Navigating the Legal Pitfalls of Augmented Reality

In the past year, augmented reality (AR) has moved beyond a sci-fi novelty to a credible marketing tool for brands and retailers. While part of a niche industry, AR applications are being championed by tech players like Google [1] and Nokia [2], and a host of mobile app developers have launched AR apps for the growing number of smartphones and portable computing devices. Tech analyst firm Juniper Research estimates that AR apps will generate close to $300 million [3] in global revenue next year.

The power of AR, particularly for marketers, is its ability to overlay highly relevant, timely and interactive data about specific products or services within a user's live physical environment. For example, companies are using AR to transform home or online shopping by bringing to life static, two-dimensional images -- see Ikea's 2013 catalog [4] and Phillips TV Buying Guide [5] mobile app -- or leveraging geolocational data to augment users' real-world retail experiences with instant data on pricing, reviews or special discounts (such as IBM's personal shopping assistant [6]).

If you're considering whether to add an AR app to your marketing mix, be aware that traditional advertising law principles still apply, and that both federal and state regulators are keeping a watchful eye on AR's potential impact on consumer privacy.

Traditional Advertising and Disclosure Rules Apply

A unique aspect of AR is that it allows retailers to give online or mobile shoppers a realistic, up-close, three-dimensional or enhanced view of their products prior to purchase (think virtual dressing rooms [7]). If your AR app is used to promote or

drive sales for a particular product, be sure to avoid overstating or exaggerating the features, functions or appearances of the product, or leaving out material information that could sway the consumer's purchasing decision.

In September, the Federal Trade Commission (FTC) published a marketing guide [8] for mobile app developers. It clarifies that long standing truth-in-advertising standards apply in the virtual world to the same extent as in the real world.

The key takeaway: Disclosures must be clear and conspicuous. That is, you should look at your app from the perspective of the average user and ensure that disclosures are big and clear enough so that users actually notice them and understand what they say. Another rule of thumb is to keep your disclosures short and simple, and use consistent language and design features within your app. Before launching your app, carefully consider how best to make necessary disclosures visible and accessible in the AR context.

You can expect more guidance on disclosures in the near future when the FTC releases its updated Dot Com Disclosures Guide [9].

Take Consumer Privacy Seriously

To unlock AR's full potential, developers are integrating the visual elements of AR with users' personal information, including geolocational and financial data, facial recognition information and users' social media contacts.

Given the increased scrutiny over mobile app privacy practices (see here [10] and here [11]), the following four recommendations should serve as the starting point for your privacy compliance analysis as you develop your AR app.

1. **Disclose your privacy practices.** As with advertising disclosures, privacy-focused disclosures must be clear and conspicuous, and they must be available before users download your app. In October, as part of an ongoing effort to improve privacy protections on mobile apps, the California Attorney General [12] notified a number of developers that their mobile apps did not comply with state privacy laws [13]. These laws require online operators that collect personal information to post a conspicuous privacy policy that is reasonably accessible to users prior to download. The developers have 30 days to comply or risk penalties of up to $2,500 for each time the non-compliant mobile app is downloaded.
2. **Obtain user consent before collecting location data.** An increasing number of AR apps tap into geolocation data to provide the user with real-time information about their surrounding physical environment. The FTC's guidance on mobile apps cautions developers to avoid collecting sensitive consumer data, such as precise location information, without first obtaining users' affirmative consent.
3. **Create a plan at the outset to limit potential privacy issues.** Companies like Viewdle [14], which was recently acquired by Google, are using facial recognition technology to enhance AR features used in mobile

gaming, social networking and social media. In October, the FTC issued a report on facial recognition technology [15] that includes the following best practices when collecting users' personal data: (1) collect only the personal data that you need, and retain it for only as long as you need it; (2) securely store the data that you retain, limit third-party access to a need-to-know basis and safely dispose of the data; and (3) tell users when their data may be used to link them to third-party information or publicly available sources.

4. **Be careful with children.** AR apps can be highly persuasive marketing tools, particularly with children, who may be unable to distinguish between the real and virtual worlds. Earlier this year, an FTC report [16] found that few mobile app targeted to kids included information on the apps' data collection practices. If you collect personal information from children under 13, you need to comply with the Children's Online Privacy Protection Act (COPPA), which requires companies to obtain verifiable consent from parents before they collect personal information from their children. Under an FTC proposal [17] now in review, "personal information" would include (1) location data emitted by a child's mobile device; and (2) persistent identifiers such as cookies, IP addresses and any unique device identifiers, unless this data is used only to support the internal operations of the app.

Have you interacted with AR apps? Do you have concerns about the technology's privacy and disclosure practices?

Read More [18]

November 21, 2012

Source URL (retrieved on *12/12/2013 - 8:04pm*):
http://www.wirelessdesignmag.com/news/2012/11/navigating-legal-pitfalls-augmented-reality?qt-blogs=0

Links:
[1] http://mashable.com/2012/06/28/brin-google-glass-2014/
[2] http://mashable.com/2012/09/05/nokia-city-lens/
[3] http://www.juniperresearch.com/viewpressrelease.php?pr=348
[4] http://mashable.com/2012/07/19/ikea-augmented-reality-catalog/
[5] http://www.youtube.com/watch?v=YBU0f0apgM0
[6] http://ibmresearchnews.blogspot.com/2012/06/your-personal-shopping-assistant.html
[7] http://mashable.com/2012/06/20/augmented-reality-retail/
[8] http://business.ftc.gov/documents/bus81-marketing-your-mobile-app
[9] http://www.ftc.gov/os/2000/05/0005dotcomstaffreport.pdf
[10] http://www.adlawaccess.com/2011/10/articles/privacy-and-information-securi/default-privacy-settings-of-mobile-app-draws-ftc-scrutiny/
[11] http://www.adlawaccess.com/2011/08/articles/privacy-and-information-

securi/ftc-settles-with-mobile-app-developer-over-alleged-privacy-violations/
[12] http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance
[13] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579
[14] http://viewdle.com/
[15] http://ftc.gov/os/2012/10/121022facialtechrpt.pdf
[16] http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf
[17] http://www.ftc.gov/os/2011/09/110915coppa.pdf
[18] http://mashable.com/2012/11/21/augmented-reality-advertising-privacy-law/