Best Practices and Guidelines for Location-Based Services

Version 2.0

Effective Date: March 23, 2010

CTIA's Best Practices and Guidelines for Location Based Services

TABLE OF CONTENTS

** The examples provided in the Guidelines are illustrative only and are not meant to indicate that LBS Providers must provide the features or services described in the examples.*

Section 1 - Purpose

CTIA Best Practices and Guidelines ("Guidelines") are intended to promote and protect user privacy as new and exciting Location-Based Services ("LBS") are developed and deployed. Location Based Services have one thing in common regardless of the underlying technology – they rely on, use or incorporate the location of a device to provide or enhance a service. Accordingly, the Guidelines are technology-neutral and apply regardless of the technology or mobile device used or the business model employed to provide LBS (e.g., a downloaded application, a web-based service, etc.).

The Guidelines primarily focus on the user whose location information is used or disclosed. It is the user whose privacy is most at risk if location information is misused or disclosed without authorization or knowledge. Because there are many potential participants who play some role in delivery of LBS to users (e.g., an application creator/provider, an aggregator of location information, a carrier providing network location information, etc.), the Guidelines adopt a user perspective to clearly identify which entity in the LBS value chain is obligated to comply with the Guidelines. Throughout the Guidelines, that entity is referred to as the LBS Provider.

The Guidelines rely on two fundamental principles: user notice and consent.

- First, LBS Providers must ensure that users receive meaningful notice about how location information will be used, disclosed and protected so that users can make informed decisions whether or not to use the LBS and thus will have control over their location information.

- Second, LBS Providers must ensure that users consent to the use or disclosure of location information, and LBS Providers bear the burden of demonstrating such consent. Users must have the right to revoke consent or terminate the LBS at any time.

Users should have confidence when obtaining an LBS from those LBS Providers that have adopted the Guidelines that their location information will be protected and used or disclosed only as described in LBS Provider notices. By receiving notice and providing consent consistent with these Guidelines, users will maintain control over their location information. The Guidelines encourage LBS Providers to develop and deploy new technology to empower users to exercise control over their location information and to find ways to deliver effective notice and obtain consent regardless of the device or technology used or business model employed.

Section 2 – Applicability

The Guidelines apply to LBS Providers. The following examples identify common situations and illustrate who is and is not an LBS Provider with obligations under the Guidelines.

Examples of LBS Providers:

Example 1. *A wireless carrier is the LBS Provider when it directly provides account holders or users an enhanced 411 LBS to locate nearby businesses.*

Example 2. *An application developer that provides the service for a downloadable LBS application (e.g., turn-by-turn driving) that is offered through an application storefront is the LBS Provider; a wireless carrier that provides user location information to that application developer for use in the LBS (e.g., through incidental assistance to the device's A-GPS or through other network data) is not an LBS Provider.*

Example 3. *A device manufacturer that pre-loads its own manufacturer-branded LBS application (e.g., a proprietary social networking application) is the LBS Provider; a device manufacturer that merely includes location enabled technology (e.g., A-GPS) on the device to support other applications and services, is not an LBS Provider.*

Example 4. *An entity that merely enables application providers to access location information from multiple wireless carriers (i.e., an aggregator) is not an LBS Provider, nor are the wireless carriers LBS Providers; instead, a party that uses an aggregator's data to make an LBS available to users is the LBS Provider.*

Example 5. *A wireless carrier that provides its customers "on-deck" access to a mapping service provided by a separate software developer is not the LBS Provider even if it provides the location information used by the third party; instead, the software developer is the LBS Provider.*

Caveat: The examples are illustrative only and do not imply that compliance with the Guidelines alone permits such uses or services. The terms on which access to location information is made available from wireless carriers to third parties, or the terms under which applications are made available to users, are beyond the scope of the Guidelines.

Section 3 – Scope of Coverage

The Guidelines apply whenever location information is linked by the LBS Provider to a specific device (e.g., linked by phone number, userID) or a specific person (e.g., linked by name or other unique identifier).

The Guidelines do not apply to location information used or disclosed:

- as authorized or required by applicable law (e.g., to respond to emergencies, E911, or legal process);
- to protect the rights and property of LBS Providers, users or other providers of location information;
- for testing or maintenance in the normal operation of any network or LBS; or
- in the form of aggregate or anonymous data.

Section 4 - Specific Guidelines

A. Notice

An important element of the Guidelines is *notice*. LBS Providers must ensure that potential users are informed about how their location information will be used, disclosed and protected so that they can make informed decisions whether or not to use the LBS, giving the user ultimate control over their location information.

The Guidelines do not dictate the form, placement, terminology used or manner of delivery of notices. LBS Providers may use written, electronic or oral notice so long as users have an opportunity to be fully informed of LBS Providers' information practices. Any notice must be provided in plain language and be understandable. It must not be misleading, and if combined with other terms or conditions, the LBS portion must be conspicuous.

If, after having obtained consent, LBS Providers want to use location information for a new or materially different purpose not disclosed in the original notice, they must provide users with further notice and obtain consent to the new or other use.

LBS Providers must inform users how long any location information will be retained, if at all. If it is not practicable to provide an exact retention period, because, for example, the retention period depends on particular circumstances, the LBS Provider may explain that to users when disclosing its retention policies.

LBS Providers that use location information to create aggregate or anonymous data by removing or permanently obscuring information that identifies a specific device or user must nevertheless provide notice of the use.

> **Example 6.** *An LBS Provider could create a dataset of mobile Internet users registered in a particular geographic or coverage area by removing or "hashing" information that identifies individual users from the dataset so that the LBS Provider could provide location-sensitive traffic management information or content to a highway safety organization. Notice that the LBS Provider creates or uses aggregate or anonymous data is required.*

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.