CHAPTER IV

PRIVACY CONSIDERATIONS FOR
PROMOTIONAL MARKETING IN THE DIGITAL AGE

Big data and the interactivity of digital promotional marketing are powerful brand activation and consumer relations management tools for companies, but data protection laws and consumer expectations have evolved in recent years resulting in new and heightened compliance and risk management issues that need to be addressed when executing campaigns. In today’s competitive marketplace, brands are relying heavily on innovative and edgy digital marketing campaigns to promote their products and services that often include the submission of user-generated content, viral marketing, the brand’s web site, a mobile application, and other social media and social networking elements. However, the tech-savvy marketing professionals that are entrusted to do implement these programs are often unaware of the complex legal overlay of the digital world and the potential significant financial repercussions for their company’s failure to comply with applicable laws. These include not only traditional advertising and intellectual property law issues, but also the data privacy and security implications of the campaign. Failure to understand and follow applicable legal requirements can potentially lead to expensive litigation or government enforcement actions and negative publicity that can harm a brand. Further, the advancement of technology allows for messaging to be behaviorally targeted, which may not be well received and deemed creepy by consumers, even if such profiling and targeting is currently legal in the United States (Europe and other territories have different regulatory constraints). The following “top 10” data protection issues that companies should be addressing before launching a digital promotional marketing campaign that collects data from consumers are intended to help promotion professionals in identifying and mitigating data privacy and security risks.

1. **Posting an appropriate privacy policy.** Not posting a privacy policy on a web site, mobile application, Facebook application or any other online service that collects personally identifiable information (e.g., first and last name, address, email address, telephone number, etc.) from a consumer is not only contrary to Federal Trade Commission (“FTC”) guidance, but is also a violation of California’s Online Privacy Protection Act of 2003 (“CalOPPA”). Companies that collect personally identifiable information from California residents through any online service for commercial purposes, even if they are not themselves in California, must conspicuously post a privacy policy that informs individuals of this collection, including:

   - identifying the categories of personally identifiable information collected and third parties with whom such information may be shared;
   - describing any process (if the site has one) for reviewing and requesting changes to collected information;
   - describing the process by which the operator notifies users regarding material changes to the policy; and
   - identifying the effective date of the policy.

Further, recent amendments to CalOPPA, effective January 1, 2014, require the privacy policy to additionally include the following:
disclose how the operator responds to Web browser “do not track” signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information; and

disclose whether third parties may collect personally identifiable information about an individual consumer’s online activities over time and across different web sites when a consumer uses the operator’s site or service.

CalOPPA requires privacy policies to accurately describe data practices and provides specifics as to how its requirement of “conspicuous posting” may be met, including with regard to placement, various types of font treatment and word content. In 2013, the California Attorney General (“AG”) sent notices to hundreds of companies, many located outside of the state, that their sites or mobile apps did not include a privacy policy, as required by CalOPPA, and where the company failed to comply within 30 days, filed suit under California’s Unfair Business Practices Act. While CalOPPA requires such a notice and opportunity to cure for failing to post a privacy policy, no notice and cure opportunity is necessary for a state or local prosecutor, or for a consumer, to bring a CalOPPA-based claim for false or misleading statements in a privacy policy. In spring of 2014, the California AG released best practices guidelines for explaining how the AG believes companies should provide consumer privacy disclosures, including when viewed via the small screen on a mobile device, and regarding the new required disclosures regarding tracking of consumers across time and locations, the foundation of interest-based or behavioral advertising. This follows earlier guidance regarding privacy policies and disclosures for mobile apps. See “Making Your Privacy Practices Public” (CA AG, May 2014) and also “Privacy on the Go – Recommendations for the Mobile Ecosystem” (CA AG, January 2013). Beyond California, the FTC has long used its deception authority to prosecute inaccurate or misleading statements in privacy policies as false advertising claims. The FTC has also issued reports and guidance that outline best practices for privacy transparency and choice, which are helpful guides for drafting privacy policies and notices. The Obama Administration has also been quite vocal about the need for industry to be more transparent and offer consumers more choice regarding data practices. See. e.g., “Big Data: Seizing Opportunities, Preserving Values” (Executive Office of the President, May 2014). In addition, certain regulated industries have specific privacy disclosure obligations, and online services directed to children have special regulatory requirements outlined below.

Accordingly, it is essential that companies assess their data collection, use, sharing, processing, storage and security practices, and ensure that their privacy policies completely and accurately explain all material practices and comply with applicable laws. Most companies will also need to meet the more stringent California requirements.

2. Working with third parties. In addition to the third party tracking disclosure requirements of the CalOPPA amendment noted above, it is important to consider what information third parties may be directly collecting on a company’s sites and what information a company may be sharing with third parties such as co-promotional partners. With regard to third parties a brand is working with on a campaign, it should consider whether it has addressed data ownership and control issues, properly disclosed information sharing practices and imposed legally required security obligations where appropriate. When addressing the sharing of information with third parties, beware that third parties can, under many laws, include affiliate companies. Further, it may simply create an inaccurate impression if a brand states in its privacy policy, or at an information collection point, that it does not share information collected with any third parties when the data is shared with corporate affiliates. Companies should particularly take care to assess their obligations under California Civil Code Section 1798.83 (also known as California’s “Shine the Light” law), which provides California residents with certain rights with respect to sharing certain consumer information (broadly defined and more inclusive than typical definitions of personal information), collected on or offline, with third parties (including affiliates) for the
third parties’ direct marketing purposes. Failure to comply with that scheme has spawned a number of class action lawsuits.

3. **Disclosing tracking technologies.** Undisclosed passive tracking is the stuff that media headlines are made of, and depending upon the scope and manner of the information collected, may now be required to be disclosed under the recent CalOPPA amendment discussed above. Cookies and other passive tracking practices are receiving increasing scrutiny domestically and globally (particularly in the EU) from both the press and lawmakers. Even where passively tracked information is not linked to what we in the US traditionally consider personally identifiable information, it can still raise privacy notice and consent issues. Also, most every site now uses Google Analytics and Google requires certain disclosures to be included in its clients’ privacy policies, as do other analytics vendors. Many other vendors a site or app publisher may engage to help operate the service, including those that are involved in ad serving discussed further below, may now similarly contractually require specific notices and opt-outs be followed. Third parties (government, media, consumer organizations, and site visitors) can use various browser add-ons (see [http://www.ghostery.com](http://www.ghostery.com)) as a means to reveal whether a site’s representations about passive tracking match up with actual practice. Misrepresentations are actionable as deceptive advertising claims. Privacy policies should address passive means of collecting information on or via a site or application. As part of a data practices audit and assessment, it is essential that IT and marketing staff be consulted to ensure that cookies, pixel tags, browser fingerprinting, web beacons and other tracking technologies are understood and that appropriate disclosures and consumer choices are provided.

4. **Behaviorally targeted campaigns.** Online behavioral advertising (“OBA”) is the term used to describe the process of companies tracking consumers’ online activities to profile and target them for interest-based advertising. Many companies advertise using OBA, but may not be directly involved in collecting and using the OBA data because they employ vendors and ad servers to do this. However, an advertiser, even if engaging in OBA on a non-affiliated site (e.g., retargeting a user who has left the brand’s site with an ad on a subsequent third party site), is subject to self-regulatory rules and best practices guidance promulgated by the FTC. Before engaging in any OBA, companies (both advertisers and publishers) should review the behavioral advertising self-regulatory guidance of Digital Advertising Alliance (“DAA”). See [www.aboutads.info](http://www.aboutads.info). The DAA’s guidance provides a self-regulatory framework for advertisers, agencies, publishers and technology companies for engaging in OBA. The DAA provides an iconic form of notice that alerts consumers to OBA and provides a method of opt-out. While the DAA licenses the icon itself for $5,000 a year, it has three approved service providers that provide compliance and analytics services, which can provide the license as part of its services. To identify and minimize risks, companies should take steps to: (i) understand what tracking is taking place through their marketing campaigns, as well as their web sites and applications; (ii) include the requisite insurance and indemnity provisions in their agreements with vendors assisting the company with OBA; and (iii) include appropriate disclosures in the company’s privacy policy, on its home page and on OBA ads to address what OBA activities may be occurring.

5. **Incorporating “privacy by design” in your campaign development process.** In March 2012, the FTC released a set of recommendations for businesses regarding the collection and use of consumer personal information. See “Protecting Consumer Privacy in an Era of Rapid Change – Recommendations for Businesses and Policymakers” (FTC, 2012). A central tenet of the FTC’s recommended privacy framework is the notion of “privacy by design” or “PbD”, which calls for embedding privacy and data security considerations from the outset into the design development of information technologies and practices and minimizing the collection and use of data to what is necessary under the circumstances. The goal of privacy by design is to minimize the privacy impact on consumers and maximize their informed choice. Companies that can “bake in” privacy protections for a new campaign in the conceptualization phase are more likely to avoid having to try to make changes right before launch or post launch when doing so may cause delay and additional cost. In order to effectively
implement PbD, it is essential that a knowledgeable privacy professional evaluate the planned data practices to identify issues. For instance, the defendants in the recent flood of lawsuits relating to collection of zip codes in connection with credit card purchases, which violates California, Massachusetts and other state laws, could have avoided those claims had they involved compliance counsel in the development of the purchase flows.

**6. Management of consumer communications.** The ability to communicate with consumers is increasingly subject to different legal requirements. Under the CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Materials Act of 2003), email marketing to consumers is largely an “opt out” regime in the U.S. (other countries are opt-in). Thus, companies are required to provide notice of how to exercise the ability to opt-out from receiving future email marketing communication, as part of that commercial message, and to maintain and scrub against a list of those that have opted out. Companies should also be mindful of special rules associated with marketing communications sent via mobile. The Telephone Consumer Protection Act ("TCPA"), telecom carrier rules and the Mobile Marketing Association Guidelines govern the sending of text messages and emails to mobile domain addresses. Companies must satisfy certain notice and express advanced written consent requirements before sending a commercial text message to a mobile device or mobile domain address, a list of which is available on the Federal Communication Commission’s web site. Additional rules govern telemarketing. TCPA violations have spawned many class actions lawsuits resulting in tens of millions of dollars in settlements paid by advertisers that failed to fully comply, and companies too often discover that the vendors they trusted to run campaigns failed to comply with applicable laws. It is not uncommon for the vendor agreements to fail to provide the company with recourse, and for vendors to lack the ability to stand behind an indemnity obligation if the agreement does include one. To avoid problems with future marketing campaigns, companies must carefully consider when it is appropriate to take an opt-in v. opt-out approach to the sending of future marketing communications and to not trust that vendors will meet compliance obligations. It is also important to evaluate whether consent language is drafted appropriately to cover the additional communications that the company will send now and in the future, including who will send the communications (company only, affiliates, other third parties), how they will be sent (do not assume that “send me updates” means “call me at home during dinner”), and types of communications (about just one product, anything related to the company, anything related to a particular topic of interest, etc.). Recording of customer service calls is also regulated by various state laws, the violation of which has generated much recent litigation. Accordingly, companies should implement appropriate consumer communications policies, and ensure that promotional campaigns are compliant.

**7. Adopting a formal, written data security compliance program.** Despite a sectorial approach to privacy and a state patchwork approach to data security regulation in the U.S., a growing number of companies are now subject to some form of legal obligation to adopt “reasonable” data security measures. Among the laws mandating some form of “reasonable security” are: (i) the Health Insurance Portability and Accountability Act (“HIPAA”) security regulations applicable to the health care industry; (ii) the Gramm-Leach-Bliley Act (“GLB Act”) “safeguards” regulations for financial institutions; (iii) state insurance law analogs to the GLB Act Safeguards Rule applicable to insurance companies; and (iv) and state laws governing businesses that maintain certain types of personal information of residents (e.g., Massachusetts, Nevada and California). Even if your organization happens to operate outside the reach of these particular data security laws, there is a growing consensus that implementation of a formal, written security compliance program is a best practice. In Massachusetts, such a “Written Information Security Program” or “WISP” is required if a company has certain personal information of Massachusetts residents. Most states also have data breach response and reporting laws, which require prompt action following a suspected compromise. Further, the FTC has been very active in exercising its unfairness authority to prosecute companies that have experienced data security breaches under the theory that failure to take reasonable measure to protect data, even data that is not sensitive (e.g., Twitter account credentials) fits within its unfairness jurisdiction, a proposition that
has been challenged, but so far unsuccessfully. For helpful guidance, see “Cybersecurity in the Golden State – How California Businesses Can Protect Against and Respond to Malware, Data Breaches and Other Cyberincidents” (CA AG, 2014).

8. Marketing to children. Children’s privacy issues are lurking in many promotional marketing campaigns, whether or not the campaign is directed to children. On July 1, 2013, the FTC updated the Children’s Online Privacy Protection Act (“COPPA”), which requires a company to obtain verified parental consent (“VPC”), in a particular manner, prior to collecting personal information from a child under the age of thirteen (“child”) online or via mobile apps with limited exceptions. The updated COPPA regulations greatly expand what kind of data requires VPC before being collected from a child, and now is defined to include persistent identifiers (i.e., an identifier used to recognize a user, browser or device over time and across sites and services such as IP address), as well as geolocation data and videos and photos of children from children. Sites and apps directed to children must assume all users are children and undertake VPC clearance before collecting personal information other than pursuant to a VPC exception. However, COPPA now creates a new category of so-called mixed use sites and apps that may in part be directed to children, but not primarily so. These sites and services may now age screen users in a neutral manner, and treat them differently based on self-reported age. This includes ensuring that behavioral advertising is not served to children, that social media plug-ins and tools where users can submit publically available content are not made available to them, and that analytics providers and other vendors do not use their identifiers or other personal information except pursuant to certain narrow exceptions. Mixed use sites cannot block children under 13 completely, but must offer them COPPA-compliant services. Even services not directed to children, so-called general audience services, can have COPPA obligations. The FTC has made it clear that once an operator has notice that a user is a child under 13, it must immediately take action to prevent an ongoing violation of COPPA.

9. Be sure to address collection of location-based information from consumers or otherwise publicly sharing a consumer’s location. Location-based services (“LBS”) have one thing in common regardless of the underlying technology – they rely on, use or incorporate the location of a device to provide or enhance a service. For instance, a consumer may be able to “check-in” at a location with their current location displayed to others using the LBS. Retailers are starting to employ in-store “iBeacons” that interact with consumer’s mobile devices. Or, user location can be tracked so that geographically relevant content or ads can be sent to them. Another popular location-based service is an application that enables users to locate other users who are near to them. While such functionality can be valued by users, it is potentially intrusive and companies should require notices and consents be given and obtained before enabling such functionality on apps or other services. General caution should also be exercised. The San Francisco District Attorney recently sued a mobile app publisher that made teenager’s location available to each other as an unfair business practice, alleging that it put minors at risk of becoming victims of sexual predators. A promotional marketing campaign that incorporates LBS technology should give a user appropriate notice about how location information will be collected, used, shared and disclosed and consider age restrictions. As noted above, LBS data is personal information under COPPA. User tracking also requires notice and consent under EU data protection laws, and U.S. best practices are to give notice and a means to disable tracking (even if by uninstalling the entire app or service). Further, U.S. mobile carriers (e.g., AT&T) and platforms (e.g., Apple) have certain notice and consent requirements. Generally, there should be a notice and opt-in permission to geolocation tracking that is displayed on a single screen with links to a more detailed privacy policy before LBS functionality is enabled. It will also be necessary to post a privacy policy on the app or service (which should be available at the point of registration, if applicable, and on an information page) that specifically addresses the collection of location-based or other sensitive data. The privacy policy should inform users how they may terminate the collection of location-based information (which may be by uninstalling the software or by exercising privacy options), and inform the user how to exercise any available privacy options.
10. **Videos in a campaign can also be a privacy issue.** The Video Privacy Protection Act ("VPPA") prohibits disclosure of information which identifies a person as having requested or obtained specific video materials or services, without having first obtained consent from the user. California, Connecticut, Delaware, Iowa, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, New York, New Hampshire, Rhode Island and Tennessee also have video privacy laws, some of which differ materially from the VPPA. Many companies wish to share video content consumption information with third parties and/or allow users to share what videos they watched on the company’s site with others via a social networking site like Facebook. Under a broad reading of these laws, in order for a company to be able to share video viewing info with a third party social media site, the company first needs to obtain user consent to do so. Video service providers can obtain advance consent electronically over the Internet from a user for sharing of the video information for a maximum period of 2 years under the VPPA as it has been recently amended. The form of consent requires a separate independent consent be obtained from the user (outside of a consent obtained in a Terms of Use/Privacy Policy). Thus, companies wishing to share video content consumption information may need to post a separate “Video Privacy Policy” on their site that complies with the requirements of the VPPA and obtain consent to this document from users that is separate and apart from the consent obtained to a company’s typical Privacy Policy and Terms of Use before sharing a user’s video consumption data. This type of advanced consent, however, is not available in some instances under some state laws, and other state laws require notices and consents to include specific language.

**Conclusion**

The last decade has seen technology change the ways companies can target consumers in ways hardly imagined. The results can be beneficial to both brands and consumers, but consumers also face real risks and burdens as a result. Companies need to weigh the benefits and risks of proposed advertising and sales schemes and campaigns and be aware of the changing regulatory landscape that is evolving as technology advances. Further, the most important asset a brand has is its consumer goodwill. New marketing and sales approaches that consumers appreciate build goodwill, but those that are perceived as misleading, unfair or too intrusive, can harm the brand. The role of legal counsel is to help promotional marketers identify and evaluate the risks of novel campaigns and techniques from conceptualization through execution so that they may minimize risk while still achieving a compelling campaign that delivers the desired return on investment.