



## WHERE R U?

First, the Internet made the world flat. Location no longer mattered. You could find and purchase products around the world just as easily as ones in your hometown. Now with the advent of GPS chip and software technology that enables your smart phone to track your exact position, where you are located has once again become important to Internet entrepreneurs and marketers. Manufacturers of netbooks and laptops are adding similar location functionality to their products as well. With these new capabilities come new business opportunities, accompanied by some familiar concerns about privacy and security.

For instance, Loopt is a free social networking application that allows you to share your status and track the location of friends via smart phones such as the iPhone, BlackBerry, Google Android, and over 100 other mobile devices. Loopt has more than 1 million users. Loopt doesn't sell information to advertisers, but does post ads based on user location: its privacy policy allows it to disclose "some personally identifiable, registration, profile, or location information to subsidiaries, affiliated companies, or other businesses or persons ... in order to serve relevant advertisements." Loopt's target is to deal with advertisers at the walking level (within 200 to 250 meters).

Although the mobile advertising market is currently small (\$760 million), it is fast-growing (up 17% from last year and expected to grow to over \$3.3 billion by 2013), as more and more companies seek ways to exploit new databases of location-specific information. For example, in May 2009, Alcatel-Lucent announced a new service to be managed by 1020 Placecast that will identify cell phone users within a specified distance of an advertiser's nearest outlet and notify them of the outlet's address and phone number, perhaps including a link to a coupon or other promotion. 1020 Placecast's clients include Hyatt, FedEx and Avis Rent A Car. Burger King and Suburu have recently run trial campaigns using

Useful Networks' Store Finder application that allowed users to click a mobile banner ad to find the nearest store location. The trial showed that the location-enabled campaign significantly increased Store Finder conversion rates compared to users who had to manually enter zip codes to find locations.

While there's no denying the potential usefulness of such a service, the specter of "Big Brother"-like location tracking has privacy advocates raising the alarm. Privacy experts such as Lauren Gelman, executive director of Stanford Law School's Center for Internet and Society wonder, "How are we going to get all the benefits that come from doing geo-location without sacrificing people's privacy?"

To date, wireless location-based services remain largely unregulated. The Wireless Communications and Public Safety Act (often called the "911 Act") added the term "location" to the definition of customer proprietary network information (CPNI) held by telecommunication carriers, to make it eligible for certain privacy protections offered by the Communications Act of 1934. The 911 Act also required that the Federal Communications Commission (FCC) establish rules regarding how telecommunications carriers treat CPNI. The FCC did so in July 2002, adopting an approach that requires an individual's affirmative consent (opt-in) for some circumstances and assuming consent is granted unless an individual indicates otherwise (opt-out) in others.

The 2003 CAN-SPAM Act required the FCC to issue rules to protect wireless subscribers from unwanted mobile service commercial messages, and provides that consumers can list their cell phone numbers in the National Do Not Call Registry. In August 2004, the FCC proposed regulations, most of which went into effect in October 2004. The FCC prohibits sending wireless commercial e-mail messages unless the individual addressee has given the sender express prior authorization. The FCC also created a publicly available list of wireless domain

names list used for mobile service messaging so that senders of commercial mail could more easily determine which addresses are directed at mobile services. In 2009, the law was used to force three firms responsible for the infamous "car warranty" scam cell phone calls to cease and pay restitution to consumers.

Congress continues to debate how to protect wireless subscribers further, but thus far no laws have passed since CAN-SPAM in 2003. Europe and Japan, in contrast, have strong government privacy protection policies forbidding the use of location-based data without user consent, and there are strict limitations on selling the information to third parties. The wireless industry, mindful of the privacy issues raised in the online e-commerce context, has issued calls for stringent self-regulation in an attempt to avoid government-imposed regulation. In July 2008, the Mobile Marketing Association (MMA) adopted a global code of conduct for wireless marketing campaigns, broadening the scope of privacy guidelines it had previously issued for the United States. The code focuses on five basic tenets:

- Notice: Users should be informed of the marketer's identity and the purpose for which location information is being captured and used.
- Choice and consent: Opt-in consent should be obtained and a simple opt-out process provided.
- Customization and constraint: Customer data should be handled responsibly and only used

for the purpose of providing relevant and valuable services.

- Security: Sufficient security to protect consumer data from unauthorized third-party access and use, should be provided.
- Enforcement and accountability: MMA members are expected must comply with the code of conduct, and should self-certify that they are doing so.

In addition, some companies are offering technological solutions. For instance, WaveMarket provides a location aggregation platform called Veriplace that serves as middleware between mobile application developers and wireless carriers. The platform allows developers to access real-time user location data in their application. WaveMarket identifies the platform's "Privacy Engine" as one of its core features. The Privacy Engine allows end users full control over disclosure of their location. For instance, an end user can decide to share or not share location information based on days of the week or hours of the day, or to generalize location information from street-corner level to zip code or city level. End users can also view a history of all location requests, so they can always see who is trying to locate them. Whether consumers will actually use these capabilities to protect their location and other personal information is a question whose answer remains to be seen, however.

**SOURCES:** "MetaPlaces 09: Location-based Ads and Privacy," *TheWhereBusiness.com*, July 16, 2009; "Alcatel Gets Into Mobile Ads," by Sara Silver and Emily Steel, *Wall Street Journal*, May 21, 2009; "LBS Apps Drive Higher Accuracy; Advertisers Follow," by Thomas Hallauer, *TheWhereBusiness.com*, May 21, 2009; "Burger King, Subaru Trial Location-based Mobile Advertising," by Dan Butcher, *Mobile Marketer.com*, May 16, 2009; "WaveMarket's Joel Grossman Addresses Privacy and Location-based Advertising," by Joe Francica, *Directions Magazine*, May 13, 2009; "Cellphone Tracking Services: Friend Finder or Big Brother," by Michael B. Farrell, *Christian Science Monitor*, May 1, 2009; "Mobile Advertising and Usage," *eMarketer*, April 2009; "A Call to Legislate Internet Privacy," by Saul Hansell, *New York Times*, March 13, 2009; "Agency Skeptical of Internet Privacy Policies," by Saul Hansell, *New York Times*, February 13, 2009; "Wireless Communications: Voice and Data Privacy" and "When a Cell Phone Is More Than a Phone: Protecting Your Privacy in the Age of the Smartphone," Privacy Rights Clearinghouse, <http://www.privacyrights.org> (undated, accessed July 31, 2009).