# The California Consumer Privacy Act of 2018: Why It Matters to Clients in Arkansas

By Drake Mann

Drake Mann is a Shareholder and Director of Gill Ragon Owen, P.A. Mr. Mann is a privacy law specialist certified by the ABA-accredited International Association of Privacy Professionals (IAPP). The IAPP has also designated Mr. Mann a Fellow of Information Privacy and awarded him certifications in privacy technology and privacy management. In addition, Mr. Mann is a Certified Information Systems Auditor (ISACA) and a Certified Cloud Security Professional (ISC)2.

The larger contours of new privacy laws may seem intuitively familiar in Arkansas, where the courts have expressly recognized a common law right to privacy since 1962.[1] But the explosion of technologies that capture, hold, and distribute massive amounts of personal data has resulted in these larger contours giving way to statutory particulars. The two most significant pieces of civil law that dramatically changed the privacy-law landscape in 2018 are the European Union's General Data Protection Regulation (the "GDPR"), which became enforceable on May 25, and the California Consumer Privacy Act of 2018 (the "CCPA"),[2] which Governor Jerry Brown signed into law on June 28. Although the CCPA will not become effective until January 1, 2020, it appears likely to impact directly thousands of Arkansas businesses (with the added kick that it provides for a private right of action, albeit qualified). The CCPA has already added momentum to the growing demand for federal data privacy legislation, in part, to reduce the risk that 50 states' different privacy laws will bog down commerce. Congress has begun holding hearings to consider what shape federal consumer privacy laws might take.

Dismissing the GDPR or the CCPA as inapplicable to most Arkansans and therefore irrelevant carries a cost. Both the

GDPR and the CCPA (as well as most other privacy laws) impose obligations regarding how businesses handle information about people—obligations that are similar, if not identical, to each other—and that in some form may be incorporated in federal privacy legislation.[3]

Making changes to any business process or a data system is rarely simple. Trying to implement a whole suite of changes at one time to comply with new legislation can be disruptive and costly. Because businesses usually make small changes to their operations and computer systems on an on-going basis, by having a rough sense of California's new law, Arkansas businesses can begin now to implement incremental changes that will get them closer to compliance with whichever privacy law particulars eventually come to govern them. In addition, as noted in one recent study, many companies are embracing privacy legislation "as an opportunity to improve privacy, security, data management or as catalyst for new business models, rather than simply a compliance issue or impediment."[4]

**The CCPA appears poised to apply to thousands of Arkansas businesses.**

The CCPA is also a useful subject of study because it appears likely to apply to thousands of businesses in Arkansas. The CCPA will become enforceable sometime next year.[5] The CCPA will apply to for-profit legal entities that collect California consumers' personal information, that do business in California, and that either (a) have more than $25 million in annual gross revenue, (b) buy, receive, or share the personal information of 50,000 or more "consumers, households, or devices," or (c) derive 50 percent or more of their annual revenues from selling consumers' information.[6] By one analysis,[7] more than 10,000 Arkansas businesses meet the first threshold (i.e., they have more than $25 million in annual gross revenue). Given the nature of modern interstate commerce, it is no great stretch to conclude that thousands of those Arkansas businesses do enough business in California to come within the reach of California's long-arm jurisdiction. Larger Arkansas businesses that process consumers' personal information therefore have particular reason to become familiar with the CCPA.

In addition, the CCPA's definition of "personal information" is notably broad and includes information "capable of being associated with, or [which] could reasonably be linked, even indirectly," with a particular consumer or household.[8] Identifying information includes obvious identifiers such as a natural person's name, address, email address, social security number, or driver's license number, but also includes information captured automatically by many website management tools, such as an advertising identifier, Internet Protocol address, or similar identifiers. Thus, if an Arkansas company hosts a website that performs basic tracking functions (logs an IP address and online advertising identifiers), there is risk that the CCPA will apply. If an Arkansas business's website merely receives these personal identifiers for 50,000 or more Californians (or California households), it should look closely at the CCPA.[9]

**What sorts of obligations does the CCPA impose?**

The CCPA, a brand-new statute, hurriedly written,[10] with more than 10,000 words and still-unwritten regulations, is not susceptible to a complete analysis in this article. But, by getting a sense of the CCPA's broader outlines, Arkansans can better understand these areas of current legislative concern and begin to adapt their business processes with the expectation that similar obligations are likely to come along soon.

Among other things, the CCPA provides California consumers with (1) the right to know what types of data a business has about an individual and the sources of that information; (2) the right to know what a business does with the data, including sharing it with, or selling it to, third parties;[11] (3) some right to deletion; (4) the right to opt out of the sale of personal information; (5) the right to know, at or before collection, the categories of information that will be collected and the purposes for which the information will be used; and (6) a prohibition against discriminating against consumers who exercise rights under the CCPA.

**Some implications of these obligations.**

Several of these obligations require businesses to track, and in some cases create, data that they never have before. For example, consider an Arkansas-based food company that periodically offers recipes and discounts to customers on its mailing list. These customers may have subscribed to the mailing list from the company's own website or the company may have bought the names and email addresses from an affiliated company that had gotten fine-print permission to share the data. In the past, the food company may not have cared where it got the names on its subscription list. Going forward, its databases will need to track the source of the information so the company can respond to requests from California consumers. In like manner, if the food company shares this information with others, the company will need to track at least the categories of third parties with whom it does so.

Many companies are treating these legislatively imposed changes as opportunities to improve the efficiency of their information-processing operations. For example, the CCPA requires a business to disclose the business purpose for collecting personal information. A business may find, on reflection, that it no longer has a good business purpose for collecting or retaining certain data. It may choose to cease doing so and thereby save storage and processing resources and reduce its potential data-liability footprint.

**"People, generally speaking, do not like being forced to do things, and the story of businesses chafing at any government regulation is as old as government regulation itself. Arkansas businesses can wait until they come under the jurisdiction of the CCPA, the GDPR, or some future federal legislation, and they can make only those changes they are forced to make.**

**Or Arkansas businesses can adopt a different attitude—an attitude expressed by one writer as the Golden Rule of Privacy: 'that companies should put the interests of the people whom data is about ahead of their own.'"**

In the same way, the CCPA's transparency and notice obligations create an opportunity to earn points with customers who have grown suspicious of data gathering in the face of public scandals involving data-processing and profiteering techniques. Opaque or vague disclosures can be replaced by simple and clear versions that engender trust.

**Responding to consumers' requests.**

Among other things, a California consumer is entitled to know what specific information a business has collected about that consumer and to request its deletion. A business must respond within 45 days of a "verifiable consumer request." The California Attorney General has not yet issued regulations regarding how a business might verify a request or document its response, but the GDPR imposes analogous obligations, and it should therefore come as no surprise if future federal legislation imposes a similar duty.

In addition, the CCPA gives consumers the right to opt out of the sale of their information before a business sells it, and a business that collects information from consumers between the ages of 13 and 16 must obtain from a parent or guardian an affirmative opt-in before selling that information.

As Arkansas businesses make on-going changes to their data-processing systems, they should consider planning mechanisms to implement a wide range of granular data-handling requests from consumers and regulators and to document their responses to those requests.

**Private right of action.**

The most-distinguishing feature of the CCPA is its qualified private right of action. The CCPA provides that a consumer whose nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of a failure to implement and maintain "reasonable security procedures and practices appropriate to the nature of the information" may institute a civil action for damages of not less than $100 and not more than $750 per consumer per incident or actual damages, whichever is greater, or injunctive relief. To pursue statutory damages, the consumer must first give a business 30-days written notice of the alleged violation, and, if the business "actually cures" the violation, no action may be initiated. There is no notice requirement, however, for a California consumer to pursue an action for actual pecuniary damages.

An Arkansas business serving Californians can therefore protect itself from the risk of a private civil judgment by encrypting or redacting personal information and implementing reasonable security procedures and practices. Practices such as these should already be commonplace, of course, even without the threat of a lawsuit from a consumer in California.

**Conclusion.**

People, generally speaking, do not like being forced to do things, and the story of businesses chafing at any government regulation is as old as government regulation itself. Arkansas businesses can wait until they come under the jurisdiction of the CCPA, the GDPR, or some future federal legislation, and they can make only those changes they are forced to make.

Or Arkansas businesses can adopt a different attitude—an attitude expressed by one writer as the Golden Rule of Privacy: "that companies should put the interests of the people whom data is about ahead of their own."[12] This approach regards the relationship between business and consumer as one of trust where companies holding data do so as "good stewards." Such a lodestar simplifies organizational governance and enables a company to express itself with clarity and congruence throughout—from its public notices to its computer code.

Dismissing others' concerns about privacy may further erode trust, and, in the not-too-distant future, result in potentially significant liability.

**Endnotes:**

1. In 1962, the Arkansas Supreme Court recognized the tort of invasion of the right to privacy when it upheld a $2,500 jury verdict in favor of a Searcy housewife whose picture had been reproduced on thousands of advertising postcards for a photography studio. *Olan Mills v. Dodd*, 234 Ark. 495, 353 S.W.2d 22 (1962).
2. Cal. Civ. Code §§ 1798.100–1798.199.
3. Examining Safeguards for Consumer Data Privacy, U.S. Senate Committee on Commerce, Science, and Transportation, hearing held September 26, 2018, https://www.commerce.senate.gov/public/index.cfm/2018/9/examining-safeguards-for-consumer-data-privacy (last accessed January 7, 2018).
4. *IBM Study: Majority of Businesses View GDPR as Opportunity to Improve Data Privacy and Security*, May 16, 2018), https://newsroom.ibm.com/2018-05-16-IBM-Study-Majority-of-Businesses-View-GDPR-as-Opportunity-to-Improve-Data-Privacy-and-Security (last accessed January 7, 2018).
5. "The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner." Cal. Civ. Code § 1798-185(c).
6. Cal. Civ. Code § 1798.140.
7. In July 2018, Rita Heimes and Sam Pfeifle, Research Director and Content Director, respectively, of the International Association of Privacy Professionals published an analysis based on "a rule of thumb in the business-reporting world that estimates a company's revenue by the number of employees it has. Under this assumption, a company will gross an average of at least $100,000 per employee." Using information from the U.S. Census Bureau, in 2015, 11,378 Arkansas businesses had "more than 500 employees, which translates to more than $50 million in revenue." Heimes and Pfeifle add: "consistent with well-established jurisprudence on long-arm jurisdiction, 'doing business' in California applies to companies that sell goods or services to California residents even if the business is not physically located in the state."
8. "Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:
   (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
   (B) Any categories of personal information described in subdivision (e) of Section 1798.80.
   (C) Characteristics of protected classifica-

tions under California or federal law.
(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
(E) Biometric information.
(F) 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.
(G) Geolocation data.
(H) Audio, electronic, visual, thermal, olfactory, or similar information.
(I) Professional or employment-related information.
(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
(K) Inferences 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, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Cal. Civ. Code § 1798-140(o)(1).

9. Although the CCPA contains an ambiguously-worded exception for de-identified data, the process of de-identifying data to the point that it could not be reasonably linked, even indirectly, to a household is no simple feat.

10. *The Unlikely Activists Who Took On Silicon Valley — and Won*, The New York Times Magazine (August 15, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html (last accessed January 7, 2019).

11. (a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:
(1) The categories of personal information it has collected about that consumer.
(2) The categories of sources from which the personal information is collected.
(3) The business or commercial purpose for collecting or selling personal information.
(4) The categories of third parties with whom the business shares personal information.
(5) The specific pieces of personal information it has collected about that consumer.
(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer.
(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:
(1) The categories of personal information it has collected about that consumer.
(2) The categories of sources from which the personal information is collected.
(3) The business or commercial purpose for collecting or selling personal information.
(4) The categories of third parties with whom the business shares personal information.
(5) The specific pieces of personal information the business has collected about that consumer.

Cal. Civ. Code § 1798.110.

12. Cameron F. Kerry, *Why protecting privacy is a losing game today—and how to change the game*, Brookings Institution (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ (last accessed January 7, 2019). ■