s)(8) provides that the "research" shall "[n]ot be used for any commercial purpose." It is hard to imagine what type of "public interest" research would be conducted by a business that does not advance the business's commercial or economic interests. *See* § 1798.140(f).

Adding to the puzzle is the research exception's requirement that it applies only when "the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research." The section 1798.140(s) definition of "research" already requires all personal information used in "research" to be "pseudonymized and deidentified, or deidentified and in the aggregate." § 1798.140(s)(2). Given this requirement, it appears that it will be quite difficult for any business to show that the deletion of a particular consumer's personal information will "seriously impair" the research.

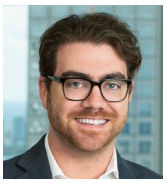
The research exception also applies only "if the consumer has provided informed consent." As drafted, it is not clear whether this means that the consumer must have given initial informed consent for the business to use his or her personal information in the study or whether the consumer must consent to the business or service provider continuing to use his or her personal information after the business determines that the data is necessary to continue its research. In practice, either interpretation is likely to substantially limit the operation of the research exception.

In the end, the research exception is seemingly too narrow to actually apply in the real world. But not all is lost for businesses that use personal information in their research. Section 1798.105(d) contains other, broader exceptions to the right to deletion, including exceptions for information necessary to provide a good or service reasonably anticipated by the consumer, for information used internally that aligns with the expectations of the consumer based on the consumer's relationship with the business, and for information used internally that is compatible with the context of the consumer's relationship with the business. §§ 1798.105(d)(1), (7), (9). A savvy business or service provider could attempt to use these broader exceptions to retain personal information used for commercial research when faced with a deletion request, even if the research exception does not apply.

Regulating Privacy on the Blockchain Starts With Understanding the Meaning of "Personal Data"

August 6, 2019

Steven Blickensderfer



Justin S. Wales

A commonality among recent data privacy regulations (including the EU's GDPR, California's CCPA, and Brazil's LGPD) is that only the storage and transmittal of "personal data" is regulated. These new regulatory frameworks generally define "personal data" (or "personal information") obliquely as elements that relate, by themselves or taken together with other data, to an identified or identifiable individual. As companies across the world explore transitioning data storage onto encrypted, open databases including blockchains or similar technologies, an emerging question has arisen over whether such uses could violate privacy regulations and, counterintuitively, force companies into adopting less secure data storage methods than available through new technologies.

Part of the challenge of applying new technologies to existing regulatory frameworks is definitional. Privacy regulations purposefully employ broad definitions of "personal data" that make it difficult to apply to all types of data. Excluded from most regulations are business-to-business data (B2B), data used solely for household purposes, and "anonymous data," meaning data that has had personal identifiers removed or rendered indecipherable. The exact bounds of these categories remain unclear, and it is not often easy to categorize data as fitting into one category to the exclusion of other, regulated data types.

Privacy regulations are generally technology agnostic and apply to all methods of storage and transmittal, including blockchains. One of the challenges of applying privacy regulations to blockchains is that not all blockchains are equal or employ the same level of security or encryption. Some have open, decentralized, and pseudonymous characteristics, and therefore may or may not be compatible with regulatory frameworks.

Generally, regulators have treated blockchain technologies like cloud computing and view it as just an additional means of collecting and processing data. Accordingly, if data on a particular blockchain cannot be used to identify an individual, then it is generally spared from data privacy regulation altogether. The same is true for data contained on a public, permissioned, or private blockchain.

A good starting point for analyzing the application of any given data privacy regulation to the blockchain (or any new technology) is to ask whether the data can be considered personal data. In some cases, the answer is obvious, like data that identifies the owner of a property. In others, the answer is less clear. One of the most common data elements related to public, proof-of-work blockchains like Bitcoin is the pseudonymous identity of the miners who help to maintain the blockchain. In most cases, this information will consist of alphanumeric characters that are not on their face personally identifiable. This database architecture can be used to maintain a high level of confidentiality; however, if an entity has access to one's private key or can link the information to an individual's identity, then the data may be considered personal data and the entire blockchain may, as impractical and unenforceable as it may be, be subject to regulation.

Such considerations are highly dependent on the architecture and unique characteristics of the blockchain, which is essential to keep in mind when implementing products or services that use distributed and encrypted technologies like blockchains. Indeed, some regulations like the GDPR require entities to build privacy into the design of their products and consider data collection practices and techniques at the outset before venturing into new technologies. Some also require an assessment of the risks associated with the exposure of personal data, which makes sense to do in any event from a business standpoint.

Privacy-by-design principles further dictate that entities employ data minimization techniques to keep as much personal data off the blockchain as possible. This can include the use of commitments, hash keys, ciphertexts, or other sophisticated technologies like zero-knowledge proofs to make the data on the blockchain practically inaccessible. Guidelines from one of Europe's leading data protection authorities in charge of enforcing the GDPR recognize the use of these crypto techniques as the functional equivalent of deleting personal data from the blockchain. As blockchain technology evolves, it is reasonable to assume that data minimization techniques will as well, and additional methods of "deleting" data from the blockchain will surface.

Therefore, to properly assess whether and to what extent data privacy regulation applies to any particular blockchain first requires an answer to this question: Is the data "personal data"? If it can be considered personal data, and this ultimately may vary across regulators and courts, then a given data privacy regulation could apply and all of its requirements should be considered. But if not, then considerable effort could be saved because it is more likely than not that data privacy regulations do not apply to that particular data. Those seeking to implement blockchain technologies in their business would be wise to keep this in mind when considering whether, and to what extent, to use blockchain technology.

Fortnite Suit Highlights Game Cos.' Need For Privacy Vigilance

August 27, 2019

Joseph W. Swanson

Steven Blickensderfer

Nicholas A. Brown

There is no denying the explosive growth and popularity that esports and competitive online gaming have experienced recently. Industry events are grabbing headlines like never before, such as the Fortnite World Cup, where a previously unknown 16-year-old competitor recently won the top prize of $3 million. With the heightened interest and attention, however, comes increased risk of data breaches and similar incidents, along with scrutiny from litigants and regulators alike.

Indeed, game companies are just as susceptible to lawsuits and regulation related to data privacy and cybersecurity as companies in any other industry - if not more so, given the sensitive data they increasingly collect and use.

A recent data privacy class action filed in federal court in North Carolina against Epic Games, the company behind the game Fortnite, serves as a stern warning that game companies must be vigilant when it comes to the collection, use and protection of their users' data. Such vigilance includes ensuring that their privacy programs and incident response guides remain up to date and reflect the unique challenges of this growing industry.

Modern Video Games Collect Troves of Personal Data

Gone are the days of Atari and the original Nintendo Entertainment System, which had no internet connection and did not collect data in any meaningful way. Virtually all modern video games require personal information in order to function. Often, personal information is required just to set up a user account and verify the age of minors in order to purchase and use games.

And the games themselves can - and often do - capture every single action, decision and communication players make, whether players know it or not. This data is used to analyze how players access certain in-game content, which helps game companies determine how and whether to develop the game going forward.

With the advent of new technologies, game data increasingly includes a player's physical characteristics (including facial features, body movements and voice data), surroundings, biometrics and information gleaned from social networks. Indeed, in order for some games to function at all, such as Niantic Inc.'s Pokémon Go and Harry Potter: Wizards Unite, geolocation data is essential. Other games, particularly those that include consequential in-game selections and choices, collect information that may reveal intimate details about the player that bear on key personality traits, such as temperament, fears and even leadership skills.

For the most part, this game data is used responsibly to improve the game experience and enable functionality that players demand. In some instances, however, the data is being used for less altruistic purposes, like figuring out how to maximize monetization, including through use of various forms of microtransactions such as loot boxes, which have received increased regulatory scrutiny of late. Other nefarious examples exist, such as the revelation that the National Security Agency used the mobile game Angry Birds to collect phone numbers, emails and device codes for purposes of mass surveillance.

Regardless of the use, the mere collection and storage of this personal data exposes game companies to newfound liability, including the risk of cyberattacks. And that risk naturally increases the more data the game collects and the longer the data is stored.

Cyberattacks Targeting Game Companies and Associated Legal Exposure

Cyberattacks take many forms and threaten organizations differently depending on the context of the particular industry target. Particularly damaging to the game industry are viruses and malicious code that can cripple systems, distributed denial-of-service attacks that take entire services offline and data breaches that result in the exposure of unencrypted data to unauthorized third parties.

The recent Fortnite lawsuit stems from phishing, which is another form of attack that preys on companies across industries, but that is particularly pernicious when involving game companies. Phishing is a form of social engineering whereby the hacker uses low-tech or nontechnical approaches to cause an individual to compromise security procedures and disclose sensitive information, most commonly through email. To fall victim to this kind of attack requires the user to click on a specially crafted phishing link or attachment designed to look like it came from a legitimate source.

In this instance, that source was Epic Games. To entice users to click on a suspicious link, hackers commonly use the promise of free game credits or steep discounts on in-game currency or items. Once the link is clicked, the hacker is able to steal the user's access token to the game through a malicious redirect and perform an account takeover. Once inside the account, the hacker is able to control the account and then, where the account is linked to a credit or debit card, make in-game purchases and pose as the player to others online.

Although the phishing vulnerability in this case was patched in December 2018, a class composed of the game's users filed a class action against the company. The lawsuit alleges that the class suffered losses in the form of stolen credit or debit card information linked to their accounts. It also alleges that the hackers used the linked credit or debit cards to purchase in-game currency to boost the stats of the stolen accounts, some of which were sold on the black market. The lawsuit ultimately demands $100 million and, regardless of how it turns out, Epic will incur significant attorney fees and other costs.

The Unique Challenges of a Changing Regulatory Landscape

While the result of this lawsuit is to be determined, the passage of data privacy regulations such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act of 2018 are already making an impact and require even greater diligence on the part of game companies with respect to the data they collect, use and store.

For instance, these new regulatory frameworks are trending toward expanding the definition of "personal data" (or "personal information") beyond mere "personally identifiable information" defined in U.S. state data breach notice laws. Now, "personal data" includes any data elements that relate, either by themselves or along with other data, to an identified or identifiable individual or household. This can have massive implications for a game company that has accumulated, and still retains, vast amounts of personal data on its players—data that was once unregulated.

Moreover, the GDPR and the CCPA impose upon companies various standards of data minimization and transparency previously unseen in the game industry. Under these laws and others being proposed, most game companies must provide users with access to the personal data that is collected and used, and in many instances users must also be afforded the right to opt out of automated processing and profiling. This demands that game companies reassess their data processing practices to determine the extent to which they are engaged in such conduct.

The CCPA, in particular, affords California consumers a new right to object to the "sale" of their personal data to third parties, and the word "sale" is broadly defined to mean the transfer of information for any value, even nonmonetary value.[1]

In addition, these new data privacy laws are expected to lead to an increase in data breach class actions. The CCPA, in particular, gives plaintiffs the ability to sue in a class for breaches in certain circumstances. And because the law permits statutory damages ranging from $100 to $750 per incident per consumer, the plaintiffs may not need to prove actual damages. Consequently, it is not surprising that 66% of companies are concerned about their future class action exposure as a result of the CCPA.[2]

Recommendations

Businesses and other organizations need to institute meaningful cybersecurity and privacy compliance programs that minimize risk. For game companies, these steps include the following:

- Ensure that the business has in place an incident response guide that is tailored to that company and its industry. This may include provisions for a response in the event the cybersecurity attack compromises online accounts, such as a plan and procedure for dealing with suspicious or fraudulent charges related to user accounts that may have been breached. A comprehensive incident response guide will help the organization detect and respond to a potential incident before it becomes a breach, as defined in the law. And if there is litigation, the presence of an incident response guide will be among the features that can be used to demonstrate the organization's "reasonable security procedures and practices."

- Update all data privacy and information security policies, procedures and programs. Be mindful that statements included in a privacy policy will be scrutinized and, in some cases, used against the company. For instance, the Fortnite lawsuit quotes from Epic Games' online privacy notice and alleges that users relied on the statements concerning how personal information is protected to their detriment. That is why it is often recommended to include disclaimers and avoid superfluous language and promises, particularly those concerning the security of the personal information. In short, only make promises that the company can keep, and then aggressively live up to them.

- Understand what personal data is being collected and how it is being used through data mapping. Data mapping is essentially a process of recording the life cycle of personal data as it is collected, used, stored and shared by the business. This process is essential for an organization to be able to act on a consumer's request related to his or her personal information under laws like the GDPR and the CCPA, and it can be a challenge for game companies that collect a lot of personal data. This is not just a one-time event. A business that has previously engaged in data mapping for the GDPR should leverage that work for new laws, like the CCPA. Given the breadth of the definitions of "personal information" and "selling" under the CCPA, a business engaged in data mapping for the CCPA should consider whether to supplement previous data mapping that may not have incorporated these concepts. And some organizations may find themselves data mapping for the first time.

- Be mindful of data collected and used belonging to minors. Most game companies are already familiar with laws that regulate the collection and use of minors' data, such as the Children's Online Privacy Protection Act, and have policies and procedures in place for complying with them. But with the passage of the CCPA, game companies must once again revisit their policies, in particular for purposes of obtaining the requisite consent for collecting and using such data. The relevant age for purposes of triggering the CCPA's new obligations is 15 and under, whereas the relevant age under COPPA is 12 and under.

Conclusion

This is an exciting time for the esports and electronic gaming industry. But the industry's newfound attention and success brings with it a variety of unique, and unresolved, challenges. Those challenges include significant risks stemming from data collection and the security of that data. The industry players who stand the test of time will be those who are able to develop and maintain games while striving to protect the privacy of their users and the security of those users' data.

[1] Cal. Civ. Code § 1798.140(t)(1).

[2] 2019 Carlton Fields Class Action Survey, available at https://classactionsurvey.com/.

Reprinted with permission of Law360. View original publication here.

Even the Games Have Eyes: Data Privacy and Gaming

March 13, 2019

Attorneys Steve Blickensderfer and Nick Brown take a deep dive into the emerging legal issues surrounding data privacy in gaming. They discuss the history of data collection in games and how that data has been used, and explore some of the regulatory restraints and challenges facing industry players. Then, in the 1v1 Showdown they debate various approaches to regulating these sensitive issues.

Transcript:

Nick: Welcome to the LAN Party Lawyers Podcast, where we tackle issues at the intersection of video gaming, law and business. I'm Nick Brown and with me is my co-host and partner in crime, Steve Blickensderfer.

Steve: Hey there, Nick.

Nick: Before we get going, we just want to remind everyone that nothing we say here is legal advice. What are we going to talk about today, Steve?

Steve: A topic very near and dear to my heart and that is data privacy regulations in video games and video game development. So to give you a roadmap of where we're going, first we're going to talk about the various data privacy regulations impacting companies in the gaming space—things like the new European data protection law the GDPR, California's new data protection law the CCPA and others. Then we're going to explain why the increase in data privacy regulations is becoming an increasingly big deal for video games in the esports industry. Then we're going to do a 1v1 Showdown where Nick and I will debate various approaches to how data privacy regulations could be implemented whether on a federal level, state level, a mix of both, or not at all, and then we're going to share some takeaways and wrap up.

Nick: Alright, so we've got a lot to cover today. To start, what is the difference from a high level between data privacy and cybersecurity? Because I always see those two things thrown around together.

Steve: Okay, so take cybersecurity, think of bad actors doing sneaky things to get your data.

Nick: Okay.

Steve: Contrast that with data privacy, and that refers to the laws and regulations that cover around the collection and processing of data.

Nick: Okay. Now today we're going to talk about the latter, which is data privacy—but we have another LAN Party Lawyers episode dedicated just to cybersecurity.

Steve: That's right.

Nick: Well before we get going, let's get some context. Here, it all started, believe it or not, with Space Invaders. In the old world of video games, when you go to an arcade, developers didn't have any real ways to interact with players after the game was released. They couldn't get any info, they couldn't interact, they couldn't see anything about the metrics of what their players were doing; they would just shoot the game out into the world and that was it. Space Invaders came along and it was actually the first game to store your high score, which doesn't sound like a big deal now, but when that came out it was revolutionary. And it also allowed users to enter their initials to announce their high score to the world, so that was the first data collection in gaming. So fast forward, then the internet came along and then people started having LAN parties where they would get all their computers in the same house and create a local area network, that was how if you wanted to play Doom or Wolfenstein with your friends for example.

Steve: Mechwarrior.

Nick: Or Mechwarrior, that's how you would do it, and then later on we got the high speed internet that we're all used to now that brought along a real online revolution in games. So now the games industry is increasingly data driven, and there's a constant two-way dialogue between developers and their players. Games nowadays

Steven Blickensderfer

Nicholas A. Brown

can—and many do—capture and log all sorts of information about the players' interactivity. So every single action taken, every decision made, every communication players make, can be logged and saved by the developers whether the players know it or not. Now sometimes this data is used for everyone's benefit in a benign way, for example, developers can analyze how many players access certain content or use certain features and that helps them determine how and whether to develop going forward and how to spend their resources. So one good example of this is that Bioware, the makers of the Mass Effect series, they had access to see which conversations in the game their players were skipping over. And that allowed them to figure out what characters in the game people wanted to listen to and then they were able in future installments of the game and in DLC to divert resources appropriately. If nobody's listening to this character, then we probably shouldn't pay a bunch of money to get a bunch of unique voice acted lines in the game, we should focus on other areas where players actually engage.

Steve: And for those people that don't play that game, this is a game where you select "A" if you want a certain type of reaction or you want to respond in a certain way and the voice that would come after that would be something different depending on what you chose.

Nick: Exactly, this type of data can also help reveal bugs or confusing user interfaces—if you have a game that's being played by millions of people and nobody's been able to turn in a certain quest or mission, then it may be revealing the fact that there's a bug with that and people aren't doing it only because they can't. And that type of data allows developers to figure out where they need to go to solve problems.

But at the same time, this data can be used for less altruistic purposes, for example, trying to figure out what makes it most likely that people will spend more money on your game, and they can figure out how to maximize monetization, they can figure out how to get more microtransactions in front of you that you might be likely to purchase. Or perhaps even worse, this data that's gathered itself can be sold to third parties with who knows what their motivations are. And so, of course, as a result there are a bunch of laws and regulations at play and that's what we're talking about today.

So Steve, tell us, are privacy laws in the U.S. organized in a certain way that affects gamers here?

Steve: Sure. So to compare the U.S. to other countries like in Europe or even maybe in Latin America, privacy laws in the United States are organized more by industry than anything else. So you have laws that regulate the healthcare space, that would be HIPAA and HITECH; then you have the banks and the financial sector and those would be governed by Gramm-Leach-Bliley Act and the Fair Credit Reporting Act; then you have the education space that's governed by FERPA. In addition to industries, you also have certain user groups that are protected and one that really sticks out are children, and the use of children's data is governed by the Children's Online Privacy Protection Act or COPPA. So that's a general overview of how the privacy laws are organized in the United States.

Nick: Alright well is there a law that specifically regulates the video game industry then?

Steve: No, there's no particular law that just governs the video game industry itself.

Nick: So what actually does end up regulating the video game industry if there's no law specifically designed for that?

Steve: Everyone engaged in trade and commerce is regulated by the Federal Trade Commission (the FTC) and the FTC Act. More specifically, Section 5 of the Act says that you can't engage in deceptive or unfair trade practices, and with respect to video games, you can say you can't engage in that kind of activity with respect to data. So everybody in that respect is governed by the FTC and Section 5 of the FTC Act. And aside from that, there really wasn't an overarching data protection law that applied here in the States across all businesses, much less worldwide, that is until...

Nick: Until recently.

Steve: ...2018.

Nick: Yeah.

Steve: 2018 some would say is the like event horizon for data protection and privacy regulation.

Nick: I'd say that.

Steve: It was huge, and there are many reasons for this. First and foremost is Europe's data protection law, the GDPR, went into effect in May of 2018. And this law has had a global reach, which the previous law that it replaced didn't—it affects all businesses and technologies that collect and process personal data which we will explain in a little bit. That's the GDPR.

Then we have California which passed the California Consumer Privacy Act which is similar but very different in many respects, one of them being where the GDPR took years to develop, the CCPA came together pretty quickly. One similarity is that they both have a global reach to protect processing of data of California residents.

And then to give another example of how big 2018 was, another large economy, Brazil, passed a data protection law in August of 2018 in Portuguese, I don't how to say it in Portuguese but the acronym is LGPD. So that's another huge law that happened in 2018.

And as we enter 2019, it looks like none of that inertia has stopped, it's just still going. Washington State recently has introduced legislation to regulate data processing called the Washington Privacy Act.

Nick: And if I'm not mistaken, Congress is considering federal legislation as well, right?

Steve: That's right and that's really the biggest news of 2019 so far is where are we going with Congress regulating it, how much are they going to regulate and we're going to get into that a little bit in our 1v1 Showdown. But suffice it to say Nick, there's an abundance of new laws regulating the collection and processing of data.

Nick: Sounds like it.

Steve: Including video game and mobile game data affecting businesses all over the world. Now, let's talk about what kind of data is being regulated, not just any data...

Nick: Okay.

Steve: ...personal data.

Nick: What does that mean?

Steve: Personally identifiable data or personal information. It depends really what act or regulation we're talking about, some statutes are in the middle of the road when it comes to the definition of personal data. Let's take the GDPR for example. In the GDPR, personal data includes data that can be used alone or in conjunction with other data to identify someone. So let's take your height and your weight separately, that doesn't say anything about you, but we add your name to that, boom, we've got something personal about you. Your name itself would be personal but this is showing the name, or the height and weight ...

Nick: Connecting all that together makes it more personal.

Steve: Exactly. And then we have the California statute which has a very broad definition of personal information and that includes any data that can be reasonably linked directly or indirectly to a person or household—and that's new, adding household to the definition. So we're talking about geolocation data, behaviors, attitudes, Nick, when you've got a bad attitude.

Nick: The California statute covers my bad attitude?

Steve: Yes, it does. Your olfactory information.

Nick: It's how I smell?

Steve: That's your sense of smell, so if you don't have one that would be pretty personal and California regulates that. But putting it back into context where we are talking about video games, importantly, personal data can include electronic data. Take cookies, for example...

Nick: Delicious.

Steve: ...cookies are delicious, but we're not talking about those cookies, we're talking about little log files placed on your computer by websites, for example, that help to improve your experience by recording your browser type, language, which kind of operating system you're using.

Nick: And that's covered by the California statute?

Steve: It's also covered by the GDPR.

Nick: Wow, okay.

Steve: To the extent it helps to identify you. Again, you have to put that into context and follow the definition under each statute. But the California statute goes even a step further, and it says your browsing history is personal information...

Nick: Really?

Steve: ...your search history, which I know your search history is pretty personal.

Nick: Incredibly.

Steve: Yeah, totally. And even a consumer's interaction with a website is considered personal information. So why is all of this important? Let me tell you, Nick. It's because these recent laws, in the context of gaming, modern games generate a tremendous amount of personal data.

Nick: I read a factoid—and tell me if I'm right or wrong about this—but that certain big publishers generate upwards of 6 terabytes of personal data a day just from video games.

Steve: That's incredible. Yeah, it just goes to show you, I don't know if there's enough awareness out there as to how much personal information is generated by video games. So why don't you walk us through what types of information are generated.

Nick: Sure. So it depends on the video game, right? You know, back in the old days of Nintendo, it would only save game data, you know, the number times of you've played, your saves, how far you've gotten, so there was not a concern that the data you generated by playing the game was going to get sent to Nintendo or someone else for any kind of analysis or other use.

Steve: Which cookies you like to eat.

Nick: Which cookies you favor. But now, things are totally different and you'd be amazed what can actually be sent. So one example: in addition to all the actual game playing data that we mentioned earlier, you'll recall a few years ago Xbox came out with a little camera controller called the Kinect, and what it would do is it would actually take a video of wherever you set it up and you could control the game, it would capture your movement, you could control the game with your movement and control other functions just with your voice. And that controller, that interface would record and gather a bunch of the players' physical characteristics, including facial features, body movement and voice data.

Steve: You know, I looked into the Xbox old privacy policy and it actually called that information "skeletal tracking," which I thought was pretty spooky.

Nick: Yeah, that's a little weird. But in addition, other games can get your location and your surroundings. One good example is the Battlefield series has a feature, they do a lot of stat tracking, one feature they offer is that you can compare based on your IP address and other playing information, you can compare not only your stats against the global leaderboards but you can also compare it against other people in your own geographic area. So I could see if I was doing better or worse than other people in Tampa, Florida, where I was playing, or in Florida or the United States or the whole world.

Steve: I think that's pretty neat.

Nick: It is pretty neat, except I usually did worse. But other games will gather your surroundings or biometrics and other information that especially glean from your social networks, if you hook up Facebook or one of your other social networks to one of your gaming tags, which is growing popular now. You also have to consider mobile games; one interesting example is that we heard the NSA is apparently watching you when you play Angry Birds.

Steve: Mm-hmm.

Nick: According to docs that were revealed from Edward Snowden, the NSA used Angry Birds to collect phone numbers, emails, and user device codes.

Steve: Scary stuff.

Nick: Yeah, I also don't want them to know how bad I am at that game. Another really good example that maybe makes a little more sense would be Pokémon Go. So personally, I play Pokémon Go. I have never played a Pokémon game in my entire life until this game.

Steve: Not even on the GameBoy?

Nick: Not even on the GameBoy. For some reason, it's a franchise I just missed. But Pokémon Go came out on mobile platforms in the summer of 2016, and it got a lot of buzz, a lot of fanfare, and a lot of controversy because of some of the information it collects. So basically, for those of you who don't know, you play it on your phone and it's a modernized, updated version of the old Pokémon games where you would go around and collect these little creatures you find out in the world and you could build out a collection, you could improve them and evolve them and you could even have them battle. And Pokémon Go allows you to actually do that

out in the world when you go places, you can catch these things and build out your little collection. And to do that, the game superimposes the graphics of your character and whatever Pokémon you find, over the real world maps and with real world weather data of where you are and so in order to function properly the game has to record your location via GPS tracking. So it collects your geolocation data, among other things that your cell phone would already be gathering.

Steve: But that game got in trouble for collecting more than just that. It actually collected Google profile information. Why does Pokémon Go need to collect that information in order to deliver a quality game?

Nick: You'd have to ask them, all I know it is a quality game.

Steve: In addition to the information that Pokémon Go collects and some of those other games, in-game data could reveal a lot more, and this is where it kind of gets a little darker. Video games could also get very personal, [they] could reveal your temperament, how you react, what fears you might have if you jump in a certain game at a certain point if that causes you fear, your leadership skills depending on maybe what traits you select in game for a character, and even your political leanings.

Nick: Right, so there was a guy a few years ago who came up with a theory that you could learn a lot about a person's personality just by watching their in-game behavior. So, not necessarily based on your statistics or whatever you chose, but certain activities and certain behavior by players was associated or correlated with certain personality traits, if you believe the theory. And so that's how, by taking this game data that other people are just shooting into the game, they can extrapolate from that and some people believe that you can tell a whole lot about a person, not just their gaming traits.

Steve: And so what's the goal of all this? What's the goal of collecting all this personal information?

Nick: Well it's twofold, right? On the one hand they can make better games, they can learn where players are engaged, where players are not engaged, what types of features players like, what type of interfaces work and are confusing or are clear and intuitive, but also, as we said, it's a good way to find out where and how people are more likely to spend money.

Steve: Okay, Nick, I think it's time. It's time for the 1v1 Showdown.

Nick: Alright, excellent. Now, this is the part of the podcast as everybody knows where we take the issue of the day and have a mock argument. We assign each other different positions and face-off. Today, we're going to be debating the different ways that data privacy regulations could be implemented in the U.S.

Steve: That's right, Nick. It's really no point in debating the con and pro in saying we shouldn't have any data regulations, because I think that's where we're going. So instead, what we're going to do is we're going to debate how best to implement data privacy regulation. So we're going to say let the states do it, let the federal government do it, let them both do it, or let the market do it.

Nick: Alright, Steve, what's up first?

Steve: Nick, I'm going to start us off with this: states should be free to regulate data protection themselves. This is the classic Tenth Amendment argument, or position, and I'm quoting from the Tenth Amendment of the U.S. Constitution here: All "powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the states, respectively, or to the people." Privacy, if it is to be regulated at all, is a day-to-day governance responsibility that states should bear. The federal government should mind its business and let the states take care of the data processing practices of their citizens. Justice Brandeis said it best, Nick.

Nick: What did he say?

Steve: The states are laboratories of democracy where we try novel, social and economic experiments. Let the states work on different variations of data privacy laws so we can figure out what works best, because there's a lot of different debates and confusion as to what's the best approach here. Eventually, what we'll see is that the best—the cream—will rise to the top and eventually be implemented across the board. That's what we saw when California adopted its first ever website privacy policy regulation, CalOPPA—C-A-L-O-P-P-A for those taking notes at home. That's why we first started seeing website privacy policies become common place.

Nick: So it's California's fault?

Steve: It's California's fault and now they're following it up with the new California statute so they're going to change the game as we move forward. So at the end of the day, Nick, what works best for residents of California, may not necessarily work best for Floridians or Washingtonians so that's why the states should regulate data privacy.

Nick: Alright, well Steve, you must have skipped a few constitutional law classes in law school because I'm going to explain why the federal government should set a single standard that preempts state laws.

Steve: You knew I was there.

Nick: As we all know, interstate commerce is the federal government's business and as we learned in Con-law, a guy growing wheat in his backyard affects commerce enough to make that the issue of the federal government, not the states. And so if growing wheat in your backyard is enough, then certainly selling games—including these monster AAA behemoths—is enough to affect interstate commerce and put this in the hands of the federal government. The gaming industry in particular is not in any one state, even though it may be, you know, more popular in some states than others.

Steve: I'd beg to differ with Farming Simulator; I think that's only in some states.

Nick: Well fortunately they can send that and sell that game anywhere they want; it's a worldwide phenomenon. So the federal government can and should regulate this. As a practical matter, how can you have different laws by state that apply to video games? You don't release a game in one state only, once it's online, it's everywhere. So state-by-state regulation would mean that the most restrictive state rules everyone because game developers would have to make them compatible with their rules from that one state and that would apply across the board. So it's better for businesses to have consistency across the board by having a federal standard. Businesses already struggle and innovation is stifled when there are too many different and sometimes inconsistent regulations that need to be met. For example, you've got one state that says you have to disclose certain information, you have another state that says you can't disclose certain information—it would be really difficult to comply with both, if not impossible. It's already difficult enough to comply with laws country by country; having all 50 states weigh in with their own little perspective would only make it worse. So I've got to say at the end of the day, some things are so important you should not encourage variation. Consider COPPA, for example, which you brought up a minute ago, which regulates the use of children's data, that statute preempts state laws—probably because protecting kids' data is not something we should be testing in your little state laboratories.

Steve: Alright, Nick, fine—if the federal government is going to get involved, it should at least permit the enactment of stronger state regulations and I'm going to tell you why. And what I mean by that: let the federal government pass a law that creates a minimum standard, let's say the floor, and let states have room to create more exacting standards if need be, the ceiling. So don't preempt states from having the right to govern themselves if they would like greater data protection for their citizens. So this is how Gramm-Leach-Bliley works. California is pretty famous for its Financial Information Privacy Act, and because Gramm-Leach doesn't preempt state laws, California was able to come out with a statute that offers greater protections than Gramm-Leach by increasing disclosure and notice requirements before processing and sharing data. The Fair Credit Reporting Act is another example where some states have their own statutes that require opt-in consent before certain data can be shared by financial institutions. Some games, take Pokémon Go which you talked about a minute ago, target and collect information from children, and parents may not be aware of what data and information their kids are giving game developers. That's why allowing states to pass tougher regulations can help. And as I said before, what works in one state may not necessarily work in another state. So we should let states decide what works best for their own citizens. The federal government doesn't explicitly treat—and this is another point—the federal government doesn't explicitly treat privacy as a constitutional right.

Nick: It's implied.

Steve: It might be implied from the Fourth Amendment, but states like California and Florida actually write it into their state constitutions, which arguably maybe they treat privacy a little, you know, more of a fundamental right. So that's another reason why states should be allowed and the federal regulation, whatever, shouldn't preempt. In a word Mr. Brown: Don't tread on me.

Nick: Wow, okay well, by my count that's four words but I'll let that go. However, I will say you've convinced me, I've changed my mind; let's not have any regulation—all the way against the other side. No regulation whatsoever. Let the market decide, capitalism at its finest.

Steve: Wow, coming from you, that's pretty big.

Nick: Listen, overly restrictive regulation can hurt business and in this case game development. Okay? You don't want to stop getting these great games just because they have to tip toe around the privacy laws. You know, and I'll say Pokémon Go gets unfairly singled out; it's hardly more dangerous to you than carrying your smartphone in the first place. As we all know, your smartphone can track you any time it wants, owning a cellular phone in your name instantly diminishes your privacy whether or not you have games on it, because most mobile devices can be tracked whether or not they're powered on by the carriers' cell towers. And so you might as well go ahead and fill out your Pokédex if you're already giving up your privacy by having a cell phone. In the end, it is your responsibility and mine to protect your own data; it's a personal responsibility issue. There are things you can do or parents can do for their children to minimize their data being collected by games and the government shouldn't come in and tell people what they can and can't do. The games that are better at allowing people to do that, to manage their own data and to know where it's going, those are the ones that are going to excel in the marketplace. If people don't want the benefits of these games, nobody's making them play, if you get scared because you don't know what a game is going to do with your data, just don't buy it.

Steve: I'm not scared, Nick.

Nick: I hope not. Not all developers, even at the end of the day, use this data for bad purposes. Player data is generally utilized to make games better, it finds out where the holes are, where people want to go and where resources should be diverted. It improves game mechanics and features and removes bugs, and for those companies who do mishandle data or do nefarious things with your data, people are going to find out about that and they're not going to be very popular. And so let the market take care of that too: survival of the fittest. We should go with the ones that handle their own data best and everyone should be in charge of their own.

Steve: Wow, I'm glad this is being recorded. Nick, the robber baron! That's a pretty bold assertion, in fact the boldest assertion I've ever heard from you.

In the end, we don't know how all this is going to shake out, Nick. Congress is considering a number of variations and states continue to introduce new statutes but there are a number of things that developers and gamers can think about going forward.

Let's start off with developers. Okay, so some takeaways for developers, I think we are in a very exciting time for privacy in that it's really top of mind for consumers. So one thing that developers can do to really stand out among their competition is to think about and maybe set their brand, their product apart by thinking about privacy implementing in their game, being transparent with their data collection practices. What does that mean? Writing clear, plain English, privacy policies and terms of service, also, taking privacy and implementing it into the design phase of games.

Nick: So think about from the start; don't think about it as an afterthought.

Steve: Exactly. Every time you have a new game maybe one of the things should be what kind of data are we going to collect? Maybe we shouldn't be collecting everything—like for Pokémon Go, maybe we shouldn't be collecting Google profile information, that's the step too far. And that would maybe avoid press issues or whatever that come later. But I think just having that implementation in the design phase is what's key and that's what helps to design a game that's maybe more data privacy-friendly. And other things that can be done, know the regulations and the various data protection laws that may apply and may affect the business, which again, it's pretty tricky in the United States because of the way that privacy has grown up, the privacy regulations are just kind of sectorial.

Nick: And it's going to change over time, right? What's true today with respect to the privacy laws may not be the case in another year or two.

Steve: That's right. It's really a brave new world when it comes to data privacy in the U.S. And also, another key thing before we move on to gamers is to understand that compliance is not going to happen on day one. Compliance is like getting on the road and starting a marathon. It's a process and every

day you're working towards getting closer to that 100% compliance goal. And so just understanding it's a process and the regulators know that and it's just a matter of trying your best, so that's another thing to keep in mind.

And also, try your best not to over promise security. In this day and age in particular, it's just getting, unfortunately a matter of when, not if, something bad would happen with data so you want to avoid that by not over promising things when you can.

Nick: And on the other side of the spectrum for consumers, gamers and esports competitors, you know, kind of similar to what we talk about in our podcast episode on cybersecurity, you always want to practice safe cyber hygiene. And part of that involves knowing what data you're giving up and not being afraid to push back or try to research more if necessary. It's always a good idea to use a password manager to change up your usernames and passwords so you don't use the same one on every site and so you can also pick a very strong password that's unlikely to get determined by somebody else. You can also use two-factor authentication to minimize the impact of any breaches that occur.

And at the end of the day it's all about consumer choice and being an educated consumer. So read up and understand what's going on. And as terrible as this sounds, take the time to read the privacy policies and the terms of service that come with your games, don't just click accept like most people do. And feel free to reach out to the game developer if you have questions, who knows, they may be happy to talk with you about this issue. But as always, the best idea is to work with an attorney who understands the industry and the legal trends that are at play in this fast-changing landscape.

Steve: Agreed 100%, Nick. That's all we have today on data privacy in gaming, that's pretty exciting stuff. Unless you have anything further to add, Nick.

Nick: That's all I've got, just make sure to be on the lookout for other episodes of LAN Party Lawyers Podcast and until then...

Steve: Game on.

Nick: ...game on.

This is a transript of a LAN Party Lawyers podcast. Listen to the podcast at https://youtu.be/QArZRAb0NS0 or on iTunes, Google, and Spotify.

The Imitation Game: How the CCPA Is Inspiring Other States to Regulate Consumer Data and Online Privacy

September 12, 2019

Joshua L. Gutter

On January 1, 2020, certain companies doing business in California will be subject to the California Consumer Privacy Act (CCPA). This statute is designed to grant California consumers various rights with respect to their personal information that is collected, stored, and monetized by commercial enterprises. Accordingly, in the absence of a federal consumer privacy statute in the United States, the CCPA is arguably the most significant law in the country in terms of regulating consumer data and online privacy.

With that said, other states in the United States are following California's lead and adopting consumer privacy laws of their own. Nevada recently amended its existing data privacy statute governing the security of information maintained by data collectors and other businesses. The amendment prohibits "an operator of an Internet website or online service which collects certain information from consumers in this State from making any sale of certain information about a consumer if so directed by the consumer." This amendment is slated to go into effect on October 1, 2019 (nearly three months before the CCPA). Maine is another state that has proposed and passed a bill related to consumer privacy. Unlike the CCPA and Nevada's statutory amendments, however, Maine's new law focuses exclusively on the regulation of broadband internet access providers.

There are a number of other states that have consumer privacy proposals in the pipeline, and the International Association of Privacy Professionals has designed a useful comparison table of these bills (while also identifying 17 common privacy provisions). While not a full-fledged consumer privacy statute, Connecticut passed a bill creating a task force to study this subject matter and what related laws might be implemented in the future. Massachusetts, on the other hand, has a comprehensive bill progressing through its legislature, which provides for a private right of action that is broader than the CCPA. Similar to the CCPA, however, any contract or agreement that attempts to waive or limit consumers' rights under the proposed Massachusetts statute will be void and unenforceable. But even in the midst of states' collective interest in protecting consumer data and online privacy, some jurisdictions are facing setbacks.

For example, New York's robust consumer privacy bill was not passed during the state's most recent legislative session. Washington, a state that even has an Office of Privacy and Data Protection, also failed to pass its Washington Privacy Act this year (and this bill sought to regulate new forms of data collection such as facial recognition technology). Nevertheless, even though some proposals are facing legislative obstacles, the comprehensiveness of these bills reinforces the trend that states are becoming more engaged in this space.

In conclusion, as the CCPA is getting ready to go into effect, states across the country are following California's lead to implement consumer data and online privacy laws within their respective jurisdictions. However, in the absence of a federal statute, it is possible that the growing number of nuanced state bills will be an administrative headache for companies that fall within the ambit of each state's laws. For now, the next step in tracking this regulatory evolution is to look to California, Nevada, and Maine to observe how these laws will be enforced in practice, how the business community will respond to this new reality, and how other states will build these practical considerations into their emerging legal frameworks.

Atlanta
One Atlantic Center
1201 W. Peachtree Street | Suite 3000
Atlanta, Georgia 30309-3455
404.815.3400 | fax 404.815.3415

Hartford
One State Street | Suite 1800
Hartford, Connecticut 06103-3102
860.392.5000 | fax 860.392.5058

Los Angeles
2029 Century Park East | Suite 1200
Los Angeles, California 90067-2913
310.843.6300 | fax 310.843.6301

Miami
Miami Tower
100 S.E. Second Street | Suite 4200
Miami, Florida 33131-2113
305.530.0050 | fax 305.530.0055

New Jersey
180 Park Avenue | Suite 106
Florham Park, New Jersey 07932-1054
973.828.2600 | fax 973.828.2601

New York
Chrysler Building
405 Lexington Avenue | 36th Floor
New York, New York 10174-3699
212.785.2577 | fax 212.785.5203

Orlando
SunTrust Center – Main Tower
200 S. Orange Avenue | Suite 1000
Orlando, Florida 32801-3400
407.849.0300 | fax 407.648.9099

Tallahassee
215 S. Monroe Street | Suite 500
Tallahassee, Florida 32301-1866
850.224.1585 | fax 850.222.0398

Tampa
Corporate Center Three
at International Plaza
4221 W. Boy Scout Boulevard | Suite 1000
Tampa, Florida 33607-5780
813.223.7000 | fax 813.229.4133

Washington, DC
1025 Thomas Jefferson Street, NW
Suite 400 West
Washington, DC 20007-5208
202.965.8100 | fax 202.965.8104

West Palm Beach
CityPlace Tower
525 Okeechobee Boulevard | Suite 1200
West Palm Beach, Florida 33401-6350
561.659.7070 | fax 561.659.7368

Carlton Fields practices law in California through Carlton Fields, LLP.

www.carltonfields.com

(10/2019)

CARLTON FIELDS