The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 19, No. 6 June 2011

Charting A Safe Course In The Perfect Storm Of Consumer Privacy Laws

Theodore C. Max

SHEPPARD MULLIN RICHTER & HAMPTON LLP

In *The Fountainhead*, author Ayn Rand wrote: "Civilization is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe." For retailers, this "progress" includes the confluence of the constant expansion of the collection of consumer information over the Internet and in the marketplace, the recent decision by the California Supreme Court in *Pineda v. Williams-Sonoma Stores, Inc*. and legislative initiatives to protect consumer privacy. Retailers are now facing a perfect storm that includes a tidal wave of class action litigations in California and a maelstrom of state, federal and international laws and regulations. In order to take advantage of the benefits of collecting and tracking consumer information and to create customized consumer coupons and benefits, care must be taken to understand the ever-changing legal climates, constantly monitor the shifting legislative shoals, and to avoid the reefs, shallows and quicksands of consumer privacy litigation.

California Supreme Court Has Retailers Singing The Song-Beverly Blues

Section 1747.08(a) of the Cal. Civ. Code of the Song-Beverly Credit Card Act of 1971 ("Song-Beverly") provides that people and entities that accept credit cards, except in limited types of transactions, may not "request, or require as a condition to accepting the credit card as payment … the cardholder to provide personal identification information." The request prohibition is much broader than the condition of transaction prohibition. The Song-Beverly Act defines personal identification information 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." Song-Beverly was modeled after the equivalent New York statute, the N.Y. Gen. Bus. Law § 520-a.[1] Suits challenging the legality of retailers' attempts to collect addresses and phone numbers have resulted in numerous consumer class actions.

Theodore C. Max

On February 10, 2011, the California Supreme Court held in *Pineda v. Williams-Sonoma Stores, Inc*. that a customer's zip code data constitutes "personal identification information" under Cal. Civ. Code § 1747.08 and that requesting the zip code data during the course of a credit card transaction, absent limited circumstances, subjects the requesting retailer to class action claims up to $1,000 per transaction, plus additional liabilities. The Supreme Court examined dictionary definitions of "concerning" and held that the cardholder's zip code "pertains to" or "regards" the cardholder. The Supreme Court examined and cited the legislative history and statutory construction of Song-Beverly in support of its decision. Since the decision, there has been a tidal wave of class actions in California based upon the collection of zip code data.

The collection of consumer information through other means, such as the distribution and use of "preferred shopper" cards, also may implicate by the Song-Beverly Act. The nuances of whether the Song-Beverly Act is implicated by marketing or retail efforts can be difficult to understand without knowledge of and experience with the case law and statute. Care should be taken to ensure that no salesperson nor any customer service personnel ask a customer to fill out the card once the credit card purchasing transaction has commenced. A sales associate can ask the customer to fill out the template card after the credit card is handed back to them and they have signed. Another option is to ask the customer to fill out the card on the floor before any purchasing decision has been made. How and when the card is presented to customers and what associates say to customers about the card is critical. Legal counsel and advice should be obtained in order to avoid and limit liability from class action cases under the Song-Beverly Act or other similar laws.

Navigating The Shoals And Reefs And Changing Climate Of Privacy Laws

Whether you operate and maintain a "brick and mortar" or online retail presence, any efforts to gather personal identification information and to communicate with consumers may, depending upon the situation, run afoul of the state and federal laws governing advertising, marketing and personal privacy legislation. For example, recently online programs that have the potential to track personal information and transactional history have come under intense scrutiny in the United States and internationally.[2]

In *In re Sears* in 2009, the FTC took action against Sears, which employed a tracking application with respect to its "SHC Community" and the purchases, emails, instant messages, prescription drug records, and online checking accounts. While no monetary award was imposed, the FTC required that Sears disclose data collection practices on a separate screen prior to the dis-

***Theodore C. Max** is a Member in the Entertainment, Media and Technology and Intellectual Property practice groups in the New York office of Sheppard Mullin Richter & Hampton LLP, where he focuses on counseling clients on intellectual property issues and litigation. He is co-leader of the firm's Fashion and Apparel team. Mr. Max combines his skill and experience as a trial attorney with his knowledge of copyright, trademark and intellectual property law in servicing the firm's diverse clientele.*

Please email the author at tmax@sheppardmullin.com with questions about this article.

play of any privacy policy or terms of use and obtain express consent from the consumer prior to installing the tracking application. The description of the tracking application in the terms of use and privacy statement and inclusion of a "check box" to indicate that the consumer had read and agreed to the terms were found to be deceptive and not found to be sufficient notice under the circumstances.

In December 2010, the FTC released a Preliminary FTC Staff Report entitled "Protecting Consumer Privacy in an Era of Rapid Change; A Proposed Framework for Business and Policymakers." The report suggested a new framework for consumer privacy that would replace mere "notice" requirements with a more meaningful choice for consumers and favors a "do not track" approach with transparency and clear language in the terms and conditions of any privacy policy and terms of use. The report also portends more stringent enforcement of privacy laws by the FTC.

In March 2011, the FTC announced a settlement in an action against Google, which alleged that its launch of the Google Buzz social networking feature in 2010 linking Gmail users with other people on Google's network involved deceptive tactics and violated Google's privacy policy. Significantly, this was the first FTC settlement involving alleged violations of the U.S.-E.U. Safe Harbor Framework privacy requirements. The FTC alleged that some Gmail users who declined enrollment in Google Buzz were enrolled anyway, Gmail users were not sufficiently informed that the people with whom consumers corresponded by email most frequently would be publicly disclosed by the "following/followers" function, and the identities of Gmail users who have turned off the function were not removed from the Google Buzz network. In another first for the FTC, Google agreed, as part of the settlement, to implement a comprehensive privacy program.[3] This settlement demonstrates that the FTC will enforce the European Union Data Protection Directive and suggests that businesses should ensure that any new products, customer marketing tools, or information gathering and tracking efforts are reviewed carefully in advance to make sure the terms of use and privacy policy are updated and in compliance with applicable state, federal and international laws.

On May 12, 2011, the FTC announced a $3 million Consent Decree and Order reflecting a settlement with Playdom, Inc. for allegedly violating the terms of its privacy policy and collecting and disclosing personal information on hundreds of thousands of children without parental consent. The FTC alleged that Playdom's collection of age and email information from children as part of online registration and affording the child-users the ability to post personal information, including names, email addresses and instant message data, without advance parental consent, were a violation of the Children's Online Privacy Protection Act ("COPPA"). The FTC also alleged a violation of the Playdom privacy policy because Playdom stated that children were not able to post profile pages, when in fact they were. This consent decree reflects the largest civil penalty under COPPA. This case underscores the need to make sure that regular due diligence is employed to ensure that the actual operation of a website and way in which personal identification information are collected and used comport with the terms and conditions of the privacy policy and terms of use.

Following the *Pineda v. Williams-Sonoma* decision, the legislative winds of change in privacy law have been blowing a gale. On February 11, 2011, one day after *Pineda v. Williams-Sonoma*, Congressman Bobby L. Rush (D-IL) introduced the BEST PRACTICES ("Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards") Act, which legislation would establish a framework for protecting personal consumer information, H.R. 611. On the same day, Congresswoman Jackie Speier (D-CA) introduced the Do Not Track Me Online Act (H.R. 654), which would require online advertisers and website operators to disclose data collection, use and disclosure activities, including identifying third parties to whom such information would be provided. The "do not track" bill would give the FTC regulatory authority to require that online advertisers or website operators provide consumers with access to stored data and the FTC and state attorneys general are given the power to enforce the Act. The bill tracks the December 2010 FTC Preliminary FTC Staff Report. On April 12, 2011, Senators John Kerry (D-MA) and John McCain (R-AZ) introduced the Commercial Privacy Bill of Rights Act of 2011, which is intended to provide consumers with better control over the collection and use of their personal identification information, whether accessed online or offline. While the bill includes provisions for consumer notice prior to the collection of personal information and opt-in and opt-out consent, depending upon the type of information collected and intended use, it does not include "do not track" provisions. One day later, on April 13, 2011, Congressmen Cliff Stearns (R-FL) and Jim Matheson (D-UT) introduced the Consumer Privacy Protection Act of 2011 (H.R. 1528), which would provide for consumer notice requirements and the ability for consumers to "opt-out" and limit disclosures of personal information to third parties. This bill is very similar to the Commercial Privacy Bill of Rights Act of 2011 introduced by Senators Kerry and McCain. It remains to be seen which if any of these bills becomes law and whether the state and federal privacy laws will change in light of *Pineda v. Williams-Sonoma*.

In order to steer clear of a privacy consumer disaster, you should take care when collecting and utilizing personal information in the marketplace and make sure that your privacy policy and terms of use have been reviewed and prepared by an experienced professional. You also need to make sure to respect the limits and terms of your privacy policy and terms of use and to review and update these regularly to comport with your activities. If marketing or advertising practices or technologies change or new ones are adopted, make sure that these changes or improvements are addressed and covered. For example, using new technological features or improvements such as mobile telephone applications or an automatic Adobe Flash Player may require amendments or additions to the privacy policy and terms of use. If you transfer information from the European Union to the United States, make sure that you have obtained Safe Harbor Certification and that you are in compliance. Be mindful that online membership programs are facing intense scrutiny; you need to make sure that the privacy policy and terms of use comply. Make sure you carefully follow state and federal privacy law developments as these also may require changes in your privacy policy and terms of use.

---

[1] Delaware, Kansas, Maryland, Massachusetts, Nevada, and Rhode Island each have comparable laws to Song-Beverly as well. *See* Delaware: Del. Code Ann. tit. 11, Sec. 914 (2010); Kansas: Kan. Stat. Ann. Sec. 50-669a (2009); Maryland: Md. Code Ann., Com. Law Sec. 13-317 (2009); Massachusetts: Mass. Gen. Law Ann. Ch. 93, Sec. 105 (2009); Nevada: Nev. Rev. Stat. Sec. 597.940 (2008), and Rhode Island: R.I. Gen. Laws Sec. 6-13-16 (2009).

[2] The European Union Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, effective in October 1998, regulates the processing of personal data within the European Union. Safe Harbor principles were negotiated with the United States to govern the transfer of personal data to the United States, and in order to be covered by the safe harbor, entities must be registered with the FTC. On March 16, 2011, the "European Privacy Platform" group of the European Parliament met in Brussels to discuss the structure and content of proposed revisions to the European Union Data Protection Directive. It was suggested that the proposed revision would be based upon four "pillars," including, the right to be forgotten; transparency, "privacy by default" and EU protection regardless of data location.

[3] In October 2010, Google settled a class action that Google Buzz violated federal and California privacy and consumer protection laws based upon its creation of automatic "follower/follow" lists for $8.5 million.