Bloomberg BNA

Privacy and Security Law Report®

Top 10 Privacy Considerations for Digital Marketing Campaigns

BY JESSE BRODY

In today's competitive marketplace, companies 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 website, a mobile application and other social media and social networking elements. However, the tech-savvy marketing professionals that are entrusted to 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 privacy laws. Failure to understand and follow these 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 might be deemed creepy by consumers, even if such profiling and targeting is currently legal in the U.S. In working closely with our clients from concept through execution of a digital marketing campaign, these are the ''top 10'' privacy questions that marketers and their lawyers should be asking before launching a digital marketing campaign that collects information from consumers.

Jesse Brody is a partner in the Advertising, Marketing & Media practice at Manatt, Phelps & Phillips LLP in the Los Angeles office. His practice focuses on legal and regulatory issues impacting the areas of entertainment, technology, advertising and privacy. Brody is accredited by the International Association of Privacy Professionals as a Certified Information Privacy Professional. He can be reached at jbrody@manatt.com.

1. Have you posted an appropriate privacy policy? Not posting a privacy policy on a website, mobile application, Facebook application or any other online service that collects personally identifiable information (*e.g.*, first and last name, address, e-mail address, etc.) from a consumer not only violates Federal Trade Commission (FTC) guidance,[1] 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.[2]

Further, recent amendments to CalOPPA, which became effective Jan. 1, 2014, require the privacy policy to additionally inform individuals of the following site practices:

- disclosing 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
- disclosing whether third parties may collect personally identifiable information about an individual consumer's online activities over time and

[1] *See* FTC, *Protecting Consumer Privacy in an Era of Rapid Change* (Mar. 2012), *available at* http://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers (11 PVLR 590, 4/2/12).

[2] Cal. Bus. & Prof. §§ 22575(b)(1)–(b)(4).

 ISSN 1538-3423

across different websites when a consumer uses the operator's site or service.[3]

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. The FTC has long used its deception authority to prosecute inaccurate or misleading statements in privacy policies as false advertising claims. Accordingly, prior to engaging in a digital marketing campaign that collects information from consumers, it is essential that companies audit 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.

2. Are you using third parties to collect information, or are you sharing information you collect 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 your sites and what information you may be sharing with third parties, such as co-promotional partners. With third parties you are working with on a campaign, you should consider whether you have addressed data ownership and control issues, properly disclosed information sharing practices and imposed legally required security obligations where necessary. When addressing the sharing of information with third parties, don't forget that third parties can under many laws include your affiliate companies. Although it may feel to you like one big, happy family when you share information among affiliates, you may be creating the wrong impression if you say in your privacy policy, or at an information collection point, that you do not share information collected with any third parties. Companies should particularly take care to assess their obligations under Calif. Civ. Code § 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, collected online or offline, with third parties (including affiliates) for the third parties' direct marketing purposes. Failure to comply with that statutory scheme has spawned a number of class-action lawsuits.[4]

3. Does your campaign incorporate cookies, pixel tags, browser fingerprinting, Web beacons or other tracking technologies, and do you disclose these practices? Undisclosed passive tracking is the stuff that media headlines are made of, and depending upon the scope 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 from both the press and lawmakers. Even where passively tracked information is not linked to what we in the U.S. traditionally consider personally identifiable information, it can still raise privacy notice and consent issues. Also, most every site now uses Google Analytics, and Google Inc. requires certain disclosures be included in your privacy policy. Many other vendors you may engage to help you operate your site or service may now similarly contractually require specific notices and opt-outs be followed by a company. Third parties (government, media, consumer organizations and site visitors) can use various browser add-ons[5] 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. Revise your privacy policy to thoroughly address passive means of collecting information on your site or application. As part of a data practices audit, talk with your information technology and marketing staff to ensure that you cover all of your bases and get an accurate picture of what is going on at your site and in connection with your digital campaigns — a step that many companies overlook to their peril.

4. Has ''privacy by design'' been incorporated 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.[6] A central tenet of this Privacy Framework is the notion of ''privacy by design,'' which is the philosophy of embedding privacy and data security considerations from the outset into the design development of information technologies 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 privacy by design, it is essential that a knowledgeable privacy professional evaluate the planned data practices to identify issues.

5. Do you take an opt-in, opt-out or give-up approach to future marketing communications? In their zeal to promote products and services, some companies may be surprised to find out that they can't send out marketing materials unless they have the proper permission to do so. The ability to communicate with consumers is increasingly subject to different legal requirements. Under the CAN-SPAM Act of 2003,[7] e-mail marketing to consumers is largely an opt-out regime in the U.S. (other countries are opt-in). Thus, companies are required to offer customers the ability to opt out from receiving future e-mail marketing communications in any marketing e-mail sent.

Companies should also be mindful of special rules associated with marketing communications sent to mobile devices. The Telephone Consumer Protection Act (TCPA)[8] and the Mobile Marketing Association Guide-

[3] *Id.* §§ 22575(b)(5) and (b)(6) (12 PVLR 1720, 10/7/13).

[4] For examples of some recent cases addressing California's Shine the Light Law, *see Boorstein v. CBS Interactive, Inc.*, 165 Cal. Rptr. 3d 669 (2013) (13 PVLR 43, 1/6/14); *Miller v. Hearst Commc'ns., Inc.*, No. 12-57231, 2014 BL 42230 (9th Cir. Feb. 18, 2014) (13 PVLR 384, 3/3/14); *Baxter v. Rodale, Inc.*, No. 12-56925, 2014 BL 48070 (9th Cir. Feb. 21, 2014).

[5] *See* http://www.ghostery.com (last visited June 5, 2014).

[6] *See Protecting Consumer Privacy*, *supra* note 1.

[7] 15 U.S.C. § 7704.

[8] 47 U.S.C. § 227.

  PVLR ISSN 1538-3423

lines[9] govern the sending of text messages and e-mails to mobile domain addresses. Companies must satisfy notice and express advanced written consent requirements before sending a commercial text message to a mobile device. Additional rules govern telemarketing. TCPA violations have spawned many class-action lawsuits resulting in tens of millions of dollars in settlements paid by advertisers that failed to fully comply.

To avoid problems with future marketing campaigns, companies must carefully consider when it is appropriate to take an opt-in versus an opt-out approach to the sending of future marketing communications. It is important to evaluate whether 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 have generated much recent litigation. Accordingly, companies should consider appropriate spam, do not fax, do not call, call recording and broader communications policies.

6. Have you and your vendors adopted a formal, written data security compliance program? Despite a sectoral 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 security regulations applicable to the health-care industry;[10] (ii) the Gramm-Leach-Bliley Act (GLB Act) ''safeguards'' regulations for financial institutions;[11] (iii) state insurance law analogs to the GLB Act Safeguards Rule applicable to insurance companies;[12] and (iv) and state laws governing businesses that maintain personal information of residents. 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 personal information of Massachusetts residents.[13] Most states also have data breach response and reporting laws, which require prompt action following a suspected compromise. Indeed, 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 are not sensitive.

7. Does your company engage in behavioral advertising? Online behavioral advertising (OBA) is the term used to describe this 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 nonaffiliated site (e.g., retargeting a user who has left your site with an ad on another site), is subject to self-regulatory rules and best practices guidance promulgated by the FTC.[14]

Before engaging in any OBA, companies (both advertisers and publishers) should review the cross-industry behavioral advertising self-regulatory guidance, which provides a self-regulatory framework for advertisers, agencies, publishers and technology companies for engaging in OBA.[15] The Digital Advertising Alliance (DAA) also provides an iconic form of notice that alerts consumers to OBA and provides a method of opt-out.[16] 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 websites 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.

8. Is your digital marketing campaign targeted to children? Children's privacy issues are lurking in many digital marketing campaigns, whether or not the campaign is directed to children. On July 1, 2013, the FTC updated its rule implementing Children's Online Privacy Protection Act (COPPA Rule), which requires a company to obtain parental consent prior to collecting personal information from a child under the age of 13 online or via mobile apps with limited exceptions.[17] The updated COPPA regulations greatly expand what kind of data requires verified parental consent before being collected from a child under 13 years of age, 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 an Internet

[9] *See Policies and Guidelines*, Mobile Mktg. Ass'n, http://mmaglobal.com/policies (last visited June 5, 2014).

[10] *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified at 42 U.S.C. § 300gg, 29 U.S.C § 1181 et seq. and 42 U.S.C. § 1320d et seq.); 45 C.F.R. pt. 160; 45 C.F.R. pt. 164, subparts A and C.

[11] *See* 15 U.S.C. §§ 6801(b), 6805(b)(2); 16 C.F.R. pt. 314.

[12] *See, e.g.*, Cal. Code Regs. tit. 10, §§ 2689.14–2689.19.

[13] *See* 201 Mass. Code Regs. § 17.03.

[14] *See* FTC, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

[15] *See Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), *available at* http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf.

[16] *See AdChoices*, DAA, http://www.youradchoices.com (last visited June 5, 2014).

[17] Children's Online Privacy Protection Rule; Final Rule, 78 Fed. Reg. 3971 (Jan. 17, 2013) (codified at 16 C.F.R. pt. 312), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-01-17/pdf/2012-31341.pdf (11 PVLR 1833, 12/24/12; 12 PVLR 1184, 7/8/13).

protocol address). Also, the COPPA Rule 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 must now age-screen users in a neutral manner, and treat them differently based on self-reported age. Mixed use sites cannot block children under 13 completely, but must offer them COPPA-compliant services.

The FTC has made it clear that once any operator (even if directed to adults) has notice that a persistent identifier belongs to a child under 13, it must immediately take action to prevent a violation of COPPA. This includes ensuring that behavioral advertising is not served to them, that social media plug-ins and tools where they can submit publicly 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.

Even if an operator could employ a cookie or other device to identify users it learns are under 13, given all the third parties affected (e.g., in the advertising ecosystem), real challenges remain to be solved before effective differentiation can become reality. In the meantime, other work-arounds can be employed to minimize risk. Digital marketing campaigns that are clearly required to comply with COPPA because they are targeted to children, even in material part, often make basic mistakes, such as not posting a COPPA-compliant privacy policy (or any privacy policy at all), making the policy hard to find, assuming that it is okay to collect information from children so long as the site does not do anything with it or failing to properly secure parental consent before personal information from a child is collected.

9. Will your campaign collect location-based information from consumers or otherwise publicly share 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 his or her 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 the user. 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 certain notices be given and consent obtained before enabling such functionality on apps or other services. General caution should also be exercised. A digital 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. With respect to location tracking and accessing certain device content or functionality, notice, an opportunity to review and consent are required by carrier and platform rules. For LBS technology, 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. Short-form notice is recommended at the point of consent.

10. How could including videos in my digital marketing campaign be a privacy issue? The Video Privacy Protection Act (VPPA)[18] and similar state laws prohibit disclosure of information that identifies a person as having requested or obtained specific video materials or services, without having first obtained consent from the user. 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 a social networking site like Facebook. In order for a company to be able to share information that links a customer to having viewed particular video materials or services with a third-party social media site, the company first needs to obtain user consent to do so. Video service providers can obtain consent electronically over the Internet from a user for use of the video information for a maximum period of two years under the VPPA.[19] The form of consent requires that 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.

Conclusion

Big data and the interactivity of digital marketing are powerful tools for marketers, but consumer data protection laws have evolved in recent years, resulting in new and heightened compliance and risk management issues that need to be addressed when executing advanced advertising campaigns. 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.

---

[18] 18 U.S.C § 2710.

[19] *Id.* § 2710(2)(b)(ii).

  PVLR ISSN 1538-3423

NEW PORTFOLIOS & TREATISES NOW AVAILABLE

SAFE DATA & SOUND SOLUTIONS

Privacy & Data Security Law Resource Center™

Unparalleled news. Expert analysis from the new Privacy & Data Security Portfolio Practice Series. Comprehensive new treatises. Proprietary practice tools. State, federal, and international primary sources. The all-in-one research solution that today's professionals trust to navigate and stay in compliance with the maze of evolving privacy and data security laws.

TO START YOUR FREE TRIAL CALL 800.372.1033 OR GO TO www.bna.com/privacy-insights

Bloomberg BNA