Publications

"Adapting Data Security To Cross-Channel Marketing"

Related Services

Intellectual Property

AUTHORED ARTICLE | 3.10.2011

Benita A. Kahn, a partner in the firm's Columbus office, authored the article "Adapting Data Security to Cross-Channel Marketing." The article was originally published in the March 10, 2011 edition of *IP Law360*.

Adapting Data Security to Cross-Channel Marketing

March 9, 2011 - Ten years ago, most consumers were clipping coupons from the Sunday newspaper, hopping in their cars, and driving to the store. Today in the U.S., nearly three-fourths of adults use the Internet, and more than half are connecting wirelessly on laptops, smartphones and other high-tech devices. All of this connectivity and mobility is changing the focus of multichannel retailers, who are creating new ways to make use of these mobile channels.

Customers are researching and shopping using a combination of channels and in ways that were not predicted a few short years ago. It's now commonplace for retailers to serve coupons to customers through e-mail and text messaging. And by making use of smartphone applications, in-store Wi-Fi, and geolocation technology, retailers are creating instant, in-store cross-channel experiences for technologically engaged consumers.

Meeting the goals of cross channel strategies requires data, which is used to respond more quickly to changes in demand patterns, reduce out-of-stocks, match product offerings to the right customer, and improve customer service. To accomplish this, however, retailers must aggregate and integrate data, which increases both risk and complexity when it comes to securing customer information.

The numerous data breaches over the last several years — Heartland Payment Systems and T.J. Maxx are just two examples — have demonstrated the risk and economic cost associated with collecting greater amounts of electronic data. A recent study put the average organizational cost for a data breach at $6.75 million in 2009. Last year, Heartland Payment Systems agreed to pay over $100 million to resolve all but the class action liability resulting from its data breach.

The complexity results from both state and federal laws. For example, federal Gramm-Leach-Bliley concerns are raised when customer information is obtained by a financial institution such as the issuer of a retailer's private label credit card. Retailers must designate that information in a database, given that its use is limited to the manner in which the financial institution can use it.

At the state level, Massachusetts has imposed detailed security requirements for storing and transmitting data that require, for example, implementation of a comprehensive information security program covering access controls, encryption, up-to-date software and patching, firewalls, system monitoring, and training. Washington, Minnesota, and Nevada have implemented data security requirements linked to an industry-imposed standard — the Payment Card Industry Data Security Standards — resulting in a need to continually update compliance measures.

Another important consideration in cross-channel marketing is the management of third-party vendors. Retailers need to conduct due diligence to monitor and contractually control those vendors. These third-party vendors run the gamut, from database management to smartphone application and text message marketing campaign providers. Making use of these new means of communicating with customers is essential, but do retailers really know what information is being collected behind the scenes by those third-party applications?

Recent class action litigation filed in California and articles about behavioral advertising would suggest that some companies do not. These new tools make due diligence and contractual obligations more important. It is critical for retailers to know exactly what data the business needs and how it will be collected and used prior to entering into agreements with vendors.

The Federal Trade Commission has shown it will impose obligations on the retailer for failures of its vendors. Imposing contractual obligations without further due diligence may not be enough.

When planning cross-channel marketing strategies, it's critical for retailers to involve a privacy professional. This person must fully understand how the technology will work — without this knowledge, it is not possible to accurately disclose data uses at the time of collection. And it is far too difficult and costly to reverse the process later to implement these privacy protections.

Although the issue is far more complex, there are four basic considerations in designing a data management plan within any organization:

1) Privacy by Design: Growing the brand through cross-channel strategies requires that privacy considerations have an important seat at the table from the outset. Retailers must build privacy into the data development life cycle from the earliest planning stages. Retailers will need a privacy professional to act as a liaison between marketing, finance, compliance and technology.

2) Accountability: Someone in the organization must have a 360-degree view across all channels and all brands. This includes understanding the technology in play, its vendors, and administering the needed controls.

3) Data Minimization: Collect only the information that's absolutely necessary. Reduce the number of places the data is stored. Permanently delete it when it's no longer needed. Retailers need to strike a balance between enhancing economic incentives for customers and reducing risk of data breaches.

4) Transparency: Retailers need to establish policies for collecting and using data. Transparency means different things to different people. From a privacy professional's view, that means having visible, clear and conspicuous policies regarding data collection and use. But to a marketing professional that may mean making the policy nonintrusive to the customer. Someone within the organization must reconcile these differences by applying the risk/reward balancing to the conversation.

The "simple" job of privacy compliance has become decidedly more complex. Not only is there a continuing need to understand and comply with privacy obligations, but it also is necessary to build a stronger relationship between marketing and privacy. Reaching the goals needed for a successful cross-channel strategy — data security, vendor management, oversight and building customer trust — requires an enterprisewide focus and a commitment to privacy polices that are driven from the top.