Mashable

5 Privacy Tips for Location-Based Services

Alysa Z. Hutnik is a partner in the advertising law and privacy and information security practices at Kelley Drye & Warren LLP. Her co-author, Sharon K. Schiavetti, is an advertising and privacy associate at Kelley Drye & Warren LLP. Read more on Kelley Drye's advertising blog Ad Law Access or keep up with the group on Facebook or Twitter.

The year 2012 is certain to reflect U.S. consumers' continued love affair with sophisticated smartphones and tablets. One of the driving forces in the popularity of these devices is their ability to run mobile apps using wireless location-based services (LBS). Among other benefits, LBS allow access to 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.

However, with these benefits also come privacy risks. And it is not uncommon for some popular LBS-enabled tools to lack clear disclosure about personal information collection, how that data is used, and the process for consumer consent.

Failing to design a mobile app that covers these bases can be costly, inviting government investigations and lawsuits. For example, the U.S. Federal Trade Commission, which enforces consumer protection, has obtained 20-year settlements with numerous companies that engaged in deceptive or unfair practices by collecting personal information from consumers without appropriate disclosures or consent to such practices (including when personal information collection is set as a default). The commission has also targeted companies for engaging in practices that differ from their privacy standards. Furthermore, class action lawsuits and media scrutiny regarding these types of practices continue to serve as warnings.

LBS-based businesses that want to avoid becoming future legal or media targets need to take stock of existing business practices and identify where updates may be appropriate. Take a look at the following privacy LBS do's and don'ts.

1. Privacy by Design

At a minimum, a business should know what its LBS service does, what type of data it collects, and whether that data is shared with affiliates, partners or third parties. Claiming ignorance to the data flow of consumer location information is not likely to protect a business from privacy-related liability.

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, marketer or a social media platform like Facebook? Is there a legitimate business rationale for the collection, disclosure

This article originally appeared on Mashable.com.
Published: January 30, 2012

and retention of such information? Understanding the data flows is the first step in preventing an LBS privacy mishap.

When performing such due diligence, businesses also should appoint privacy-trained personnel to ensure that privacy considerations are identified 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 has been released publicly. These are the core principles of the FTC's "privacy by design" framework.

2. Transparency 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) which explain:

- What personal information will be collected, retained and shared.
- The consumer's choices as to such data collection.
- How to exercise such choices.
- Provide a periodic reminder to consumers when their location information is being shared.
- 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 her choice as to that new use.

These disclosures should be presented prominently, in concise and plain language (i.e. not legalese or technical jargon).

3. User Consent

There can be some flexibility in how a business obtains a consumer's consent to LBS information. That being said, a business generally bears the burden of demonstrating that it 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 location information, and to keep accessible, organized business records of such disclosure and consent. It also is advisable to allow consumers the option of revoking consent previously given.

This article originally appeared on Mashable.com.
Published: January 30, 2012

Mashable

4. Treat Children's Data as Sensitive

The use of mobile devices by children and young adults raises additional privacy and safety concerns. Therefore, be sensitive to consumer expectations on how to treat such data, as well as to the extra legal scrutiny that accompanies marketing efforts targeted to young people. A business also needs to be mindful whether it is 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 law (the Children's Online Privacy Protection Act). Navigating through these legal obligations with a privacy expert is critical to avoid mishaps.

5. Stay Current on Fast-Moving Privacy Developments

One common complaint by many a business is that it was unaware a particular business practice was considered 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, law enforcement examples and best practices, rather than from clear restrictions in a particular statute. For this reason, it makes good sense to periodically monitor law enforcement actions announced by the FTC and State Attorney General that highlight privacy-related practices, as well as guidelines issued by organizations that focus on LBS and privacy issues.

In 2012, we'll witness legal action against companies that engage in LBS without accounting for privacy developments. While privacy investment is not inexpensive, proactively implementing best privacy practices at the outset is far less costly than being singled out by regulators, litigants and the media after-the-fact.

This article originally appeared on Mashable.com.
Published: January 30, 2012