How to Manage Mobile ‘Big Data’ Legal Risks

Michael Reif

Mobile devices and their related applications offer food industry members extraordinary big data [1] opportunities. With more than 6 billion in use worldwide, mobile devices produce a constant stream of data — from user location to transactions and activity — that can be analyzed to provide insights on key consumer sentiment, behavior and movement patterns. Mobile devices also serve as an effective delivery mechanism for near real-time, highly personalized messages and incentives regarding goods and services through techniques like geo-fencing, augmented reality packaging and e-coupons. But the opportunities accompanying mobile’s big data possibilities are not limitless. Government policies and privacy laws create very real exposures that food industry members must keep in mind as they seek to leverage mobile big data.

Mobile, Big Data and Food: Finding the Line

Taking advantage of mobile’s many marketing opportunities requires navigating both existing and emerging government rules and regulations intended to protect consumer privacy. Getting privacy right matters. First, some privacy regulations impacting mobile impose hefty fines for violations. More important, when big data efforts make consumers feel stalked, brand value declines. As a result, understanding current privacy rules gives the double benefit of lowering legal risks for mobile privacy breaches as well as protecting brand value.

Mobile and the TCPA

In a field still largely unregulated, the clearest rules for interacting with consumers via mobile devices come from the Telephone Consumer Protection Act [2] (TCPA), 47 U.S.C. § 227 *et seq*. The TCPA restricts the use of automated telephone dialing systems (ATDS) to send unsolicited telemarketing and text/SMS messages. States and individuals who prove a violation of the TCPA may receive a $500-per-violation award, which can be tripled to $1,500 if the violation was willful or knowing. The majority of states have laws similar to the TCPA that cover the use of ATDS to deliver marketing messages. TCPA litigation has increased significantly in recent years, and companies have paid tens of millions of dollars to resolve consumer TCPA class actions.

Effective October 16, 2013, new TCPA regulations now require prior express *written* consent for all telemarketing robocalls and text/SMS messages to wireless numbers and residential lines. These new requirements mean many companies' "opt in" lists are now insufficient or obsolete. Companies that failed to contact customers before the October deadline now are struggling with how to get the consent they need without running afoul of the TCPA's restrictions.

Food companies that use text messaging as part of their marketing efforts need to understand the TCPA's increased consent requirements and ensure that any third-party service providers do too. Under the TCPA, companies may be held vicariously liable for calls made through third-party telemarketers. The FCC [3] has said a formal agency relationship does not need to exist for this kind of liability to arise — and courts have agreed.

Managing Privacy and Mobile Apps

Given the potential TCPA-related liability, many marketers are bypassing text messaging or phone calls and instead using mobile apps to reach consumers. When consumers download and sign-in on apps, they often provide personal information that allows for deeper specificity and targeting of data-driven marketing efforts.

But those efforts are not entirely unrestricted. While no current law or regulation directly targets mobile applications at the federal and state level, both the FTC [4] and the California Attorney General have issued guidelines to protect consumers. These guidelines reflect government concerns about the sometimes unintended access to consumers' personal information created by mobile's big data capabilities.

For example, the makers of the social networking app Path routinely accessed users' address books, collecting and storing information about users' contacts without disclosing this practice. Information collected included the contacts' names, birthdays, email addresses and Twitter handles. Path also obtained personal information from users under the age of 13 without their parental consent — a violation of Children's Online Privacy Protection Act [5]. The FTC brought an enforcement action against Path, which Path settled for $800,000 without an admission or denial of wrongdoing.

The FTC's enforcement action against Path shows that the FTC will actively enforce

consumers’ mobile privacy rights. Similarly, California — a hotbed of technology and innovation — has effectively set the industry’s privacy standard by issuing guidelines to app developers, app platforms and advertising networks. As a result, even though they are “just guidelines,” current mobile privacy standards deserve close attention.

Making Mobile Big Data Work

The rich opportunities to engage consumers offered by the marriage of big data and mobile make it worthwhile to manage the legal risks involved. Some suggested best practices include:

For SMS/Text messaging:

- Vet current text message marketing lists to make sure they comply with updated TCPA rules regarding written consent and get good advice on how to obtain any additional consent needed.

For apps and advertising (Adapted from California Attorney General Recommendations):

- Prepare a privacy policy that describes your collection, use, disclosure and retention of personally identifiable user data.
- Provide your privacy policy to the app developers who enable the delivery of targeted ads through your network. Provide a link to your privacy policy for developers to make available to users before they download or activate the app.
- Avoid delivering ads outside the context of the app. Examples are delivering ads by modifying browser settings or placing icons on the mobile desktop.
- Use enhanced measures and obtain prior consent from users before accessing personal information such as phone number, e-mail address or geolocation.
- Transmit user data securely, using encryption for permanent unique device identifiers and personal information, such as an e-mail address or phone number.
- Create and implement a plan for secure data storage and timely data destruction.

Conclusion

Consumers are often willing participants in big data-generated efforts that enable them to interact with brands and make their choices matter. But consumers also

are gaining a growing understanding of the privacy implications that come from carrying a data-transmitting-and-receiving device with them at all times. Only food companies that understand the brand and legal risks mobile creates can take the steps needed to manage such risks — and put big data mobile to work for them.

Michael Reif [6] *is an attorney at Robins, Kaplan, Miller & Ciresi L.L.P.* [7] *He has served Food and Beverage companies, including grocery and consumer electronics retailing, and multinational food and beverage distribution, in complex business disputes. mdreif@rkmc.com* [8].

For more food industry news and information, subscribe here ***[9] and follow us on*** Twitter ***[10],*** Facebook ***[11] or*** LinkedIn ***[12].***

Source URL (retrieved on *07/23/2014 - 12:56am*):
http://www.foodmanufacturing.com/articles/2014/04/how-manage-mobile-%E2%80%98big-data%E2%80%99-legal-risks

Links:
[1] http://www.foodmanufacturing.com/articles/2014/03/harnessing-big-data-turn-consumer-social-media-trade-secrets
[2] http://transition.fcc.gov/cgb/policy/TCPA-Rules.pdf
[3] https://twitter.com/FCC
[4] https://twitter.com/FTC
[5] http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
[6] http://www.rkmc.com/lawyers/michael-reif
[7] http://www.rkmc.com/services/food-and-beverage
[8] mailto:mdreif@rkmc.com
[9] http://subscribe.advantagemedia.com/fm_ods/landing.aspx?cmpid=footerlink
[10] https://twitter.com/foodmfg
[11] https://www.facebook.com/FoodManufacturing
[12] http://www.linkedin.com/groups/Food-Manufacturing-wwwfoodmanufacturingcom-4656128?trk=my_groups-b-grp-v