Bloomberg Law®

bloombergbna.com

INSIGHT: The California Consumer Privacy Act's Radical Impact on the Digital Ad Ecosystem

BY MICHAEL HAHN AND MATTHEW SAVARE

The State of California recently enacted into law the new, sweeping California Consumer Privacy Act of 2018, which will go into effect on Jan. 1, 2020. Experts estimate that the Act will apply to more than 500,000 U.S. companies, reaching businesses of various sizes in virtually every sector. To be sure, the Act will have profound implications for the digital advertising industry, given its breadth and seeming extraterritorial reach. In this article, we explore the scope of the law and how its more significant provisions will impact digital advertising.

Scope of the Act The Act's incredibly broad scope is moored in the Legislature's finding that consumers need protection from businesses that collect, sell, or otherwise disclose broad swaths of personal data for business purposes. The Act specifically identifies the Cambridge Analytica controversy as necessitating a legislative response.

That response was indeed broad in providing California consumers with a new set of rights: the right to know what personal information relating to them is collected; the right to know whether their personal information is sold or disclosed and to whom; the right to say no to the sale of their personal information; and the right to access – and demand the deletion of – their personal information. Of course, as the digital advertising industry has learned in its experience with the General Data Protection Regulation (''GDPR''), creating rights is easy; creating technology and policy mechanisms to comply is not.

Michael Hahn is General Counsel of the Interactive Advertising Bureau, IAB Technology Laboratory and Trustworthy Accountability Group. Matthew Savare is a partner at Lowenstein Sandler, where he practices digital advertising, blockchain, intellectual property, media, entertainment, technology, and privacy law with a particular focus on new media.

In many ways, the breadth of the Act is hidden in its definitions. Indeed, while the Act applies to ''businesses'' that ''sell'' or ''collect'' the ''personal information'' of ''consumers,'' those terms have broad reach beyond their plain meaning. ''Consumer'' means a natural person who is a California resident, however identified, including any unique identifier. Thus, the definition presumably includes California residents regardless of whether they are physically in the state (i.e., residents traveling or temporarily working outside of California). That alone vastly extends California's extraterritorial reach beyond its borders.

''Business'' means any legal entity that is operated ''for the profit or financial benefit of its shareholders or other owners'' that ''does business in the State of California'' and satisfies at least one of the following: (i) has annual gross revenues in excess of $25 million; (ii) buys, sells, or receives or shares for commercial purposes personal information gathered from 50,000 or more consumers, households, or devices; or (iii) derives 50% or more of its annual revenues from ''selling'' consumers' personal information. Cal. Civ. Code § 1798.140(c)(1).

While the $25 million gross revenue requirement is objectively measurable and clear, the other two prongs are not. Fifty thousand or more consumers, households, or devices is ambiguous because, as noted, the definition of ''consumer'' is limited to California residents.

However, because the Act does not expressly require households or devices to be of California residents (or even located in California), it is unclear exactly what the Legislature intends here. A reasonable interpretation – in light of the Act's other overly broad provisions – is that the 50,000 number is not intended to be limited to California households or devices. Similarly, the 50 percent threshold applies to revenue generated from ''selling'' consumers' personal information. Importantly, in light of well-established case law on long-arm jurisdiction, the ''doing business'' in California proviso likely applies to any for-profit business that sells goods or services to California residents even if the business is not physically located in the state.

As with other recent privacy legislation, the definition of ''personal information'' is so expansive that one would be hard-pressed to conceive of any data that is not ''personal information.'' It includes 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). The Act then provides a non-exhaustive list of 11 broad categories of data that constitute ''personal information,'' many of which are standard, but some of which are not common and have profound implications on the digital advertising industry. For example, the definition of ''personal information'' includes ''Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement'' and ''[i]nferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.'' Cal. Civ. Code § 1798.140(c)(1)(F) and (K).

The Act does state that it does not restrict a business's ability to ''[c]ollect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.'' Cal. Civ. Code § 1798.145(a)(5). It defines ''deidentified'' as ''information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer. . . .'' Cal. Civ. Code § 1798.140(h). Given this very narrow definition, it is unclear if – and the extent to which – this carve-out will be meaningful in the digital advertising context. Specific interpretations of this definition may require guidance from the California Attorney General's Office, which is statutorily authorized to provide advisory opinions concerning the application of the law.

The definition of ''sell'' is virtually boundless. It means ''selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or **other valuable consideration**.'' Cal. Civ. Code § 1798.140(t)(1). Thus, the definition is clearly aimed at businesses that transact in any way in customer data, regardless of whether the data is actually sold or licensed for a fee. Simply disclosing data – even as part of, or incidental to, a larger transaction involving a product or services – likely constitutes a sale. It is difficult to conceive of an activity that does not fall within this definition given that the digital advertising ecosystem is built and predicated upon utilizing consumer data for ad decisioning, reporting, and optimization.

Finally, the definition of ''collect'' is expansive – well beyond the term's plain meaning – such that it reaches industry intermediaries. ''Collect'' means ''buying, renting, gathering, **obtaining, receiving**, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.'' Cal. Civ. Code § 1798.140(e).

In light of these definitions, all the participants in the digital advertising ecosystem (from publishers to supply-side platforms, exchanges, demand-side platforms, trading desks, advertisers, agencies, data management platforms, and verification service providers) are governed by and impacted by the Act.

Notices and Disclosures Regarding Data Practices and Access to Data The Act imposes a number of notice and disclosure requirements on businesses. Although these requirements are inartfully and incoherently drafted, they can be summarized as follows:

Any business that collects a consumer's personal information must, at or before the point of collection, inform the consumer as to (i) the categories of personal information to be collected; (ii) the purposes for which such personal information will be used; (iii) a description of a consumer's rights under the Act, including a ''clear and conspicuous'' opportunity to opt out from the sale of his or her personal information, as discussed below; and (iv) the designated methods for submitting privacy inquiries and requests, including, at a minimum, a toll-free telephone number and a website address. These general disclosures must be made in the business's online privacy policies and in any California-specific descriptions of a consumer's privacy rights and updated at least once every 12 months. As noted below, the opt-out notice must also be provided on the business's homepage.

Upon receipt of a verifiable request from a consumer, a business must disclose (i) the categories of personal information it has collected about that consumer; (ii) the categories of sources from which the personal information is collected; (iii) the business or commercial purpose for collecting or selling personal information; (iv) the categories of third parties with whom the business shares personal information; and (v) **the specific pieces of personal information the business has collected about that consumer.**

The Legislature's use of the expansive definition of ''collect'' in this context is not limited to publishers and other sites that obtain personal information **from** consumers. Rather, it ostensibly covers a wide range of activities, including those intermediaries that **receive** personal information from third parties. In the digital advertising context, this is incredibly broad as most parties in the ecosystem will – at some point – touch consumer data. And, given the broad definition of ''personal information,'' it is reasonable to conclude that this disclosure requirement falls not only on the publishers with which the consumer has direct contact (and contractual privity pursuant to the publishers' terms of use and privacy policy), but also on all the other intermediaries and participants in the ecosystem.

The Act contains a similar disclosure requirement for businesses that ''sell'' or disclose for a ''business pur-

pose'' any personal information. Among the many ambiguities and operational and technical challenges these requirements present, they also beg several important questions. Given all the participants in the complex ecosystem and the vast and myriad pieces of data each has ''collected,'' is it even realistic to provide the required disclosures, particularly with respect to the ''specific pieces of personal information the business has collected''? Are these the best ways to give the average consumer disclosure? To what extent, if any, are businesses required to educate the public?

In addition to providing information to consumers **about** the personal information businesses have collected, sold, or disclosed, the Act also requires them to deliver to consumers, free of charge, the actual data they maintain. Such data may be delivered by mail or electronically, and a business is not required to provide information to a consumer more than twice in any 12-month period.

Deletion of Data Consumers also have the right to request that businesses delete their personal information to the extent it was collected. Any business that receives a verifiable request for such deletion is required to delete the personal information from its records and direct any of its ''service providers,'' which are defined very broadly under the Act, to do the same.

There are nine exceptions to this deletion requirement that permit businesses to maintain consumer personal information in order to (i) complete a transaction; (ii) detect security incidents; (iii) debug errors; (iv) exercise, or ensure others may exercise, a right provided for by law (such as free speech); (v) comply with the California Electronic Communications Privacy Act; (vi) engage in research in the public interest; (vii) enable solely internal uses of the personal information that are reasonably aligned with the consumer's expectations; (viii) comply with legal obligations; and (ix) otherwise use the personal information internally and lawfully in a manner consistent with the context in which the consumer provided it.

Although the obligation to delete the personal information upon request seems to be a reasonable and simple request, it is not in the context of digital advertising. As an initial matter, there are literally dozens of companies that ''collect'' vast amounts of ''personal information'' (each as broadly defined in the Act) of end users in connection with a single ad unit. The notion that there is a single data controller and several data processors each with a single database for each end user is simply unrealistic in the digital ad realm. Moreover, as a practical matter, even if end users request deletion of their data from publishers, there is no corresponding obligation on the publisher to effectuate further deletion with downstream partners other than its service providers. That being the case, and the fact that data in this industry is often voluminous and dispersed, the right provided by the Legislature imposes a material burden on publishers but to no purposeful end.

Restrictions on Sale of Data The Act places significant restrictions on the sale of personal information, which has far-reaching implications given that ''sale'' is broadly defined to cover any transaction where personal data is part of the value exchange. In particular, companies that wish to sell ''personal information'' to third parties must first provide consumers with the ability to opt out. Publishers and website operators, as the entities that have direct relationships with consumers, must provide consumers with the ability to opt out in the particular manner specified in the Act – a ''clear and conspicuous link'' on the publisher's homepage, in its privacy policy, and in any California-specific description of consumer's rights titled ''Do Not Sell My Personal Information.'' While other requirements exist, this one is nothing short of a game changer in creating a highly visible modification in the way publishers interact with their consumers.

Importantly, the statute implicitly governs conduct outside of the State of California by requiring a ''Do Not Sell My Personal Information'' radio button because, as a practical matter, it is very difficult for publishers to discern if a consumer is located in California, New York, or any other state. Indeed, when a web server receives an IP address from a browser, it can call on a third-party database for geolocation information. Not only is such information imprecise for legal compliance purposes, but doing so would turn the purpose of the statute on its head by causing a look-up of personal information before an opportunity to opt out is provided. Therefore – even though it is not expressly required by the Act – publishers will likely present the radio button to all U.S. consumers in an attempt to comply with the Act.

Industry intermediaries are also presumably swept up by the Act's restrictions upon the sale of personal data. Assuming that intermediaries lawfully receive the personal information of certain consumers after a publisher provides an opt-out, such intermediaries are still ostensibly prohibited from selling such data as part of a digital advertising transaction unless consumers have the ability to opt out for a second time. Of course, DSPs, SSPs, and exchanges might reasonably ask how they can present consumers the opportunity to opt out when they do not have a direct relationship with them. The most obvious result is that the publisher would have to do it for them. Undoubtedly, this too will require guidance from the California Attorney General's Office.

To add to this complicated milieu, the Act prohibits the sale of personal information when a business has actual knowledge that the data pertains to a person under the age of 16 unless opt-in authorization is provided by either a parent or guardian (in cases where the consumer is under 13) or by the consumer (in cases where the consumer is between 13 and 16 years of age). Moreover, any company that ''willfully disregards'' the consumer's age is deemed to have actual knowledge. The Act has the practical effect of expanding the compliance regime required by the Children's Online Privacy Protection Act (''COPPA''), which, along with its implementing regulations, enhances parental control over the personal information collected from children under 13. Unlike COPPA, which defines the requirements for verifiable parental consent, the Act does not describe what constitutes a valid authorization.

Non-Discrimination The digital advertising industry is what economists call a two-sided market, where publishers connect advertisers to consumers. On one side of the market, advertisers pay to advertise on publishers' websites and applications, and on the other side, publishers enter into a quid pro quo with consumers where the publishers give away content in return for exposing the consumer to advertising, while utilizing consumer data that renders such advertising more valu-

able. The Act explicitly disrupts the value exchange in the second half of the two-sided market with a non-discrimination requirement that bars publishers and other website operators from denying access to consumers that choose not to provide their personal information. In essence, the law mandates giving consumers content with less in-kind value provided in return. In some ways, it is like ad blocking, where consumers block ads but take the content, except here such taking is state-sanctioned.

The Legislature attempted to ameliorate this constitutionally-questionable requirement by including a proviso that states companies can charge different prices, but only if the differential approximates the value of the data withheld. Not only does this provision not address the right of a business to refuse service when it receives little in-kind value in return, it mistakenly assumes that a market value can be reasonably ascribed to any particular piece of data at the point of collection, instead of the value when data is aggregated and enhanced. As those who have litigated the cost justification defense to the federal price discrimination law (i.e., the Robinson-Patman Act) well know, courts spent decades trying to create a workable standard for how to assess cost differentials in sales of goods to competitors. Here, such a task would be infinitely more difficult because the value of data is intrinsically more complicated to determine, especially at the point of collection, relative to the cost of manufacturing and selling a good.

Conclusion In many respects, the Act is the most far-reaching state privacy legislation in the United States. Unfortunately, the law was rushed through the Legislature, the results of which show in its circuitous cross-references, numerous vague provisions, and some clear mistakes. Less than a week after passage, certain legislators – after a backlash from different groups – have already conceded that the Act needs a number of changes to address ''technical, non-substantive, and non-controversial drafting errors.'' This sweeping and inartful legislative response will create significant compliance challenges. Worse yet, this law begins the first of what may be a patchwork of state laws with potentially ambiguous and conflicting requirements.

About the Authors

Michael Hahn is General Counsel of the Interactive Advertising Bureau, IAB Technology Laboratory and Trustworthy Accountability Group. Matthew Savare is a partner at Lowenstein Sandler, where he practices digital advertising, blockchain, intellectual property, media, entertainment, technology, and privacy law with a particular focus on new media.