THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor: Kirk J. Nahra, CIPP/US
April 2012 • Volume 12 • Number 3

Location-based services: Why Privacy "Dos and Don'ts" Matter

By Alysa Zeltzer Hutnik

2012 is certain to reflect U.S. consumers' continued love affair with sophisticated smart phones and mobile tablets. For many consumers, one of the driving forces in the popularity of these devices is their ability to run software and mobile applications (mobile apps) using wireless location-based services (LBS). With LBS-enabled services, individuals can share real-time and historical location information online--whether to facilitate a social interaction or event, play games, house-hunt or engage in many other activities. Among other benefits, these mobile services also can quickly enable consumers to locate proximate stores and restaurants, share their current location by "checking" themselves in at venues and navigate to a desired location.

But alongside the benefits, mobile LBS capabilities also involve consumer privacy risks. For example, the top perceived consumer risk of LBS-enabled services is the unintended revelation of a user's home address, and websites like "Please Rob Me" demonstrate the danger of location-sharing by providing a database of empty homes based on users' "check-ins" elsewhere. While these may be some of the more extreme examples, it is not uncommon for some LBS-enabled popular services to omit clear disclosures about the extent to which personal information is collected from the consumer and how it is used, and have a process that obtains informed consumer consent for such data collection. These are not "low risk" academic concerns but rather reflect practices that stand a good chance of inviting the scrutiny of federal regulators, including the Federal Trade Commission (FTC), as well as lawsuits by privacy litigants.

For businesses with an LBS-enabled service that want to avoid being a future legal target, it makes sense to take stock of existing business practices and to identify where updates may be appropriate in light of emerging legal "do's and don'ts." This article describes the rapid growth of the LBS-enabled mobile services market and associated privacy implications, and outlines practical guidance for entities that utilize LBS in their marketing practices.

Overview of the LBS market

LBS technology has become a mainstay in numerous products and services--from Facebook Places, which allows users to check themselves and their friends in at locations such as restaurants and bars, to Foursquare, a location-based social networking website that allows registered users to post their location at a venue and connect with friends. LBS applications can also be linked to existing social media platforms, allowing third-party developers to integrate LBS into their service. For example, The North Face and Sonic are leveraging location-tracking capabilities with ShopAlert, a service that will enhance a customer's shopping experience by providing a personal marketing message to a consumer entering or exiting the retail location. Other websites, like Groupon and Living Social, are testing real-time local

offers to users. The concept behind these marketing initiatives is to anticipate what users want based on location information trends.

The market possibilities for LBS are nearly unfathomable. LBS services are expected to generate $10 billion in revenue by 2016, with nearly half from LBS search advertising. Consumers are cautiously optimistic. A large percentage of consumers express discomfort with the concept of advertiser tracking--nearly three-quarters in one study--with a large majority preferring to have the ability to make a choice--whether opt in or opt out--of targeted mobile ads. Yet, a large percentage of consumers surveyed--52 percent--also expressed a willingness to let their usage patterns and personal information be tracked by advertisers if this resulted in lower product costs or free online content, and 43 percent of consumers said they were willing to receive targeted advertising in exchange for lower fees or service.

So the key question facing many LBS providers is how to strike the appropriate balance in meeting consumer demand in the provision of desired LBS-enabled services without overstepping privacy boundaries.

Do many existing LBS providers fall short on meeting consumer and legal expectations?

In February 2010, the Carnegie Mellon University studied the privacy controls of 89 popular LBS applications. Of those surveyed, only 66 percent had some form of privacy policy. The majority of those with privacy policies collected and saved all data; e.g., location, personal user profile information, and identifying web information such as IP address, for an indefinite amount of time. While 76 percent had some form of privacy controls, the majority of those controls were not easily accessible from the application's main page and were reached only after clicking through multiple screens.

In December, the reputable privacy certification organization, TRUSTe, reported that, of the top 100 U.S. websites, 97 percent had some form of privacy policy in place, though many companies had a "weak understanding" of their privacy policies and the third-party software used on their website. Notably, many companies reportedly did not understand the extent to which they collected personal data from consumers.

These figures at a minimum suggest that there is room for improvement on the privacy LBS front that would better meet consumers' expectations, as well as promote trust and confidence in businesses' privacy practices.

LBS privacy "Do's and Don'ts"

In addition to promoting consumer confidence and trust, adhering to emerging LBS best practices in privacy is likely to reduce the chance of facing an investigation by federal and state regulators, as well as lawsuits by private litigants. For example, the FTC, charged with consumer protection enforcement, has obtained 20-year settlements with numerous companies for engaging in deceptive or unfair practices by collecting personal information from consumers without appropriate disclosures and consent to such practices--including when personal information collection is set as a default--or for engaging in practices that differ from a business's privacy representations. The continued flurry of class-action lawsuits and media scrutiny regarding these types of practices also serve as a warning.

The bottom line: Even in the absence of black-letter law on LBS practices, there are some clear "dos and don'ts" that are worth considering when engaging in business practices involving LBS-enabled services.

A) Privacy on the back end: Due diligence in designing the LBS service

At a minimum, businesses should know what their LBS service does, what type of data it collects and whether that data is shared with affiliates, partners or third parties. Claiming ignorance as to the data flow of consumer location information is not likely to protect a business from privacy-related liability. Accordingly, consider carefully the intentional and unintentional data flows from LBS offerings. Is the data personally identifiable, either individually or when combined with other elements in the company's database? Will it be shared with an online advertiser or marketer or a social media platform like Facebook? Is there a legitimate business reason for the collection, disclosure and retention of such information? Understanding the data flows is the first step in protecting against a LBS privacy mishap.

In performing such due diligence, businesses also should appoint privacy-trained personnel to lead these efforts to ensure that privacy considerations are identified appropriately and satisfied, both at the outset of the design of a new service or product, as well as at periodic intervals after the service or product is released publicly. These are the core principles of the FTC's "privacy by design" guidance.

B) Privacy on the front end: Be transparent with users about LBS

Treat LBS information collection and disclosure as sensitive personal information, which means being transparent and careful with the data. This includes providing clear disclosures to consumers--before they download the LBS-enabled service--that explain what personal information will be collected, retained and shared; the consumers' choices as to such data collection, and how to exercise such choices; provide a periodic reminder to consumers when their location information is being shared, and if location information previously collected will be used for a new purpose, provide an updated disclosure to the consumer about the new use and an opportunity to exercise their choice as to that new use.

These disclosures should be presented prominently in plain language; i.e., not legalese or technical jargon.

C) Consent

While there can be some flexibility in how a business obtains a consumer's consent to the collection of LBS information, businesses generally bear the burden of demonstrating that they have obtained informed consent to the use or disclosure of location information before initiating an LBS service. Thus, it is not advisable to use pre-checked boxes or other default options that automatically opt users in to location information collection, or any other manner that ultimately leaves the consumer unaware of such data collection. The key is to clearly provide a disclosure about the location information collection, to clearly obtain consumers' consent to use their location information, and to keep accessible, organized business records of such disclosure and consent. It also is advisable to allow consumers to have the option of revoking consent previously given. (As additional guidance, the Center for Democracy and Technology, a consumer and technology advocacy organization, suggests an opt-out/opt-in choice framework: LBS providers should offer a persistent opt-out for first-party data collection and use, and obtain opt-in affirmative consent for the collection and use of sensitive information. The CDT also recommends that providers obtain opt-in consent for the default sharing of sensitive information with third parties.)

D) Sensitivity in LBS targeted to children and young adults

The use of mobile devices by children and young adults raises additional privacy and safety concerns. Indeed, a recent Carnegie Mellon study revealed that participants with children rated location-sharing technologies significantly more useful than those participants without children. That is to say, parents highly valued the check-in features of LBS-enabled applications but were also wary of risks associated with unsolicited advertising and unauthorized tracking by unwanted persons. Accordingly, it makes good

business sense to be sensitive to consumer expectations as well as the extra legal scrutiny that often follows any marketing efforts targeted to young people. Businesses also need to be mindful of whether they are collecting location information from children under the age of 13 and the corresponding legal obligations that may be triggered under the federal children's privacy statute, the Children's Online Privacy Protection Act. Navigating through these legal obligations with a privacy expert is critical to avoid mishaps.

E) Stay current on privacy developments and resources

One common complaint by many businesses is that they were unaware a particular business practice was considered to be unlawful--a complaint that is generally made after a regulator or litigant initiates legal action. A practical tip: In the sometimes murky area of consumer protection and privacy law, the "rules of the road" often are gleaned from analyzing cases and law enforcement examples and expert resources on best practices rather than clear restrictions set forth in a particular statute. For this reason, it makes good sense to periodically monitor (adlawaccess.com) law enforcement actions that are announced by the FTC and state attorneys general that highlight privacy-related practices to avoid, as well as guidelines issued by organizations that focus on LBS and privacy issues.

Conclusion

If there are any 2012 predictions with favorable odds, they include the continued growth of LBS-enabled services and the commensurate examples of law enforcement against companies that engage in LBS without accounting for privacy developments. While privacy investment is not inexpensive, proactively implementing best practices at the outset is far less costly than being singled out by regulators, litigants and the media after the fact for privacy mishaps.

Alysa Zeltzer Hutnik is a partner in the Privacy and Information Security practice at Kelley Drye & Warren LLP in Washington, DC. She counsels on high-level domestic and global privacy, data security and related consumer protection issues, including those involving emerging technologies such as mobile apps, gamification and social media.