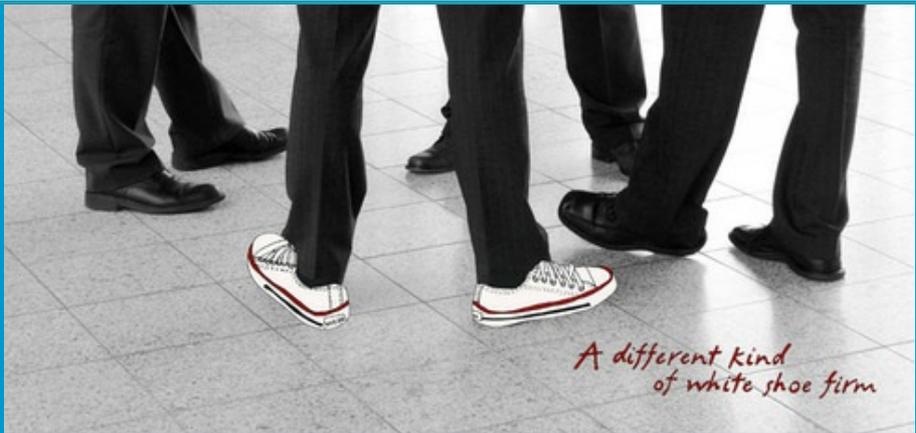


THE INGRAM YUZEK WIRE



INGRAM YUZEK GAINEN CARROLL & BERTOLOTTI, LLP

May 10, 2011

Best Practices for New Media Part 1: Privacy and Information Management

By: [Douglas Pulitzer, Esq.](#)

The Internet, virtual worlds, social media sites such as Facebook and Twitter, and mobile applications, or “New Media” as they are collectively known, have opened up entirely new ways for companies to communicate and interact with their customers and prospects. With this new territory, however, comes a raft of new risks for businesses. This article explains some of the best ways to avoid common pitfalls:

1. Know Your Company’s Partners, Affiliates and Vendors. Setting up a single service on New Media can involve a complex network of developers, retailers, communications providers, vendors, advertisers, and fulfillment and transaction processors, all associated through various types of legal relationships. Any or all of these parties may be using sensitive customer information while conducting business important to your company’s New Media objectives, whether collecting, transmitting, accessing, processing, storing, disclosing, securing and or disposing of such data.

Tip: Companies should understand how sensitive or personal customer information is being used by such parties and the risks that this exposes your company to. Where appropriate, make sure that your company’s information use and securitization (encryption) policies and requirements are being followed.

2. Mobile Application Privacy Requirements. When customers install a mobile application with your company’s name and logo, they expect your company to adequately safeguard the personal and sensitive information they keep on their phones. Breaching that trust may harm a company’s reputation, in addition to presenting legal repercussions.

Tip: It is important that those who use your company’s mobile application(s) are aware of, and explicitly accept during installation, the way that the application uses their personal and sensitive information. In addition, if you hire a third party to develop your company’s branded mobile application, ensure that the developer agreement states your company’s information use and securitization (encryption) requirements and adequately protects your company from the developer’s failure to comply with these requirements.

3. History Sniffing and Behavioral Advertising: You should know whether your company or any of its providers/partners is accessing information about visitors to the company website and the devices they use. This access could be in the form of cookies, which deposit files on the visitor’s computer, or perhaps “history sniffing” devices which draw on a visitor’s browsing history to generate targeted or “behavioral” advertising.

Tip: Schedule regular audits by outside counsel to determine whether and to what extent your company is using cookies, history sniffing and other such devices. If these technologies are being used, the company should develop and implement a legally compliant tracking and behavioral advertising policy and make certain that its privacy and terms of use policies are up to date.

4. Clear Rights to Your Company’s Customer Information: Clearly defined rights in and to your customer’s information without unwarranted liability is crucial to building and maintaining a productive and sustainable business through New Media.

Tip: Make sure your company’s New Media agreements with its partners, licensors and licensees explicitly state: (a) who owns the information collected by such parties on your company’s behalf, (b) who may use it during and after the agreement terminates and (c) who is responsible for data security breaches and for compliance with applicable security notification breach statutes.

5. Up-to-Date Privacy Policies. Public facing privacy policies can quickly become stale as your company adds new online offerings or tracking technologies, or changes the way it handles personal and sensitive 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 Federal Trade Commission and state Attorneys General have pursued failures to uphold privacy policies, which are binding public representations about how a company will deal with personal and sensitive information.

Tip: Conduct a thorough review of how your company collects, uses and shares personal and sensitive information via mobile apps and other online services. Such a review should examine whether your company's published privacy policies reflect actual data usage practices and are reasonably comprehensive, easy to read and easy to access. At a minimum, make certain your company's published privacy policies are up-to-date and clearly state what type of information your company collects, who may provide information, how it uses and secures this information, who it may share this information with, how an individual may request changes to such information, and the policy's effective date.

6. Marketing Laws. Violations of any international, federal and state offline and online marketing laws that apply to your company's New Media campaigns could lead to enforcement actions, and in some cases, private rights of action. Such laws may limit whom your company can contact, have notification requirements, or require affirmative consent or certain opt-out choices.

Tip: Make sure your company adheres to all such laws, by establishing compliance policies and programs that are implemented and regularly updated, conducting training of relevant marketing personnel in such policies, and conducting regular audits to ensure compliance.

Future articles will discuss the related New Media topics of: trademark and domain name licensing, registration and transfer, privacy by design and worldwide information governance.

To discuss best practices for New Media privacy and information management further, please contact Douglas Pulitzer whose practice specializes in privacy, information management, intellectual property, technology, ecommerce and mcommerce. Douglas may be reached at: dpulitzer@ingramllp.com and (212) 907-9690.



[The Ingram Yuzek Wire](#)

Ingram Yuzek attorneys author timely articles on the latest developments on regulatory and legislative activities, court rulings and case law on a number of legal topics. These articles are delivered to Ingram Yuzek Wire subscribers and serve to keep readers up-to-date on late-breaking legal developments in a number of areas, including New Media, information, privacy, intellectual property, technology, tax, real estate, corporate and commercial law.



[Forward this message to a friend](#)

© [INGRAM YUZEK GAINEN CARROLL & BERTOLOTTI, LLP](#). ADVERTISING MATERIAL. These materials are to inform you of developments that may affect your business and are not to be considered legal advice, nor do they create a lawyer-client relationship. Information on previous case results does not guarantee a similar future result.

[Ingram Yuzek Gainen Carroll & Bertolotti, LLP](#)

250 Park Avenue
New York, New York 10177
Tel: (212) 907-9600
Fax: (212) 907-9681

[Click to view this email in a browser](#)

This communication was sent to {email_address} as a contact of Ingram Yuzek LLP. If you wish to unsubscribe, please reply to this message with "Unsubscribe" in the subject line or click here: [Unsubscribe](#)

Ingram Yuzek Gainen Carroll & Bertolotti, LLP
250 Park Avenue
6th Floor
New York, New York 10177
US