Expert Analysis

New 'Shine The Light' Suits Highlight Privacy Issues

By **Stephanie Sheridan, Anthony Anscombe and Meegan Brooks**

July 16, 2018, 6:12 PM EDT

Stephanie Sheridan

Anthony Anscombe

Meegan Brooks

California caught national attention on June 28, 2018, when the state legislature passed the California Consumer Privacy Act of 2018, already being hailed as one of the toughest data privacy laws in the country. The CCPA, which sailed through the legislative process in less than two weeks, will not take effect until Jan. 1, 2020, and could very well be amended before then. California's enactment of CCPA is not entirely surprising given the introduction of its European counterpart, the General Data Protection Regulation, which came into effect in May 2018.

Although the CCPA is certainly California's most comprehensive privacy legislation to date, it is certainly not its first. Indeed, over the past few weeks, several putative class actions have been filed alleging violations of California's Shine the Light law (Civil Code § 1798.83), a privacy "right to know" statute enacted in 2005. More could follow. Retailers should use this as an opportunity to review their own practices to ensure compliance before they receive a summons and complaint — and well before the CCPA takes effect.

For those unfamiliar with it, the Shine the Light law is part of California's Consumer Records Act, which requires companies doing business with California residents to take certain steps to protect customers' personal information, including providing notice if personal information is compromised. The Shine the Light law provides consumers with a way to contact companies they believe may have disclosed their personal information for direct marketing purposes, in order to obtain information about those disclosures and opt out of them, if they so choose.

The Shine the Light Law's Requirements

The Shine the Light law applies to most companies that, during the last year, “disclosed” the “personal information” of “customers” to a “third party” that the company knows or has reason to know used that information for “direct marketing purposes.”

The statute provides expansive definitions for most of the quoted terms:

- “Disclose” means to “transfer” — whether orally, in writing, electronically “or by any other means.” The statute provides limited exceptions, such as disclosures for account administration or customer service purposes.

- "Personal information” means any information that identifies, describes or is even associated with an individual. The statute includes an extensive list of information that fits within this definition, including name, address, email address, telephone number, date of birth, medical and financial information, information about children, race, religion, occupation and education and information about the transaction. Crucially, the law is not limited to personal information collected online, meaning that companies should also consider their data sharing practices with respect to customer data collected offline as well.

- “Customer” means an individual, resident of California, who provides personal information to a business pursuant to an “established business relationship.”

- “Established business relationship,” in turn, means an ongoing relationship between a business and a consumer, formed by a voluntary two-way communication, for the purpose of purchasing, renting or leasing a product or service or a relationship which was ongoing within the last 18 months.

- “Third party” means a legal entity separate from the business that has access to a shared database used for direct marketing purposes; third parties include both affiliates and separate third parties, but do not include businesses affiliated by common ownership or corporate control.

- “Direct marketing purposes” means the use of personal information to “solicit or induce” a purchase, rental, lease or exchange of products, goods, property or services “directly to individuals” using the mail, telephone or email. Certain exemptions apply.

Businesses that fall within the definition above have three options for compliance:

- Provide an accounting to customers upon request of the categories of personal information disclosed to third parties and identities of those third-party entities (an “accounting”), as discussed below.

- Develop and implement an opt-in or opt-out policy allowing customers to control whether their information will be shared with third parties for marketing purposes.

- Companies subject to the Gramm-Leach-Bliley Act (which requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data) may satisfy Shine the Light’s requirements by complying with that Act’s disclosure requirements.

If companies are already complying with the GDPR’s requirements to obtain “freely given, specific, informed and unambiguous” opt-in consent to direct marketing (which would include obtaining their specfic consent to sharing their personal data with third parties), then they are likely to satisfy the Shine the Light law’s opt-in policy requirements, detailed at (2) above. Businesses which go this route can comply with the law by “notifying the customer of his or her right to prevent disclosure of personal information, and providing the customer with a cost-free means to exercise that right.” Cal. Civ. Code § 1798.83(c)(2).

Focus of the New Wave of Litigation — The Accounting Requirement

The new wave of litigation that has been recently filed is brought pursuant to the Shine the Light law’s accounting requirement, which mandates that companies disclose, upon request, the names and addresses of third parties with whom personal information was shared, as well as a list of all categories of personal information provided. This information may be provided in a standardized format — it does not need to be specific to the individual. If the customer’s request is made through the designated channels, the company must provide a response within 30 days.

If made through other channels, the response should be made within a reasonable time, but no more than 150 days. Customers may request an accounting once per year.

Businesses going the “accounting” route must designate a specific postal address, email address or toll-free phone or fax number that customers may use to request an accounting. This method of contact must be communicated to customers through at least one of the following:

- Managers and agents: Businesses can comply by having managers and agents who directly supervise customer-contact employees (including cashiers, clerks, customer service, sales or promotions agents), educate those employees as to where to direct customers who request an accounting.

- Websites: A second option is to add a link to the homepage of the company’s website titled “Your Privacy Rights,” or to add the same words to the homepage’s link to its privacy policy. The first page of the link should describe the customer’s rights under Section 1798.83 and provide the designated mailing or email address, as required, or toll-free telephone or facsimile number, as appropriate.

- Brick-and-mortar stores: Businesses can also make the designated method of receiving customer requests, or the means to find that designated address, available at every California place of business where the company or its agents have regular contact with customers.

Although businesses have three options to comply with the disclosure requirement, online retailers and other e-commerce sites should, at a minimum, comply with the second option above by adding a hyperlink and disclosures on their websites. This is essential, because plaintiffs in past Shine the Light cases alleged businesses that operate primarily online do not qualify to satisfy the disclosure requirements through the other two options.

Under Section 1789.84(b), a customer must be “injured” by a violation to file a civil action to recover civil penalties of $500 ($3,000 for willful, intentional or reckless violations), for each instance in which the company did not adequately respond to a customer request, provided there is a limit of one violation per customer per year. In addition, prevailing plaintiffs may recover their reasonable attorney’s fees and costs.

Previous Shine the Light Litigation

While the statute has been in effect since 2005, it received little attention until late 2011, when several putative class actions were filed in California state and federal courts. Those lawsuits primarily targeted prominent media and technology companies with significant (if not exclusive) online presences. That spurt of lawsuits dissipated in December 2013 and February 2014, however, once the California Court of Appeal, and then the Ninth Circuit, affirmed the dismissal of Shine the Light cases for lack of injury, finding that to plead a statutory injury, a plaintiff must have made, or attempted to make, a request for an accounting.

The plaintiffs in the new suits have tried to plead their way around those earlier Ninth Circuit and California Court of Appeal decisions by expressly alleging that they submitted written requests but the companies failed to timely respond.

The CCPA Expands on 'Shine the Light,' and the GDPR Imposes Additional Requirements

The Shine the Light law partially overlaps with the the CCPA as currently enacted. CCPA allows California residents to request twice a year (more frequently than under Shine the Light): (1) the categories and specific pieces of data the company has collected from that individual; (2) the categories of sources from which the data was collected; (3) the categories of third parties to which the data has been disclosed or sold; and (4) the purposes for which the information was disclosed or sold (unlike Shine the Light, the CCPA is not limited to marketing purposes). The company must provide this information electronically (in a portable and readily usable format, if technically feasible), and within 45 days (subject to a 45- or 90-day extension where necessary).

Separately, the CCPA will require that companies provide customers with means to opt out of having their information sold. Thus, while offering an opt-out provision is a way for companies to comply with Shine the Light's accounting requirement, the CCPA requires both opt-out and accounting requirements.

As highlighted above, GDPR also overlaps with the Shine the Light law. Indeed, to the extent that US businesses are required to comply with GDPR, it is likely that many of the Shine the Light requirements will already be met. In addition to numerous other requirements, GDPR allows customers to request from businesses access to their personal information — which includes requiring businesses to provide information about the recipients or categories of recipients to whom their personal information has been, or may have been, disclosed — and to restrict the

ways their information is being used. Companies are required to respond to such requests within one month (subject to a limited 3-month extension in certain circumstances). Unlike Shine the Light or CCPA, however, GDPR does not restrict the number of times any given customer may submit such a request.

Thus, as companies evaluate their compliance with GDPR (to the extent that they are required to do so) and prepare to comply with the CCPA, they should make sure that they are also buttoned-up under Shine the Light's related requirements.

Conclusion

Businesses facing these claims should have several strong defenses to liability and class certification, but as always, it is better not to be sued at all. Careful compliance with the technical requirements of these laws is very important, as plaintiffs' lawyers will look for any opportunity to sue, regardless of how well-intentioned and proactive companies have been about their privacy policies.

Indeed, in each of the new Shine the Light suits, the defendant's privacy policy disclosed each defendant's practice of sharing information with third parties (as it should), and also included an online disclosure notifying customers of where to submit Shine the Light accounting requests (as required under the law). Because online retailers are required to disclose such information, it would be easy for plaintiffs, or lawyers trolling for lawsuits, to find potential targets via their privacy policies, send requests for accountings to each website and file suit for any that fail to timely respond. In-house counsel should confirm with those in charge of their company's designated Shine the Light contact information that protocols are in place to ensure timely and compliant responses to each accounting request.

Stephanie A. Sheridan and Anthony J. Anscombe are partners and Meegan Brooks is an associate at Steptoe & Johnson LLP.