SHEPPARD MULLIN
SHEPPARD MULLIN RICHTER & HAMPTON LLP
ATTORNEYS AT LAW

Fashion & Apparel Law BLOG
Legal Issues Facing the Fashion, Apparel & Beauty Industry

Fashion Apparel Law Blog

June 7, 2011 by Sheppard Mullin

Beauty Is In The Eye Of The Beholder And New Commercial Privacy Legislation Is Before The U.S. Senate

On April 12, 2011, United States Senators John Kerry and John McCain formally proposed the Kerry-McCain Commercial Privacy Bill of Rights Act of 2011 ("CPBRA"). This proposed legislation would apply to all retailers, including those in the fashion, beauty, and apparel industries, that request and record their customers' personal information. If passed in its current form, the CPBRA would preempt similar state laws, would not provide a private right of action upon which an individual claim could be based, and would cap penalties at $3 million. While that is good news in light of the burgeoning class action privacy-related litigation filed against companies by private plaintiffs under state consumer protection laws, compliance with the CPBRA could potentially be onerous because the CPBRA replaces industry self-regulation with government regulation.

Below are some of the highlights of the proposed CPBRA, in its current form:

- The CPBRA will apply to "covered information", which includes: "personally identifiable information" ("PII"), "unique identifier information", and any information that is collected, used, or stored in connection with the two former categories of information in a manner that may reasonably be used to identify a specific individual. [CPBRA Sect. 3(3)(A)].
- "Covered information" does not include PII from public records not merged with "covered information" gathered elsewhere, PII obtained from a forum where the information was voluntarily shared and is widely and publicly available (think Facebook), PII reported in the public media, or PII dedicated to contacting an individual at work.
- PII includes: names, postal addresses, email addresses, telephone numbers, Social Security Numbers, credit card account numbers, "unique identifier information" (as defined below), biometric data (like a fingerprint), or any of the foregoing used, transferred or stored with a birth date, birth certificate number, birth place, "unique identifier information", precise geographic location (with GPS specificity, but not including an IP address), information regarding use of voice services, and "any other information concerning an individual that may

reasonably be used by the party using, collecting, or storing that information to identify that individual." [CPBRA Sect. 3(5)].

- "Unique identifier information" includes items such as a customer number held in a cookie, a user ID, or a serial number. [CPBRA Sect. 3(9)].
- "Unauthorized use" means use of "covered information" for any purpose not authorized by the person to whom such information relates. [CPBRA Sect. 3(8)(A)]. There are several notable exceptions, for example: to process a transaction or deliver a service requested by the individual, to prevent or detect fraud, to investigate a crime, to advertise to an individual within the context of the business's website if the individual affirmatively requested it, and to improve the transaction or service, among others. [CPBRA Sect. 3(8)(B)]. However, the exceptions only apply if the use is reasonable and consistent with the practices and purposes described in the notice given to the individual in accordance with CPBRA, described below. [CPBRA Sect. 3(8)(C)].
- Companies should only collect data they need to complete transactions or to provide services. [CPBRA Sect. 301]. Companies can collect and use information for research and development to improve the transaction or service, provided they retain that information for only a reasonable period of time.
- Companies must implement privacy protection procedures [CPBRA Sect. 101-103], provide clear, concise and timely notice regarding collection, use, transfer, and storage of covered information and the purpose of those practices [CPBRA Sect. 201], set up an opt-out consent mechanism regarding unauthorized use and use by third-parties for advertising or marketing, set up an opt-in mechanism for use of "sensitive" PII (with certain exceptions), provide individuals with access and ability to correct their information, and to give individuals the opportunity to revoke consent to use such information if the company undergoes a change in corporate structure or goes bankrupt. [CPBRA Sect. 202].
- The CPBRA will allow the Federal Trade Commission ("FTC") and Department of Commerce to oversee voluntary "Safe Harbor" programs that if implemented, would allow companies to shield themselves from liability under the CPBRA. [*See* CPBRA Sect. 202(c); Sect. 501].
- Only the government (state Attorney Generals or the FTC) can enforce the law, and can only enforce it against companies that collect information concerning more than 5,000 people during a 12-month period. [CPBRA Sect. 401 - 403]. If the FTC institutes an action, no Attorney General is allowed to bring an action based on the same violation. The civil penalty can be up to $16,500 per day or per individual violation, not to exceed $3 Million. [CPBRA Sect. 404]. The CPBRA expressly bars a private right of action. [*See* CPBRA Sects. 405(b), 406 ("This Act may not be construed to provide any private right of action")].
- CPBRA Section 405 expressly states that the CPBRA will supersede any state laws that "relate to the collection, use, or disclosure of covered information addressed in this Act or personally identifiable information or personal identification information addressed in provisions of the law of a State." [*See* CPBRA Sects. 405].

In conclusion, under the proposed CPBRA, retailers can still request and use the requested information, but they will need to very clearly inform consumers what they intend to do with the information at the time that it is requested in order to avoid a violation of the CPBRA.

The full text of the proposed bill can be found here.