VENABLE LLP

the download

DEVELOPMENTS IN E-COMMERCE, PRIVACY, INTERNET ADVERTISING, MARKETING AND INFORMATION SERVICES LAW AND POLICY

ISSUE EDITORS

Stuart P. Ingis
singis@Venable.com
202.344.4613

Michael A. Signorelli
masignorelli@Venable.com
202.344.8050

ADDITIONAL CONTRIBUTORS

Emilio W. Cividanes
ecividanes@Venable.com
202.344.4414

Tara Sugiyama Potashnik
tspotashnik@Venable.com
202.344.4363

Julia Kernochan Tama
jktama@Venable.com
202.344.4738

Kelly A. DeMarchis
kademarchis@Venable.com
202.344.4722

1.888.VENABLE
www.Venable.com

MARCH 2011

In this Issue:

In the Courts

- **California Supreme Court Announces State Law Prohibits Marketing Requests for ZIP Codes**
- **Suit Filed Against Apple for Alleged Privacy Violations Arising from Applications**

Heard on the Hill

- **Senate Judiciary Committee Holds Hearing on Targeting Sites Dedicated to Stealing American Intellectual Property**
- **House Armed Services Subcommittee Convenes Hearing on Cybersecurity**

Around the Agencies

- **"In-App" Purchases Draw Congressional and Regulatory Attention**

In the Courts

California Supreme Court Announces State Law Prohibits Marketing Requests for ZIP Codes

In a case with major implications for retailers and marketers, the Supreme Court of California ruled on February 10, 2011, that the state's Song-Beverly Credit Card Act of 1971 ("Song-Beverly Act") prohibits businesses from requesting and recording ZIP codes from consumers prior to credit card transactions, including requests for use in marketing. *Pineda v. Williams-Sonoma Stores, Inc.*, S178241 (Cal., Feb. 10, 2011). Numerous other states have laws similar to California's that regulate merchant practices with respect to collecting and recording personal information in connection with a credit card purchase.

The Court held that its interpretation of the statute applies retroactively, opening the door to class action consumer lawsuits based on businesses' prior practices. The Song-Beverly Act provides for statutory damages of up to $1,000 per violation of the law. In the weeks since the Court's decision, numerous cases have already been filed in California against major retailers.

Case History

Plaintiff Jessica Pineda claimed that Williams-Sonoma violated the Song-Beverly Act by requesting and recording her ZIP code during a credit card transaction. The Song-Beverly Act generally prohibits merchants that accept credit cards from

requesting, or requiring as a condition of accepting the credit card payment, "personal identification information" ("PII") that the merchant then records. The central question in the *Pineda* case was whether a ZIP code alone constitutes PII. The Song-Beverly Act defines PII as "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." Cal. Civ. Code § 1747.08(b).

Williams-Sonoma prevailed at the trial court and intermediate appellate levels. The California Supreme Court reversed, concluding that "requesting and recording a cardholder's ZIP code, without more, violates the [Song-Beverly] Credit Card Act." *Pineda*, S178241 at 2. In part, the Court reasoned that interpreting the ban to include ZIP codes is more consistent with the principle that remedial statutes should be construed broadly to effectuate their purpose of protecting the public. The Court also expressed concern that retailers might use ZIP codes to "end run" around the statute's prohibition on requesting addresses.

The Court's ruling will not only guide future business practices, but creates the possibility of significant liability arising from past practices. The Court ruled that its new interpretation of the statute applies retroactively to past conduct, rejecting the defendant's argument that this interpretation renders the law unconstitutionally vague. As a result, plaintiffs may bring cases against businesses challenging requests for ZIP codes that occurred before the Supreme Court decision announcing that such requests are prohibited. The Court also did not agree with the defendant that the new legal interpretation makes the statute unconstitutionally oppressive, despite the Song-Beverly Act's statutory penalties of up to $250 for the first violation and $1,000 for each subsequent violation.

Suit Filed Against Apple for Alleged Privacy Violations Arising from Applications

Four lawsuits, at present count, have been filed against Apple and some of its application ("app") developers alleging violations of the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and state statutes based on app functionalities that shared consumers' personal information with advertisers. The lawsuits commenced after the *Wall Street Journal* published an article in mid-December detailing the results of tests of 101 popular smartphone apps for iPhone and Android phones, which claimed that 56 of the apps tested transmitted the phone's Unique Device Identifier ("UDID") to third parties. Allegedly, some apps transmitted information such as age and gender in addition to the UDID.

The complaints allege that after consumers purchased and downloaded certain apps from the iTunes Store, Apple transmitted their UDID to the application developers who, in turn, installed tracking identifiers on the mobile devices which allowed them to track all of the data generated by the mobile device. This information was allegedly provided to advertisers, and impaired the speed and functionality of the device. Along with Apple, the lawsuit names popular app developers such as WebMD, NPR, Groupon, Pandora, and the *New York Times* as defendants. The lawsuits seek class action status.

Heard on the Hill

Senate Judiciary Committee Holds Hearing on Targeting Sites Dedicated to Stealing American Intellectual Property

On February 16, 2011, the Senate Committee on the Judiciary ("Committee") held a full Committee hearing focusing on websites dedicated to unlawfully infringing U.S. intellectual property ("IP"). The 111th Congress had previously considered this issue through the vehicle of the Combating Online Infringement and Counterfeits Act ("COICA"). At the end of last year, the full Committee had voted 19-0 in favor of COICA, as amended by a Manager's Amendment. The stated purpose of the bill was to combat illegal online copyright infringement, and the bill called upon entities in the Internet ecosystem – including registrars, registries, Internet service providers ("ISPs"), payment system providers, and ad networks – to play a role in addressing this issue. While the full Senate never had an opportunity to consider COICA before the end of the congressional calendar, Committee Chairman Leahy

(D-VT) promised to revisit the matter in the new Congress.

Following through on his pledge, Chairman Leahy convened a hearing in mid-February with witnesses representing the interests of registrars, ISPs, payment system providers, and IP holders. Throughout the hearing, Chairman Leahy indicated that COICA legislation would pass this year, while Ranking Member Grassley (R-IA) asked witnesses for their views on the need for legislation. Witnesses from the IP holder groups urged the Committee to act now to protect their interests with legislation. Representatives from the registrar and payment system provider sectors, however, noted that many in industry already have procedures in place to help IP holders protect their rights. To the extent that any legislation may be appropriate, these witnesses recommended that any such bill should include a safe harbor for entities that respond to stop sites dedicated to stealing American IP from engaging in illegal activities.

As he noted in the hearing, Chairman Leahy has been in conversations with his counterpart in the House, House Judiciary Committee Chairman Smith (R-TX), to gain congressional momentum on this issue.

House Armed Services Subcommittee Convenes Hearing on Cybersecurity

The House Armed Services Subcommittee on Emerging Threats and Capabilities ("Subcommittee") convened its first hearing of the 112th Congress on February 11, 2011, to examine the role of the Department of Defense ("DoD") in cyberspace. Subcommittee Chairman Thornberry (R-TX) noted that the Subcommittee's new name underscored its focus on ensuring that the United States is prepared to deal with emerging threats (e.g., cyber threats) and nurturing capabilities to address these threats. He explained that our expectations of the DoD to protect us in the physical world are clear, but that expectations are less clear in the area of cyberspace. Chairman Thornberry further suggested that the subcommittee should examine whether the government (through the DoD and other departments) is authorized to act in this area. Subcommittee Ranking Member Langevin (D-RI) expressed concern that the government may lack the authority to mandate certain protections to keep the country safe in the realm of cyber and stated that it was a "tragedy of the commons" that no one, including industry, was willing to address the issue.

In a search for a solution, dialogue ensued among the Subcommittee members and witnesses, in which all agreed at a high level that the DoD, civilian government, and industry each have a role to play. Witness testimony also suggested that industry's commitment to addressing cyber threats has increased in the past few years, and that industry's role as a partner in cybersecurity could be improved through increased information sharing by the government. At the same time, witnesses recommended that the government could do more to create a welcome environment for industry to share its experiences pertaining to cyber threats with the government.

As the hearing came to a close, Chairman Thornberry concluded that witnesses were in agreement on the following: (1) the government should take some action to address cyber threats; (2) such action could take the form of incentives or mandates to increase cybersecurity; and (3) at a minimum, the DoD should ensure that the appropriate entities in the private sector have access to information from the DoD to help protect those private systems over which they have control.

In the months to come, the debate over the appropriate role for the government in cybersecurity is sure to continue, both in the congressional arena and within the Administration.

Around the Agencies

"In-App" Purchases Draw Congressional and Regulatory Attention

Representative Markey (D-MA) sent a letter to the Federal Trade Commission ("FTC") on February 8, 2011 regarding the privacy implications of mobile applications ("apps") and referencing an article published in the Washington Post on the same day about "in-app purchases" by children. (Cecilia Kang, "In-app Purchases in iPad, iPhone, iPod Kids' Games Touch Off Parental Firestorm") The

ABOUT VENABLE

One of American Lawyer's top 100 law firms, Venable LLP has attorneys practicing in all areas of corporate and business law, complex litigation, intellectual property and government affairs.

Venable serves corporate, institutional, governmental, nonprofit and individual clients throughout the U.S. and around the world from its headquarters in Washington, D.C. and offices in California, Maryland, New York, and Virginia.

article interviewed several parents whose young children had racked up hundreds of dollars of charges while playing games targeted at children on popular mobile devices. The apps profiled in the article are games designed for young children that are free or low cost to download, but feature the option to purchase intangible game pieces or other features during the course of the game. The apps were linked to parents' credit cards or online accounts and, according to the article, the children often made purchases without understanding that they were spending "real" money.

Last fall, Rep. Markey, with Rep. Barton (R-TX), authored a series of letters to online companies whose privacy practices had been singled out and commented upon in an ongoing series on online privacy published by the Wall Street Journal. These letters requested responses from the individual companies cited in the media reports.

Rep. Markey's most recent letter encouraged the FTC to "pursue measures to provide consumers with additional information about the marketing and delivery of these applications" and to investigate whether activities related to these apps potentially constituted unfair or deceptive acts or practices. On February 24, 2011, FTC Chairman Jon Leibowitz responded to notify Rep. Markey that the FTC "will look closely at the current industry practice with respect to the marketing and delivery of these types of applications." Rep. Markey vowed to monitor developments in this area.

Rep. Markey has vowed to make children's use of technology a priority for this congressional session and, in December 2010, he announced his intent to introduce legislation early in 2011 to prohibit the tracking of children's Internet usage. The FTC's response reflects the agency's ongoing focus on issues related to children's privacy. The FTC is already considering the privacy implications of children's use of mobile apps as part of its review of the Children's Online Privacy Protection Rule ("COPPA Rule") which began about a year ago. In March 2010, the FTC announced that it was expediting its review of the COPPA Rule in light of technological changes that have taken place since the COPPA Rule was promulgated a decade ago. As part of its review, the FTC has accepted public comment and convened a COPPA Rule workshop, but has not yet proposed modifications to the COPPA Rule.

Venable's Privacy and Data Security Team serves clients from these office locations:

WASHINGTON, DC
575 SEVENTH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300

NEW YORK, NY
ROCKEFELLER CENTER
1270 AVENUE OF THE AMERICAS
TWENTY-FIFTH FLOOR
NEW YORK, NY 10020
t 212.307.5500
f 212.307.5598

TYSONS CORNER, VA
8010 TOWERS CRESCENT DRIVE
SUITE 300
VIENNA, VA 22182
t 703.760.1600
f 703.821.8949

LOS ANGELES, CA
2049 CENTURY PARK EAST
SUITE 2100
LOS ANGELES, CA 90067
t 310.229.9900
f 310.229.9901

BALTIMORE, MD
750 E. PRATT STREET
SUITE 900
BALTIMORE, MD 21202
t 410.244.7400
f 410.244.7742