Proskauer

Same Song, Different Tune: Plaintiffs' Bar Adds the Song-Beverly Credit Card Act to its Privacy Repertoire

Proskauer on Privacy on **September 5, 2024**

Repurposing old laws to challenge new technologies has become the new normal in the privacy space. Plaintiffs continue to bring a kaleidoscope of privacy claims against companies in the tech age, reviving laws like the California Invasion of Privacy Act of 1994 ("CIPA"), Video Privacy Protection Act ("VPPA"), Telephone Consumer Protection Act ("TCPA"), Pennsylvania Wiretapping and Electronic Surveillance Control Act, and Arizona Telephone, Utility, and Communication Service Records Act.

Internet tracking tools (e.g., pixels and cookies) have been at the center of many of these claims, and they now face yet another foe: California's Song-Beverly Credit Card Act (the "SCCA" or the "Act"). The SCCA became law in 1971 and regulates the types of information businesses may request from customers during credit card transactions. Now, more than fifty years later, increased scrutiny of these tracking technologies has led to the Act's renaissance.

What is the SCCA?

The SCCA prohibits businesses from requesting or requiring customer disclosure of personally identifiable information ("PII") before or during a credit card transaction and creating a record of that PII. Under the SCCA, PII includes "information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number." The California Supreme Court has expressly held that ZIP codes qualify as PII. See *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524, 530 (2011).

Several major exceptions apply. For example, businesses may collect PII when they are obligated to do so by law or contract. Business may also collect PII for identification purposes, so long as the information is not written or recorded, or when PII is required for "a special purpose incidental but related to the individual credit card transaction," such as shipping or delivery.

How are Plaintiffs using the SCCA today?

This particular trend of SCCA cases follows a recent wave of claims brought under CIPA, a wiretapping and eavesdropping law plaintiffs have retooled to target businesses integrating tracking technologies on their websites. Like the CIPA cases, SCCA claims hinge on the installation and utilization of cookies and pixels on companies' websites.

The crux of these SCCA claims rests on allegations that the tracking technologies businesses employ are unavoidable for any customer navigating their websites. According to plaintiffs, the very presence of tracking technologies on e-commerce platforms is unlawful when a user makes a credit card transaction because the tracking technologies lurk in the background, collecting the user's PII from the second they enter a website. Plaintiffs therefore argue that this automatic collection is a de facto "condition" of the credit card transaction, which violates the SCCA.

A class action filed in California Superior Court this past May against the popular outdoor gear and clothing brand Patagonia, Inc. is instructive. *Semain v. Patagonia, Inc.*, Docket No. 2024CUBT024729 (Cal. Super. Ct. May 15, 2024). In this case, plaintiff alleges that Patagonia requires consumers to provide their telephone number, email address, and IP address to complete credit card transactions on their website. According to the plaintiff, this practice violates the SCCA because this information constitutes PII, and the collection of this particular kind of PII was unnecessary to complete plaintiff's transaction because, in part, he did not purchase any electronically downloadable product that requires e-delivery.

While the SCCA expressly treats telephone numbers as PII, it is unclear whether email or IP addresses are, as well. Nevertheless, the Patagonia plaintiff assumes all three types of information qualify and alleges that the company has installed the Facebook Tracking Pixel, Google Analytics Tracking Tool, and PayPal Pixel onto their website. According to the plaintiff, these tracking tools automatically began "requesting" and "recording" his PII as soon as he navigated to the Patagonia website, which purportedly continued when he engaged in a credit card transaction. Accordingly, he had no choice but to provide his PII to Patagonia, creating a condition to credit card transactions in violation of the SCCA.

What does this mean for businesses who use tracking technologies on their websites?

At least nine complaints of this sort have been filed in California since May of this year, each alleging violations of the SCCA through the use of tracking technologies. One critical matter to monitor throughout all of these cases will be how the California judiciary lands on the issue of whether email and IP addresses constitute PII under the SCCA and, if they do, whether such collection by tracking technologies qualifies as an unlawful condition or otherwise falls under any of the Act's exceptions. Should courts determine that the use of tracking technologies to collect this information does violate the SCCA, businesses harnessing these tools could be held liable for up to $1,000 per violation. And, since these complaints have generally been brought as class actions, companies may face fairly sizeable penalties for their use of these technologies.

These SCCA cases are fresh, and their future success is unknown. The privacy landscape is constantly changing, making it vital for companies to collaborate with outside counsel to navigate challenges like SCCA claims. If your organization needs assistance assessing its risk posture with respect to these technologies and guidance on risk mitigation, please reach out to our Privacy & Cybersecurity Practice Group lead Leslie Shanklin. Organizations may also reach out to our litigation partners Baldassare Vinti, David Fioccola and Jeff Warshafsky for class action litigation defense strategies.

View Original

Related Professionals

- **Jeff H. Warshafsky**
  Partner

- **Aaron M. Francis**
  Associate