Wrapping Paper Update: Top 12 Ways Retailers Can Address Privacy Issues This Holiday Season

THIS SERIES OF UPDATES contains information regarding issues and trends facing the retail industry during the holiday season.

In this installment of "Perkins Coie Wrapping Papers," we take inspiration from "The Twelve Days of Christmas" to provide an overview of the top twelve privacy and data security issues retailers should consider as the year comes to a close. Although we cannot provide gold rings or even a single drummer drumming, we can offer you practical pointers that, if implemented, will pay dividends throughout 2015 and beyond.

1. **Review data security practices.** The 2013 holiday season brought with it unfortunate headlines for Target, and the bad news kept coming for major retailers throughout 2014. In addition to Target, Neiman Marcus, Michaels and Home Depot all suffered data security breaches, resulting in the exposure of tens of millions of customers' names and credit card numbers. During this holiday season, keep the focus where it should be—on sales, not data breaches. Review your data security program and practices to make sure they are keeping up with the rising standard of care. Where you can, learn from the mistakes of others.

2. **Think about chip and pin and encryption standards.** In a report that is garnering a lot of attention, the California Attorney General's Office recently recommended that all retailers "move promptly" to update their point-of-sale terminals so that they are chip-enabled, as well as implement end-to-end encryption. Consider what the California AG's report means for your company.

3. **Make sure you're ready.** In the event something does go wrong, be ready. Have a complete incident response plan in place. Know who is responsible for each task, and practice implementing your plan so that the first time you go through the exercise it is not after you've already suffered a breach.

4. **Make sure you're covered.** Insurance can play an important role for retailers in minimizing the financial impact of a breach, including legal expenses incurred as a result of the breach, third-party lawsuits, business interruption losses, damage to online systems or data losses, government investigations, and/or fines, costs associated with investigating a breach, costs of complying with consumer notification laws and providing credit monitoring services, breach of contract and negligence claims, and loss of intellectual property. Gather all potentially applicable insurance policies, evaluate the potential for claims, and make sure you're adequately covered for the costs you are likely to incur in the event of a security breach. Don't forget to review your vendor contracts for insurance requirements. Find out more here.

5. **Make sure your privacy disclosures are up to snuff.** It has long been the law that companies (at least those collecting personal information from California residents) were required to disclose their data collection, use and disclosure practices. But the California Online Privacy Protection Act of 2003 (CalOPPA) was amended in 2013 to impose additional requirements on retailers and other "first parties,"

who now must disclose whether they allow "third parties" to track users on their websites or online services, including mobile apps. The California AG's office recently built upon these amendments, issuing particular recommendations for presenting privacy disclosures. These include ensuring that they are conspicuously available, use straightforward language and include a separate section to cover online tracking.

6. **Put your tracking disclosures in the right place.** The self-regulatory rules issued by the Digital Advertising Alliance (DAA) and enforced by the Better Business Bureau (BBB) require that websites that allow users to be "tracked" by third parties—even if only to enable simple retargeting—provide notice outside of the privacy policy, such as through a link entitled "Interest Based Ads." The BBB recently brought enforcement actions against five companies, including one retailer, for the failure to provide this "enhanced" notice. If your customers see ads on other sites or apps that are informed by their visits to your company's site or app, make sure they are provided notice of that collection outside of your company's privacy policy.

7. **Think about how you are collecting and using personal information in-store for electronic receipts or loyalty programs.** Retailers have seen increased litigation under California's Song-Beverly Act in recent years. Originally enacted (along with other state point-of-sale laws) to protect consumers from being required to provide their names as part of paper-based credit card transactions, creative plaintiffs' attorneys are now using the laws to bring claims with respect to retailers' practices of requesting personal information as part of loyalty card programs and to issue electronic receipts. Consider how and where customers are being asked to provide personal information in your stores, and separate requests for personal information from underlying transactions to the extent feasible.

8. **If you are tracking customers in your stores via their mobile devices, make sure you understand the rules of the road.** It has been a busy year for in-store tracking issues, with an FTC workshop dedicated to the issue, a voluntary code of conduct developed, and Apple's increasing rollout of its iBeacon technology. In-store tracking presents countless new opportunities to communicate with users and to understand their shopping patterns, but the sensitivity of location data argues for proceeding with caution.

9. **Don't forget the TCPA.** Despite recent favorable rulings from courts with respect to the definition of autodialer and from the FCC with respect to consent, the Telephone Consumer Protection Act of 1991 (TCPA) remains among the most litigation-rich areas in privacy. And, despite numerous requests to do so, the FCC has failed to provide the clarity that businesses seek regarding how the new TCPA rules apply to common methods retailers use to communicate with their customers. If your company is texting its customers or calling their mobile devices, make sure that its means of providing notice and obtaining consent are consistent with the new TCPA rules.

10. **Make sure your Safe Harbor certification is up-to-date.** If your privacy policy indicates that your company participates in the Safe Harbor, but your certification with the Department of Commerce has lapsed, your company is subject to an enforcement action under section 5 of the Unfair and Deceptive Trade Practices Act, as many companies learned in 2014. Regardless of how your company transfers data from Europe to the United States, make sure that your international data transfer practices will withstand scrutiny by reviewing, documenting, and where necessary, enhancing the safeguards you have in place, and by ensuring that your practices comply with data transfer laws in the countries where you do business.

11. **Evaluate your relationships with vendors and ad technology companies.** Make sure your data is protected and not available for other companies' independent use. Review your relationships with ad technology companies and other vendors to ensure that their collection and use of data from your sites, services or about your customers are consistent with the representations you've made to your customers. Ensure that you have an adequate process for conducting diligence on, and negotiating appropriate contractual protections with, any companies that collect data on your websites or mobile apps, or with which you share your customers' personal information.

12. **Look at ages.** You could be ensnared by the Children's Online Privacy Protection Act (COPPA) even if you don't market to kids or host any content that is appealing to children. If your company asks customers to enter their ages on any websites, mobile apps or other online services, make sure that users who indicate that they are under 13 years of age are not able to submit personal information unless their parents have provided valid parental consent for that collection.

CONTRIBUTING AUTHORS:

MEREDITH B. HALAMA

+202.654.6303

MIRIAM FARHI

+206.359.8195

THOMAS C. BELL

+ 206.359.8845