

## Spies in Your Mobile Phone

Heather Green

*Consumer advocacy groups argue that mobile marketers are collecting personal data without enough disclosure*



Just as advertisers and wireless companies are hoping for the business of marketing on mobile phones to take off, consumer groups are raising pointed questions about the business practices of these companies. On Jan. 13, the Center for Digital Democracy (CDD) and the U.S. Public Interest Research Group (PIRG) filed a complaint with the Federal Trade Commission charging that wireless ad companies need to disclose more to their customers about what data are being collected about them and how those data are being used.

Mobile phones can provide a gold mine of data to marketers. The devices can pinpoint where a person is at any given time and trace any travels during the day. Mobile phones can also relay what kinds of restaurants a person looks for on her phone or which headlines are being read. "You're talking about a device that can identify an individual," says Jeff Chester, executive director of the CDD, a nonprofit group based in Washington. "It's carried with you wherever you go and raises the stakes in terms of consumer protection in the digital era."

Wireless marketers do have voluntary guidelines that require them to get a customer's consent—called "opt in"—before collecting data about them. In addition, the Federal Communications Commission ordered mobile marketers in 2007 to get opt-in consent from customers before carriers release information they collect to marketers. But the consumer groups argue that these permission clauses can be buried in the fine print of contracts that customers agree to when they sign up to get, for example, sports updates on their phones. Consumers may not understand that they're agreeing to hand over data about their tastes and location, and that the data information may be used for marketing. The consumer groups want these disclosures to be much more explicit, and they want the FTC to help consumers understand—through, say, public service campaigns—how targeting technologies can use the geographic location information gathered by marketers.

### Consumers Can Complain

Mike Wehrs is president of the Mobile Marketing Assn., the trade group that includes AT&T (T), Verizon (VZ), Vodafone (VOD), AOL (TWX), and Yahoo! (YHOO). He says the industry has taken proactive steps to protect privacy, such as creating consumer best-practices guidelines. Still, he agrees that as mobile marketing gets more sophisticated, the industry needs to do more. That's why the MMA is already discussing putting new programs for addressing privacy concerns and providing more disclosure, Wehrs says.

These include a complaint system that consumers will be able to use to report what they consider to be privacy violations. Standardized privacy guidelines would provide shorthand guides to different privacy policies. For example, when someone signs up to get weather updates, he might see a pop-up saying that the service uses Mobile Privacy Policy 1. A search online could show that that policy entails sharing location information. "We've behaved

responsibly, and we've tried to create a level of openness that consumers are comfortable with. There are an additional set of steps that we need to go forward with," Wehrs says.

The 52-page complaint filed by the consumer groups outlines ways mobile marketers collect information. Marketers can gather location data from a service that uses a global positioning system to help people stay in touch with their friends. Advertisers can collect behavioral or contextual information, such as social networks people visit or movie review services they use. Ad networks can compile gender and income provided by publishing partners or outside data partners such as Acxiom (ACXM), which projects income and education levels by analyzing Zip Codes.

### Targeting and Tracking Teens

The complaint focuses on mobile marketers, although it also criticizes the carriers, mobile-phone companies, and software makers. BusinessWeek obtained a copy of the complaint before its release and contacted some companies named in the complaint, including Verizon, AdMob, and Acuity Mobile. Verizon declined to comment without seeing the full complaint, and Acuity Mobile didn't return a request for comment.

AdMob, a mobile ad network, was one of several companies the consumer groups flagged as the most egregious marketers. The complaint argues that AdMob gathers data and targets teens without sufficiently warning mobile users that they're being tracked and providing a way to opt out. AdMob works with about 6,000 publishers, creating profiles of users within its network by collecting demographic data and registration data.

AdMob says the groups' findings are off base. The company says its profiles don't contain personal information, such as name, address, or phone number. "AdMob takes consumer privacy and protection very seriously and our policies are consistent with industry guidelines," says Ali Diab, AdMob's vice-president of product management. "That said, we do collect anonymized data that does allow us to deliver relevant ads to consumers. That's the only reason why we collect data."

### Carriers Have Lots of User Data

Carl Howe, an analyst at the research firm Yankee Group, says consumers are concerned about such marketing data because their wireless service providers already have lots of personal data about them. "People are very sensitive to the fact that telecom operators have quite a bit of information about you," Howe says. "Location is just one piece, but they also have credit history and addresses and phone numbers."

The carriers, though, are the most conservative in using data, analysts say. And while targeting is becoming more sophisticated, the amount of targeting is modest, says Andrew Frank, a Gartner (IT) analyst. "We don't have the volume [of usage] where a great deal of segmentation makes much sense," says Frank.

The CDD's Chester says that's exactly why the FTC should take a closer look at mobile targeting now. The agency was slow to pay attention to some targeted advertising practiced on the Internet, Chester says. Only in the past couple of years, through pressure from the European Union and privacy groups, have Internet companies put more stringent disclosure and data retention policies in place for behavioral and search data. "What I am saying to the commission is they have to look now and figure out what are reasonable consumer protections [for mobile advertising]," Chester says.

**Business Week, New York, 13 jan. 2009, Online Marketing, online. Disponível em <[www.businessweek.com](http://www.businessweek.com)>. Acesso em: 2 fev. 2009.**