Mobile Food & Beverage Marketing

State Law Approaches to Address Digital Food Marketing to Youth

Essentially every new youth-focused food marketing campaign includes mobile components or is mobile-focused. Federal and state laws have not kept up with rapidly evolving mobile technologies, and jurisdictional issues may forestall state regulators' efforts to protect child and teen consumers in their states. This section will describe the mobile food marketing industry, location-based tactics, the harm mobile marketing poses, and the federal and state legal frameworks governing mobile marketing.

Mobile Marketing

Figure 1: Dum-Dum Flick-A-Pop App

In 2010, the mobile marketing industry in the United States netted $24 billion, with as much as $80 billion in earnings projected for 2011.[1] The direct mobile marketing industry is comprised of wireless service providers (companies with which consumers contract for cell phone and mobile data services, such as Verizon Wireless and T-Mobile) and companies involved in the third-party wireless content industry, who are in the business of delivering wireless content to consumers' mobile phones. This category includes advertisers, content and application providers, aggregators of third-party mobile content and Internet marketing companies. Since consumers can now access the Internet on their smartphones, even companies that send traditional commercial messages by e-mail to consumers participate in mobile marketing. Companies that make marketing calls and/or send short message service (SMS) texts to wireless phones also utilize mobile marketing techniques.

Figure 2: Chuck E. Cheese "Say Cheese" Augmented Reality App

A major component of mobile marketing is the use of applications (apps) that consumers download to their mobile devices. Advertisers and app developers form relationships for their mutual benefit; advertisers get their ads out to the mobile audience, while app developers get paid when users click on the ads. Advertisements may be used to partially or completely subsidize the price of a mobile app or the services provided by an app.[2] Food companies can design and disseminate apps that are advergames (Figure 1). Apps can be designed to interact with other marketing materials like product packaging, e.g., a consumer downloads an app that displays augmented reality features when aimed at product packaging. Augmented reality puts the consumer in an artificial digital environment that utilizes some aspects of the physical world (Figure 2). Apps designed and disseminated by food companies are very popular with children.[3] Food companies also can reach chil-

dren and teens through in-app advertising in the form of banners, splash pages utilized eye-catching effects, links and mobile coupons that are designed to be easily shared with friends.[4]

Location-Based Techniques

The power of mobile marketing is amplified by the fact that it can be combined with a user's location data. Location-based mobile marketing allows food marketers to make pedestrians and drivers aware that they are in close proximity to fast food restaurants, make travelers aware that a certain product is available in an unfamiliar place, or alert youth when they enter a shopping center's parking lot of special offers available in the food court.[5] 77% of teenagers own mobile phones,[6] and they are more likely than adults to use their mobile devices for text messaging, social networking and accessing entertainment and information, making them prime targets for location-based advertisements for unhealthy snacks, beverages and fast food.[7] In this section we describe location-based marketing using apps, and how "geo-fencing" and "micro-fencing" can be used to target young consumers with food marketing.

Mobile apps

Apps running on smartphone operating systems equipped with Global Positioning System (GPS) technology have access to information about consumers' geolocation,[8] and can use it to provide a specific service, such as identifying and connecting users playing a game with others playing the same game in a geographical area, delivering special offers or providing directions to a retail location.[9] Even when a user's location information is not necessary to provide the service associated with the app, apps may still collect location data.[10]

Food company-designed apps and in-app advertisers use consumer geolocation information in several ways. They use it to reach users in a particular geographic location, and/or to display different messages to users based on their precise location.[11] For example, advertisers can use location information to provide alerts and serve offers when a customer is near a unique store location. Advertisers may use "check-in"-based contests and games that reward users with discounts or coupons for visiting store locations and "checking-in" via their GPS-enabled mobile devices.[12] When the consumer checks in at the location, she provides a valuable marketing service to the food company because her location is broadcast to her friends on Facebook or her followers on sites like Foursquare.

Applications that require location information to provide a specific service to users and those that collect it unnecessarily may share that data with third parties involved in mobile marketing.[13] Ad networks such as AdMob by Google connect advertisers and publishers, allowing application developers access to a pool of ads, and marketers access to the mobile audience. Ad networks manage mobile campaigns and use consumer information provided by applications to insert ads that are relevant to consumers' demographic information, interests and geolocation.[14] Service providers providing the advertising content and other services within an app may also be privy to consumers' geolocation information.[15]

Geo-fencing

Geo-fencing companies are independent businesses that contract with telecommunications carriers or retailers to place virtual boundaries around stores, events and other locations. Geo-fences allow retailers to reach consumers on their mobile phones within a defined geographic area in two ways: subscribers may download an app onto their phones and receive information via the app when they are inside a geo-fence, or consumers are alerted by their mobile carriers via a text or multi-media text.[16] In the first scenario, the geo-fencing company assists the retailer in developing an app that cell phone users can download onto their phones, places virtual boundaries around certain stores or events, and sends alerts to consumers who have downloaded the app and

have it running when they enter a geo-fenced area.[17] In the second scenario, wireless carriers such as AT&T offer such messages as an opt-in service to their subscribers. The mobile carrier contracts with a geo-fencing company, who places virtual boundaries around stores and events and then "pings" or communicates with the carrier's network periodically to see which users are inside a geo-fence. Those users then receive a message alert on their phones. In this scenario, consumers do not need to have smartphone technology, and can be reached at any time.[18]

Micro-fencing

Since GPS technology does not work indoors, micro-fencing companies are rapidly developing ways to deliver indoor consumer location. Food retailers can use indoor location information to send special offers and walking directions to a store. The micro-fencing market is relatively new, and currently there are a number of competing technologies. These include: near-field communication and radio frequency identification (RFID) that both require tags and tag readers; light field communication whereby light bulbs are retrofitted to emit different strobes in various locations throughout a building that are not visible to the human eye but that can be captured by a mobile phone camera to determine precise indoor location;[19] and Wi-Fi access point triangulation that leverages a building's network of Wi-Fi access points to determine a user's indoor location.[20] The legal and privacy implications of micro-fencing are rapidly emerging. In addition to the serious privacy issues raised, especially for teens who are not covered by the Children's Online Privacy Protection Act (COPPA), the powerful cueing effect of receiving a special coupon or a reminder to visit a food retailer or vending machine should be of concern to the public health and state regulatory communities when children and teens are targeted.

What Is the Harm?

Food marketers are at the forefront of mobile marketing targeting youth, and present a new set of issues for regulators. Food and beverage marketers don't simply want young consumers to recognize their brands or desire their products -- their ultimate goal is to generate actual purchases. Mobile marketing dramatically shortens the distance between a company's marketing message and the consumers' purchase decisions. Food and beverage company marketing executives are not shy about the intent of their mobile campaigns. When discussing Coca-Cola's marketing plan to "reach every hand with a mobile phone," one Coca-Cola executive said: "I am looking at how we can use mobile technology and content to get a transaction. We are not just in the brand building business, we are in the direct response business."[21] A major snack company executive echoed the sentiment: "We want to use mobile to drive impulse purchase behavior."[22]

Young people are especially vulnerable to predation by mobile marketers because they often grant permission to access personal information and location data or agree to pay for services without fully understanding the commercial nature of the messages delivered to their phones.[23] A survey of girls 6 to 16-years-old found that almost one quarter (22%) reported that they always tap on mobile ads they see in mobile apps regardless of whether they are interested in the featured product, and more than half (56%) said they tap on ads for products that interest them. Forty-two percent reported that they share ads they like with friends via text and in-ad share buttons.[24]

Unfair and deceptive mobile food marketing harms young consumers economically through the purchases of food items they would not otherwise have purchased. It also harms their health from the excess calories, sodium, caffeine, etc. consumed as the result of the marketing. Potentially unfair and deceptive mobile food marketing practices targeting youth include campaigns that

are designed to: trigger impulse purchases of unhealthy products; blur the line between entertainment or mobile content and marketing; and appear to be from friends when in fact they are generated by a food company.

State Attorney General Oversight of Mobile Marketing

Mobile marketing is subject to the federal and state laws that regulate other types of advertising, but is complicated by the fact that it is deployed using telephonic and Internet-based communication systems. The Federal Trade Commission (FTC) regulates unfair and deceptive advertising practices, and the Federal Communications Commission (FCC) regulates interstate communication.[25] The FTC is granted the statutory power to enforce the Federal Trade Commission Act (FTCA), and every state has its own consumer protection law enforceable by the state Attorney General (SAG).[26]

Jurisdictional challenges

Mobile marketing claims brought under state Unfair and Deceptive Acts and Practices (UDAP) statutes and anti-fraud laws must contend with jurisdictional challenges and federal pre-emption. Defendants may claim that the FTC or FCC has primary jurisdiction over claims brought against mobile marketers' advertising practices, and/or that the agencies' regulations pre-empt state law. The primary jurisdiction doctrine provides that when an issue falls within the special competence of an administrative agency, such as the FCC, it should be referred to that agency.[27] In cases involving fraud or deceptive practices perpetrated by wireless carriers and other communications companies, courts have repeatedly upheld states' authority to protect their citizens.[28] Claims brought under state UDAP and anti-fraud laws may also face subject-matter jurisdiction challenges. Defendants may attempt to remove such claims from state to federal court, under the theory that the FTCA or other federal law justifies pre-emption of state claims and removal of claims to federal court.[29] Courts have held that the FTCA and other FTC and FCC regulations do not have the pre-emptive force to require removal of claims brought under state laws to federal court simply because consumers could have pursued complaints in federal court.[30]

Mobile marketing as a violation of anti-spam laws

Mobile marketing practices may violate federal and state anti-spam laws. Anti-spam laws protect against unsolicited bulk e-mail and malicious attachments, viruses and links to fraudulent websites frequently contained in spam e-mail. In 2003, Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) in order to reduce spam and end false and deceptive spamming practices. CAN-SPAM empowered the FTC and FCC to promulgate a large body of complementary regulations.[31] The FCC was granted the specific authority to promulgate rules regulating wireless spam, which it did in 2005.[32]

Marketers are able to send marketing messages directly to a consumer's mobile phone by using an e-mail address consisting of a combination of the consumer's phone numbers and an Internet domain name provided by a wireless carrier.[33] The resulting message is called a mobile service commercial message (MSCM) and arrives to the recipient's phone in the form of a textual or multi-media message.[34] MSCMs differ from SMS texts, which are texts are sent from other mobile phones without passing through an e-mail channel. The FCC has created a list of commercial domain names belonging to wireless service providers; senders of MSCMs utilizing domain names found on the list are subject to specific FCC regulations. Among other requirements, marketers using domain names on the FCC's list must obtain the consumer's express consent prior to sending MSCMs (opt-in consent), with exceptions for transactional and relationship messages.[35] The FCC's regulations apply only to messages sent using domain names registered on the FCC's website. They do not apply to messages

sent from other phones, messages sent to consumers' e-mail addresses and forwarded to or accessed on consumers' mobile phones, or to MSCMs sent using domain names not listed on the FCC's website.

Marketers can also send e-mails containing commercial content from other e-mail addresses, which recipients frequently access on their Internet-capable mobile phones. CAN-SPAM and complementary FTC rules apply to commercial messages sent to consumers' e-mail addresses, including those accessed on mobile devices.[36] Among other requirements, the relevant laws allow marketers to send unsolicited commercial e-mail as long as recipients are given the option to refuse the receipt of future messages (opt-out consent).[37]

State authority to regulate SPAM

CAN-SPAM grants SAGs enforcement authority, but limits that power to the sections of the statute that impose requirements on the transmission of spam sent to consumers' email addresses on their computers (non-wireless spam).[38] SAGs are thus empowered to enforce CAN-SPAM's prohibitions on commercial e-mail containing false or misleading transmission paths and deceptive subject headers. They can also enforce CAN-SPAM's requirement that senders place warning labels on commercial e-mail that contains sexually explicit material.[39] SAGs are empowered to prosecute persons who engage in a "pattern or practice" that violates CAN-SPAM's mandates that senders cease to send e-mails after the recipient objects, that marketers clearly identify messages as advertisements, and that senders of commercial e-mail include functioning opt-out mechanisms and accurate return e-mail and physical addresses.[40] CAN-SPAM expressly pre-empts state laws regulating commercial e-mail, but contains a savings provision for state laws that prohibit "falsity or deception" in commercial e-mail that are not specific to electronic mail, and that are related to fraud and computer crime.[41] Courts have split on which state laws fall into CAN-SPAM's exemption from pre-emption for state laws, including UDAP statutes, prohibiting "falsity or deception" in commercial e-mail.[42]

Mobile marketing as a violation of telemarketing laws

When mobile marketers make calls or send text messages to consumers' wireless phones, federal and state legislation regulating telemarketing practices apply. Such legislation is designed to protect consumers from harassing phone contacts and fraudulent and unfair telemarketing practices.[43] The exact laws that apply depend on whether a call or text is sent by a live person or an auto-dialer.

The Telemarketing and Consumer Fraud and Abuse Prevention Act (TCFPA) empowered the FTC to establish the National Do-Not-Call Registry and to issue the complementary Telemarketing Sales Rule (TSR), which governs live calls and text messages sent to wireless phone numbers from other phones.[44] The TSR prohibits calling phone numbers placed on the Do Not Call Registry, certain deceptive practices, calling at early or late hours, and requires telemarketers to disclose up front the marketing purpose of their call.[45] These prohibitions may apply to commercial text messages sent to wireless phone numbers.[46]

The Telephone Consumer Protection Act (TCPA) and the complementary FCC TCPA Order govern autodialed and pre-recorded calls and texts made to wireless numbers.[47] While live telemarketing calls and texts to wireless numbers are permitted as long as such calls comply with relevant laws and regulations,[48] calls and text messages made using automatic telephone dialing systems (ATDS) (also known as auto-dialers) and/or prerecorded messages are prohibited if the customer is charged for the message, unless consumers give prior consent.[49] While the TCPA was written before SMS technology was common and does not specifically refer to SMS or text messages, the FCC's TCPA Order and a recent Ninth Circuit decision make clear that the text messages are

considered "calls" and that the TCPA and FCC's prohibitions on using ATDS or prerecorded messages applies to the sending of text messages.[50]

State authority to regulate

The Telemarketing and Consumer Fraud Prevention Act (TCFAPA) (governing live calls and granting the FTC the power to regulate telemarketing) does not preserve exclusive enforcement power for federal regulators, nor pre-empt state law.[51] The statute grants SAGs the power to enforce FTC rules, and the FTC's Telemarketing Sales Rule has equivalent provisions.[52] Both the TCFAPA and the TSR explicitly specify that state officials are not prohibited from proceeding in state court for violations of state statutes.[53] The TCPA grants a private right of action to consumers and enforcement power to SAGs to bring suits in federal court against telemarketers that use ATDS and pre-recorded messages to make calls or send texts.[54]

Jurisdictional challenges

Jurisdictional challenges to cases brought in TCPA suits include motions to dismiss for lack of personal jurisdiction, similar to those brought against CAN-SPAM plaintiffs. Defendants may also argue that because they made calls from a state other than the forum state, the forum state has no authority to regulate the interstate calls.[55] Although these challenges are framed in pre-emption language, the basis of the conflict is states' jurisdiction to reach conduct that occurs outside of their borders but affects their citizens. While some courts have upheld states' ability to enforce state laws against out-of-state defendants,[56] other courts have upheld defendants' allegations that the TCPA pre-empted state statutes imposing stricter standards on interstate communications than the federal law.[57]

State oversight of apps targeting youth

Apps that consumers download onto their smartphones present a unique mobile marketing challenge for state regulators and are subject to yet another subset of federal law. Mobile carriers such as Verizon Wireless and T-Mobile are governed by the federal Communications Act and the FCC's corresponding regulations.[58] The relevant laws mandate consumer opt-in consent before disclosing or permitting access to personal information, including geolocation data.[59] These laws currently do not apply to app providers and third parties involved in mobile advertising.[60] These parties are governed by their contracts with app stores and mobile carriers, and subscribe to a set of industry self-regulation guidelines. A 2012 FTC staff report found that the Apple store, iTunes and the Google Play store contractually require app developers to disclose the information their applications collect but routinely do not enforce these requirements.[61]

The Mobile Marketing Association (MMA) and CTIA-The Wireless Association (CTIA) are self-regulatory bodies that maintain guidelines for mobile carriers and third parties using location information. The MMA instructs marketers to notify consumers about how their location information will be used, disclosed and protected, and to obtain user consent before collecting consumers' precise geolocation data or sharing that information with third parties.[62] CTIA's guidelines recommend that consumers receive notice about how location information will be used and shared, and that they consent to the use or disclosure of location information.[63] The FTC's February 2009 staff report on online behavioral advertising also indicates that precise geolocation data is sensitive data which requires express consent to use.[64]

Current data shows that disclosures from application providers are far from adequate. A 2012 FTC staff report examined four hundred mobile applications designed for children and found that the disclosures provided by application providers regarding the collection, sharing and use of geolocation and other personal information

overwhelmingly failed to reveal whether the apps collected any data, the purpose of any such collection and the identity of the entities collecting and/or obtaining access to the data.[65]

Updated COPPA regulations, effective July 1, 2013, are applicable to child-directed mobile marketing, contain an expanded definition of personally identifiable information and extend coverage to the use of that information by third parties.[66] COPPA is enforceable by SAGs and it applies to apps and the collection and use of location data of children under 13 by marketers and third parties. Even prior to the 2013 COPPA update, which included new protections from marketing practices, state regulators had an impact on child-directed apps. In 2012, New Jersey's Attorney General Jeffrey Chiesa initiated a COPPA lawsuit against 24x7 Digital LLC, a Los Angeles based company that develops children's apps. The suit alleged that the company collected, maintained and transmitted to a third party the personal information of children. The parties settled with a consent decree stipulating that 24x7 Digital would stop collecting personal data from its app users and would destroy all previously collected data that allegedly violated COPPA.[67] 24x7 Digital was enjoined from failing to provide notice on its website or its mobile device app of the type of personal information it collects from children and from failing to provide notice to parents of the types of information it collects from children and how it is used.[68]

Regulating geolocation tactics

Wireless carriers are governed by the Communications Act and the FCC's regulations; geo-fencing marketing that utilizes mobile carriers' networks will be affected by these laws.[69] The relevant laws require telecommunications companies to obtain opt-in consent before sharing geolocation or other personal information with third parties -- such as geo-fencing companies -- for marketing purposes. The type of consent required for a mobile carrier to share geolocation data with a geo-fencing company depends on whether the geo-fencing company is considered to be a carrier's affiliate or agent, or a carrier's joint venture partner or independent contractor.[70] Opt-in consent from subscribers is required if the geo-fencing company is a joint-venture partner or an independent contractor. Opt-out consent is required if the geo-fencing company is an affiliate or agent of the carrier.[71] The Communications Act defines an affiliate as "a person that (directly or indirectly) is owned or controlled by, or is under common ownership or control with another person."[72] Geo-fencing companies are likely to be deemed independent contractors of wireless carriers, requiring wireless carriers to obtain the opt-in consent of consumers before sharing their geolocation.

If a retailer and a geo-fencing company market to consumers via in-app advertising like banners and mobile display ads, they are not subject to laws requiring disclosure and consent. App developers may also get in on the action. Pandora's iPhone app targets ads for McDonald's to consumers using the app while near one of the restaurants (Figure 3).[73] As long as the ads consist of visual ads like banners or radio commercials, no privacy laws apply; if the ads are sent via text or multi-media message, the laws discussed below may apply.

Figure 3: McDonald's In-App Marketing on the Pandora Music App

Geo-fencing companies, retailers and carriers sending alerts to consumers via text are subject to CAN-SPAM

and the TCPA. CAN-SPAM requires opt-in consent from consumers in order to send them texts using a combination of their phone number and a domain name from a company on the FCC's list.[74] There are exceptions, however, for transactional messages or relationship messages such as receipts, warranties or account balances.[75] Messages that subscribers sign up for as a service provided by their mobile carrier may be deemed to be transactional or relationship messages, as they could be deemed "product updates… that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender."[76] SAGs do not have enforcement power over this provision of CAN-SPAM.[77]

The TCPA forbids automatically dialed or pre-recorded texts from being sent to wireless phones without express prior consent, even if there is an established business relationship between the sender and the recipient.[78] A text message that utilizes a domain name but is automatically dialed may be a violation of both CAN-SPAM and the TCPA.[79] SAGs have enforcement power over the TCPA.[80]

Conclusion

The dramatic growth of highly localized digital marketing enables precise targeting of individual children and teens -- in school, at the playground or near a store. Location-sensitive marketing incorporates information from users' profiles -- their offline and online interests, social relations, shopping behavior, entertainment interests and more. Teens are not covered by COPPA, and as their information and buying experiences are collected and analyzed for subsequent use, these young people become vulnerable to ongoing food marketing campaigns. Location-based mobile campaigns can be fully integrated with social media to create new ways for marketers to promote their products beyond individuals to their social networks. The rise of location marketing requires robust safeguards that protect the privacy and well-being of teens.

Endnotes

[1] Bryan Clark & Blaine Kimrey, *Litigating Mobile Marketing Claims,* 27 Comm. Lawyer 4, 4 (2010).
[2] Mobile Marketing Association, *Mobile Advertising Overview* (Jan. 2009), http://www.mmaglobal.com/bestpractice (under "Educational Documents" follow hyperlink "Mobile Advertising Overview" dated January 2009).
[3] Anton Troianovski, *Child's Play: Food Makers Hook Kids on Mobile Games,* Wall St. J., Sept. 17, 2012, 10:35 PM, http://online.wsj.com/article/SB10000872396390444812704577605263654758948.html.
[4] Mobile Marketing Association, *Mobile Advertising Overview* (Jan. 2009), http://www.mmaglobal.com/bestpractice (under "Educational Documents" follow hyperlink "Mobile Advertising Overview" dated January 2009).
[5] For example, the company Geoloqui provides location-based services including geo-fencing services. For more information visit https://geoloqi.com/.
[6] Aaron Smith, *Americans and Text Messaging: 31% of Text Message Users Prefer Texting to Voice Calls, and Young Adults Stand Out in Their Use of Text Messaging* (Sept. 19, 2011), http://pewinternet.org/~/media//Files/Reports/2011/Americans%20and%20Text%20Messaging.pdf; Amy Lenhart, *Teens, Smartphones, and Texting*, (March 19, 2012), http://www.pewinternet.org/~/media/Files/Reports/2012/PIP_Teens_Smartphones_and_Texting.pdf.
[7] Amy Lenhart, *Teens, Smartphones, and Texting*, (March 19, 2012), http://www.pewinternet.org/~/media/Files/Reports/2012/PIP_Teens_Smartphones_and_Texting.pdf; Press Release, Center for Digital Democracy, *Consumer Groups File FTC Complaint Against PepsiCo for "Deceptive and Unfair Digital Marketing Practices" Targeting Junk Food to Teens* (October 19, 2011), http://digitalads.org/sites/default/files/news-releases/digitalads_ftccomplaint_news_release_2011.pdf
[8] FTC Staff Report, Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.
[9] FTC Staff Report, Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf; Christian Levis, *Smartphone, Dumb Regulations; Mixed Signals in Mobile Privacy,* 22 Fordham Intell. Prop. Media & Ent. L.J. 191, 195 (2011).
[10] FTC Staff Report, Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.
[11] Mobile Marketing Association, *Mobile Advertising Overview* (Jan. 2009), http://www.mmaglobal.com/bestpractice (under "Educational Documents" follow hyperlink "Mobile Advertising Overview" dated January 2009).
[12] *Id.*
[13] FTC Staff Report, Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.
[14] Mobile Marketing Association, *Mobile Location Based Services Marketing Whitepaper* (Oct. 2011), http://www.mmaglobal.com/bestpractice (under "Educational Documents" follow hyperlink "Mobile Location Based Services Marketing Whitepaper dated Oct. 2011); *see also* the Network Advertising Initiative, Consumer Education website at http://www.networkadvertising.org/consumer-education.
[15] FTC Staff Report, Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (February 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.
[16] Alistair Goodman, Building Fences in the Sky: Geo-Fencing Has Arrived (Mar. 13, 2010), *available at* http://schedule.sxsw.com/2011/events/event_IAP6647.
[17] *Id.*
[18] *Id.*
[19] The company Bytelight provides indoor location services using interior lighting. For more information visit http://www.bytelight.com/.
[20] Nick Farina, *Meridian Goes to Aruba: Why WiFi Networks are the Future of Location Based Mobile*, Nick Farina News Post, (May 2013), http://nfarina.com/post/50427245962/meridian-goes-to-aruba-why-wifi-networks-are-the
[21] Laura O'Reilly, *Coke Unveils Plan to Reach 'Every Hand With a Mobile Phone'*, Marketing Week (Feb. 26, 2013), http://www.marketingweek.co.uk/news/coke-unveils-plan-to-reach-every-hand-with-a-mobile-phone/4005825.article).
[22] Atifa Silk, *Mobile Believer: Modelez's Bonin Bough*, Campaign Asia-Pacific (May 6, 2013).
[23] Press Release, Center for Digital Democracy, *Consumer Groups File FTC Complaint Against PepsiCo for "Deceptive and Unfair Digital Marketing Practices" Targeting Junk Food to Teens* (October 19, 2011), http://digitalads.org/sites/default/files/news-releases/digitalads_ftccomplaint_news_release_2011.pdf.
[24] Gavin O'Malley, *Tween Girls Susceptible to Mobile Advertising*, Mobile Marketing Daily (May 24, 2013, 3:23 PM), http://www.mediapost.com/publications/article/201140/tween-girls-susceptible-to-mobile-advertising.html?print#ixzz2Uc7XJMEu.
[25] Federal Trade Commission Act, 15 U.S.C. § 41-58 (2006); 47 U.S.C. § 151 (1996).
[26] 15 U.S.C. §45(a) (2006).
[27] *In re Connecticut Mobilecom,Inc. v. Cellco Partnership*, Nos. 02-1725 REG, 02-02519 WHP, 2003 WL 23021959 at *6-7 (S.D.N.Y. Dec. 23, 2003).
[28] *In re Connecticut Mobilecom,Inc. v. Cellco Partnership*, Nos. 02-1725 REG, 02-02519 WHP, 2003 WL 23021959 at *6-7 (S.D.N.Y. Dec. 23, 2003); *Holiday Magic, Inc. v. Warren,* 357 F. Supp. 20, 28 (E.D. Wis. 1973) (overruled on other grounds); *Weinberg v. Sprint Corp.*, 165 F.R.D. 431, 436 (D.N.J. 1996) (It is important to note that in cases involving issues such as rate-setting, interstate calling, and banking practices, FCC and FTC regulations may pre-empt state law); *People of State of Cal. v. F.C.C.,* 75 F.3d. 1350, 1359 (C.A. 1996), *Miller v. U.S. Bank of Washington*, *N.A.*, 865 P. 2d 536, 540-41(Wash. App.

Div. 1994).
[29] *Austin v. American General Finance, Inc.,* 900 F. Supp. 396, 399 (M.D. Ala. 1995).
[30] *Austin v. American General Finance, Inc.,* 900 F. Supp. 396, 399-400 (M.D. Ala. 1995); *Weinberg v. Sprint Corp.*, 165 F.R.D. 431, 436 (D.N.J. 1996).
[31] CAN-SPAM Act, 15 U.S.C. §§ 7701-7713 (2004); CAN-SPAM Rule, 16 C.F.R. § 316 (2008); FCC Wireless E-mail Rule, 47 C.F.R. § 64.3100 (2005);
[32] 15 U.S.C. § 7712(b) (2004); FCC Wireless E-mail Rule, 47 C.F.R. § 64.3100 (2005).
[33] Nancy King, *Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices,* 60 Fed. Comm. L. J. 229, 272-73 (2008).
[34] *Id.*
[35] 15 U.S.C. § 7712(b)(1) (2004); FCC Wireless E-mail Rule, 47 C.F.R. §§ 64.3100(c)(2) (2008); FCC Wireless E-mail Rule 47 C.F.R. §§ 64.3100(c) (8) (2008).
[36] Nancy King, *Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices,* 60 Fed. Comm. L. J. 229, 272-73 (2008).
[37] CAN-SPAM Act, 15 U.S.C. §§ 7701-7713 (2004); CAN-SPAM Rule, 16 C.F.R. Part 316 (2008).
[38] 15 U.S.C. § 7706(f)(1) (2004).
[39] *Id.*
[40] *Id.* (referencing § 7704(a) paragraphs 1, 2, 3, 4, and 5, and § 7706(d)).
[41] 15 U.S.C. § 7707(b) (2004).
[42] *See* Roger Allan Ford, Comment, Preemption of State Spam Laws by the Federal CAN-SPAM Act, 72 U. Chi. L. Rev. 355 (2005).
[43] Jonathon Pompan & Mikhia Hawkins, *Lead Generation through Mobile Marketing: Legal and Regulatory Realities* (Nov. 17, 2011), http://www.venable.com/lead-generation-through-mobile-marketing--legal-and-regulatory-realities-03-10-2011/; Telemarketing Consumer Fraud and Prevention Act, 15 U.S.C. § 6101(2012).
[44] Telemarketing Consumer Fraud and Prevention Act, 15 U.S.C. §§ 6101- 6108 (2012), 16 C.F.R. § 310 (2010)
[45] 16 C.F.R. § 310 (2010).
[46] Luis Salazar & Mitchell Brecher, *Jumping Into Mobile Marketing? Text: Caution!* 9 E-Commerce L. Rep. 1, 1 (2007).
[47] 47 U.S.C. § 227 (2010); TCPA Order, Rules and Regs. Implementing the Tel. Consumer Prot. Act. of 1991, *Rpt. and Order,* 18 F.C.C.R. 14014 (June 26, 2003), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-153A1.pdf.
[48] *See* Telemarketing Consumer Fraud and Prevention Act, 15 U.S.C. §§ 6101- 6108 (2012); 16 C.F.R. § 310 (2010)
[49] Nancy King, *Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices,* 60 Fed. Comm. L. J. 229, 309 (2008); Report and Order, *Rules and Regs. Implementing the Tel. Consumer Prot. Act. of 1991*, 18 F.C.C.R. 14014 (2003), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-153A1.pdf; 47 C.F.R. § 64.1200(e) (2008).
[50] Report and Order, *Rules and Regs. Implementing the Tel. Consumer Prot. Act. of 1991*, 18 F.C.C.R. 14014 (2003), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-153A1.pdf; *Satterfield v. Simon & Schuster, Inc.,* 569 F.3d 946, 954 (2009).
[51] 15 U.S.C. § 6103(2011).
[52] 15 U.S.C. § 6103(a) (2011); 16 C.F.R. § 310.7 (2012).
[53] 15 U.S.C. § 6103(f) (2011); Telemarketing Sales Rule, 16 C.F.R. § 310.7 (2012).
[54] 47 U.S.C. § 227 (2010).
[55] *TSA Stores, Inc. v. Dep't of Agric. & Consumer Services*, 957 So.2d 25, 30 (Fla. Dist. Ct. App. 2007).
[56] *TSA Stores, Inc. v. Dep't of Agric. & Consumer Services*, 957 So.2d 25, 31-32 (Fla. Dist. Ct. App. 2007), *quoting* 47 U.S.C. § 227 (f)(6) (2010).
[57] *Klein v. Vision Lab Telecommunications, Inc.*, 399 F.Supp.2d 528, 541-42 (S.D.N.Y. 2005), *Patriotic Veterans, Inc. v. Indiana ex rel. Zoeller,* 821 F.Supp.2d 1074, 1078 (S.D. Ind. 2011).
[58] Communications Act, 47 USCA § 222 (2001); Customer Proprietary Network Information 47 C.F.R. § 64.2001 et seq.
[59] Communications Act and corresponding FCC regulations require mobile carriers to protect consumer proprietary network information (CPNI). The Wireless Telecommunications Act added location information to the definition of CPNI in 1999. 47 U.S.C. § 609 (1999). The FCC's 2007 CPNI Order added requirements that carriers obtain advance consent from subscribers before allowing access or disclosing personal data to third parties for marketing purposes. Report and Order and Proposed Notice of Proposed RM, Fed. Commc'n Comm'n, 22 F.C.C.R. 6927, para. 4 (2007).
[60] *Carriers, System Makers Defend Location Protection*, 77 Telecommunications Reports 11 (May 15, 2011).
[61] FTC Staff Report, Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (February 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.
[62] Mobile Marketing Association, *Mobile Location Based Services Marketing Whitepaper* (Oct. 2011), http://www.mmaglobal.com/bestpractice (under "Educational Documents" follow hyperlink "Mobile Location Based Services Marketing Whitepaper dated Oct. 2011); Mobile Marketing Association, *Mobile Advertising Guidelines 5.0* (May 2011), http://www.mmaglobal.com/bestpractice (under "Guidelines and Best Practices" follow hyperlink "Mobile Advertising Guidelines 5.0" dated May 2011).
[63] CTIA The Wireless Association, *Best Practices and Guidelines for Location-Based Services*, (March 23, 2010), http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf.
[64] FTC Staff Report, Federal Trade Comm'n, *Behavioral Advertising: Tracking, Targeting, & Technology*, (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.
[65] FTC Staff Report, Federal Trade Comm'n, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing,* (Feb. 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.
[66] Alan S. Gutterman, *Changes to Children's Online Privacy*

Protection Act Go Into Effect on July 1, 2013, 6 Bus. Counselor Update 2 (2013).

[67] Consent Decree and Order for Injunction and Other Relief, *Chiesa v. 27x7 Dicgital, LLC*., No. 2:12-cv-03402, (D.N.J., June 26, 2012), *available at* http://www.nj.gov/oag/ca//press/6272012r.pdf.

[68] *Id.*

[69] 47 USCA § 222 (2001); 47 C.F.R. § 64.2001 (2012).

[70] Nancy King, *Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices,* 60 Fed. Comm. L. J. 229, 309 (2008); Telecomm. Carriers' Use of Customer Proprietary Network Info and Other Customer Info, *Rpt. And Order and Further Notice of Proposed RM,* 22 F.C.C.R. 6927 (2007).

[71] Telecomm. Carriers' Use of Customer Proprietary Network Info and Other Customer Info, *Rpt. And Order and Further Notice of Proposed RM,* 22 F.C.C.R. 6927 (2007), e*nforced, National Cable and Telecommunications Ass'n v. FCC*, 555 F.3d 996, 1003 (App. D.C. 2009).

[72] 47 U.S.C. § 153(2) (2010); 47 C.F.R § 64.2003(c) (2007).

[73] George Avalos, *'Geo-fencing' Mobile Apps that Watch You*, Oakland Tribune, Jan. 8, 2012, http://www.bendbulletin.com/article/20120108/NEWS0107/201080320/.

[74] 15 U.S.C. § 7712(b)(1) (2004); 47 C.F.R. § 64.3100(a)(2) (2005).

[75] 15 U.S.C. § 7712(b)(3) (2004); 47 C.F.R. § 64.3100(c)(8)

[76] 15 U.S.C. § 7712(b)(3) (2004); 47 C.F.R. § 64.3100(c)(8)(iii)(E) (2005); 16 C.F.R. § 316.3(c)(5).

[77] CAN-SPAM that grants SAGs enforcement power limits that power to the sections of the statute that impose requirements on transmission of messages to *computers*. 15 U.S.C. § 7706(f)(1)(2004). In CAN-SPAM, Congress granted the FCC the power to promulgate rules regulating wireless spam, which it did in 2005. 15 U.S.C. § 7712(b) (2004); 47 C.F.R. § 64.3100 (2005).

[78] 47 U.S.C. § 227(b)(1)(A)(iii) (2010); 47 C.F.R. § 64.1200(a)(1)(iii), (a)(2) (2012).

[79] *Joffe v. Acacia Mortgage Corp*., 121 P. 3d 831, 841 (Ariz. App. Ct. 2005).

[80] 47 U.S.C. § 227(e)(6)(2010), 47 U.S.C. § 227(g)(1) (2010).