wiley

ARTICLE

Look Out for Privacy Traps

Multichannel News
May 2, 2011

Media companies are benefitting from all sorts of new tools, like enhanced websites, social networking and mobile applications. New functionality can drive users to online offerings, and raise the profile of associated TV and radio stations, for example. It can also strengthen the historical partnership between local media and local businesses, as the recent online coupon craze demonstrates. Also, online advertising provides an important new revenue stream, and as targeted advertising grows more sophisticated, media outlets can demand higher premiums for advertising space.

Yet with these opportunities, care must be taken to keep privacy-related risks in check. A good operating assumption is that new media tools will collect some information about individuals. Such information does not necessarily need to identify an individual by name in order to carry concerning privacy implications. Wrong steps could lead to reputational injuries at least, and data breaches, enforcement actions or civil penalties at worst.

Each use of new media raises different privacy risks. But privacy hot spots tend to appear consistently in the following areas:

- **Does your content attract children?** Online offerings might foreseeably be attractive to kids 12 years old and younger. Or you could be aware that your website actually has collected children's personal information. Consider, a website reflecting a station's "Top-40" format might officially target an older teen/young adult demographic, but offer considerable "tween" appeal. Such situations are rife with legal risk under the Children's Online Privacy Protection Act (COPPA), which is actively-and publicly-enforced by the Federal Trade Commission (FTC), sometimes with seven-figure settlement

Authors

Ari Meltzer
Partner
202.719.7467
ameltzer@wiley.law

Practice Areas

Media
Privacy, Cyber & Data Governance
Telecom, Media & Technology

penalties.

- **Is your privacy policy up to date?** Privacy policies can quickly become stale as companies add new online offerings or change the way they handle personal information in response to new opportunities. An outdated policy poses legal risks, as falling short of its promises could amount to "unfair or deceptive trade practice." Both the FTC and state Attorneys General have pursued failures to uphold privacy policies, which is a binding public representation about how a company will deal with personal information.
- **Have you covered the information security basics**? If your website or mobile app engages in any type of e-commerce, do you encrypt the transaction, and especially any credit card numbers? In the "back office" supporting your online offerings, are default user names or passwords avoided? Wireless connections secured? Where basic security precautions were not taken, the FTC has publicly shamed companies that suffered security breaches. Notably, a company need not necessarily make a public representation concerning information security in order to be caught in the FTC's net.
- **Do you know which marketing laws apply to your campaigns?** Do you plan to market your offerings or those of your partners by text message? Email? Phone call? Fax? If so, federal or state law could limit whom you can contact or require certain opt-out choices. Violations of such law could lead to enforcement actions, and in some cases, private rights of action.
- **Do your mobile applications use location information?** Media companies using mobile applications could be using location information to enhance the service. Yet, location information is sensitive, and certain legal limitations apply.
- **Do you know what your partners and vendors are doing?** New media is truly an "ecosystem," where a single service can involve a web of retailers, communications providers, vendors, advertisers, transaction processors and so on, connected through different types of legal relationships. All of these parties could be using personal information while conducting business important to your new media strategy. Thus, you should understand how your associates are using and securing personal information, the risks that could rebound upon your company, and where appropriate, make sure that the broadcaster's privacy policy is being upheld.
- **Do you use online advertising best practices?** Congress, the FTC, state authorities and privacy advocates are ready to regulate online targeted advertising, unless industry self-regulation is found to work. Media companies have an interest in maintaining a self-regulatory regime, where innovative technology and business arrangements can be quickly put to use. Further, unintended consequences of regulation could choke off the important revenue streams that ultimately fund free online services. Accordingly, you should consider adhering to voluntary guidelines concerning online ads that industry groups have developed. Your company may also wish to participate in ongoing policy debates. You should understand the types of technology that your ad networks use, and avoid especially intrusive or aggressive mechanisms.

Every company should periodically review its privacy and security practices to make sure that it is avoiding common pitfalls.

*District of Columbia Bar (pending, supervised by principals of the firm)