



**LOCATION PRIVACY
REQUIREMENTS
FOR
LOC-AID LBS DEVELOPERS**

VERSION 3.0

Updated: MARCH 2010

LOC-AID, the world's largest mobile location data gateway, has also built the most secure LBS location data exchange available today. Our patent-pending privacy protocols ensure that users decide how they wish to share personal information and location-based data for their devices.



March 2010

Dear Developer,

Thank you for choosing LOC-AID as your mobile location partner. LOC-AID is the largest location enabler in North America and Mexico, with access to over 200 million wireless subscribers. We've become the leading location enabler in the world because of two kinds of talented people. First, we serve developers like you who want deliver location based services to new, innovative mobile applications. And second, we serve the carriers, who agree to provide the location data you need to make your mobile applications "location-aware."

Our relationships with carriers are cherished. We've worked hard to establish network connectivity to the likes of AT&T, Bell Mobility, Rogers, Sprint, TelCel, TELUS and Verizon Wireless, among others. These carriers (and more to come) allow their location information to be utilized by mobile applications like yours because they trust LOC-AID and they trust you. Carriers trust you to respect all aspects of mobile subscriber privacy and preferences. Without this trust, the mobile location ecosystem would not exist.

To help you better understand how you can become a trusted developer in this mobile location ecosystem, we've published this LBS Developer Requirements document. You will note that these guidelines draw heavily from the latest *CTIA Best Practices and Guidelines for Location-Based Services*. While these read like guidelines, consider them to be LOC-AID requirements. By adhering to these privacy and authorization practices, your application will stand a better chance of being approved on our carrier networks. And a better chance of thriving.

Again, I thank you for taking the first step to location-enabling your application with LOC-AID. In the mobile marketplace, it really is all about "location, location, location." Which is why, at LOC-AID : Location Matters™.



Rip Gerber
President & CEO
LOC-AID Technologies, Inc.

Location, Privacy and LOC-AID

Privacy and security are paramount in LBS services. That’s why “lock” is part of our name at LOC-AID. Locking down privacy is not only core to our brand, it’s also our unwavering business practice. As the world’s largest location-enabling mobile transaction platform, we insist on the highest levels of privacy that exceed even the most rigorous industry guidelines.

LOC-AID has been recognized in the LBS industry for our excellence in privacy innovation. Our unique Privacy Vault™ approach to personal location information is unparalleled, and award-winning. We offer the most consistent, user-friendly privacy controls and security features for wireless operators and application developers. Every program we location-enable is 100 percent permission-based, with complete controls for the developers and their mobile customers.

We invite you to explore our Privacy procedures and our rigorous Location Privacy Policy. For further information, or to speak with one of our LBS privacy experts, please email us at sales@loc-aid.com.

CTIA Best Practices and Guidelines

This document draws heavily from the March 2010 *CTIA Best Practices and Guidelines* (“Guidelines”), which is 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



CTIA-The Wireless Association® is an international nonprofit membership organization that has represented the wireless communications industry since 1984. Membership in the association includes wireless carriers and their suppliers, as well as providers and manufacturers of wireless data services and products.

The association advocates on behalf of its members at all levels of government. CTIA also coordinates the industry’s voluntary efforts to provide consumers with a variety of choices and information regarding their wireless products and services. This includes the voluntary industry guidelines; programs that promote mobile device recycling and reusing; and wireless accessibility for individuals with disabilities.

CTIA also supports important industry initiatives such as Wireless AMBER Alerts; “On the Road, Off the Phone,” a teen-focused safe driving public service announcement campaign; text4baby, a free mobile educational service to promote the birth of healthy babies; and the “Get Wise About Wireless” program that equips parents and teachers with tips and tools to help students defeat digital bullies by practicing proper cell phone etiquette and safety behaviors.

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.). For the latest version of the CTIA Guidelines, visit: <http://www.ctia.org>

How to Use This Document

This document is intended for mobile developers and anyone, business or consumer, who may be interested in the privacy policies and practices concerning personal location information usage in mobile communications and applications. This document is written from a perspective that focuses on the mobile end user whose location information is used or disclosed. LOC-AID takes great care to focus all privacy discussions on the impact on the mobile end user, because in almost all cases, this mobile end user is a customer of a wireless service provider, or carrier.

In mobile application development, it is important to keep an "end user" perspective. This is especially true in the LBS industry. It is the user whose privacy is most at risk if location information is misused or disclosed without authorization or knowledge. Yours is not the only company providing services when a customer engages with your service, feature or application: there are many potential participants who play some role in delivery of LBS to users. These include at least three players: 1) you, the application creator/provider, 2) LOC-AID, the aggregator of location information, and 3) one or several wireless carriers, such as Sprint, who provide network location information.

You will note this document and the LOC-AID Privacy Vault™ and all LOC-AID privacy language adopts a user perspective to clearly identify which entity in the LBS value chain is obligated to comply to the LOC-AID Privacy Requirements. Ultimately, most of the responsibility for end user privacy falls on the responsibility of the mobile application developer.

Everything we do at LOC-AID regarding location enablement for mobile users follows two fundamental principles: user notice and user consent.

"Permission-Based Locations"

"Permission-Based Location," or PBL, is a new phrase in the mobile location industry. It was first used by LOC-AID back in 2005 to refer to an obvious issue arising from the intersection of the physical and mobile worlds. It goes without saying that asking permission and receiving permission is paramount to any product or service, especially in the online and mobile environments. The term "permission-based locations" is a term first coined by LOC-AID and is used in mobile development in general and LBS

services specifically. The undesirable opposite of permission-based locating is "stealth locating." Mobile developers must obtain permission to locate a mobile end user before requesting a location fix (or ping or dip) that delivers the latitude and longitude position of the end user's mobile device. For example, a mobile developer might ask permission to locate a user when activating a map feature on an iPhone. "Permission-based locations" are mostly used by mobile developers, notably smart phone application developers, as well as certain developers who want to locate many phones at once, as in the example of M2M (machine-to-machine) and fraud management applications.

"Permission-based locations" require that the mobile end user has either granted explicit permission to allow an application to locate his or her device (e.g., clicking a pop-up button to approve the processing a specific location request) or implicit permission (e.g. signing a contract or clicking an online agreement to subscribe a service). Permission can be granted via any number of means and media: a signed paper contract, an online email opt-in form, a website click-through agreement, a reply to an SMS message or by using a service which clearly states terms that include location usage.

To illustrate, consider someone who visits an online car dealership in hopes of buying a car, and provides their mobile number and consent to be notified if they are in the vicinity of a local dealership that has an available car in the make and model desired. The online car dealership has the mobile end user's permission to send a promotional message (SMS or email) if that interested buyer travels within the vicinity (e.g., geo-fence) of a dealership matching the car buyer's criteria. This practices follows "permission-based locations."

Over the years LOC-AID has learned that mobile applications find it is a more efficient to demand permission first because the location-based message or offers are only sent to people that are actually interested in location-enabled content and notifications.

LOC-AID Privacy Principle #1: Notice

It's common sense. But at LOC-AID, it is also formal practice: to be approved as a LOC-AID Developer Partner, you must agree to the LOC-AID Service Terms and Privacy Policies. Those documents are available at www.loc-aid.com. With regard to end user permissions and privacy, you must fully embrace the concept of USER NOTICE. LOC-AID Privacy Principle #1 is NOTICE. Simply put, you must ensure that your mobile end users receive meaningful notice about how location information will be used, disclosed and protected, so that mobile end users can make informed decisions whether or not to use the location-based services. This way, mobile end users have complete control over their location information.

LOC-AID Privacy Principle #2: Consent

However, simply providing notice of a location query is not enough. You must also be granted access, or permission. LOC-AID Privacy Principle #2 is CONSENT. You must ensure that your mobile end users consent to the use or disclosure of location information, and you, the application developer, bear the burden of demonstrating such consent. Mobile end users must have the right to revoke consent or terminate the your location-based service at any time.

Putting the End User in Control of Their Location Information

These requirements from LOC-AID are good business practice and common sense. Your mobile end users must have complete confidence when using your application or service that their personal location information will not be misused or improperly

*LOC-AID Privacy Principles #1 and #2
NOTICE and CONSENT.
By receiving notice and providing consent
consistent with these LOC-AID
requirements, mobile end users will
maintain control over their location
information.*

obtained. LOC-AID plays an important role in ensuring that mobile end user location rights are protected and enforced at all times. By adhering to the LOC-AID requirements in this document and as expressed in your LOC-AID Terms of Service, your end users will have additional comfort knowing that you have adopted LOC-AID's user-friendly requirements for governing location information, and that their

personal location information will be protected and used or disclosed only as described in the agreements they have executed with you and their designated service providers.

We welcome your feedback and comments as we continue to improve our policies and procedures. We want to encourage you to develop and deploy new technologies that empower your customers, while at the same time allowing your customers to exercise control over their location information. There are new and exciting ways to deliver effective notice and obtain consent regardless of the mobile device, wireless carrier or application technology, for both consumers and businesses. Some of our customers have launched innovative "permission locating" processes that we'd be happy to share with you.

Exclusions

There are some exceptions. In almost all cases, every LOC-AID Developer Partner must adhere to the LOC-AID Privacy Terms of Service and the LOC-AID Privacy Policy. If your application or service is requesting location information from a specific device, and you are obtaining the location by referencing a mobile phone number, customer reference number or other userID, or your using a specific person as the unique identifier, you will need to follow the LOC-AID policies to the fullest. In some cases, LOC-AID will consider exceptions to the standard Privacy Terms and Conditions, though these situations are rare. Examples include:

- as authorized or required by applicable law (e.g., to respond to emergencies, E911, or legal process);
- to protect the rights and property of a developer or LBS Provider, mobile end user 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.

What Kind of Notice Does LOC-AID Require?

By working with LOC-AID, you have access to the industry's most advanced privacy protection platform in the LBS industry. We take care of many of the aspects of mobile end user privacy, notifications and consent for you, the mobile developer. But it's important that you fully understand what we mean by notice.

Notice is more than just sending a confirmation message about a location request or status. On the LOC-AID platform, you must ensure that your existing and potential mobile end 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 location aspect of your application. This gives your mobile end user ultimate control over their location information.





Take the test: *"I'm just analyzing rush hour patterns. Do I have to notify users? Get user consent?"*

- must notify
- must get consent
- must do both
- neither is required

Answer: Let's say you want to create a dataset of mobile Internet users registered in a coverage area by removing or "hashing" information that identifies individual users. That way you could provide location-sensitive traffic information or content to a highway safety organization. In this case, you are using aggregate or anonymous data. But if you share that information with third parties, you must disclose what information will be provided and to what types of third parties so that mobile end users can understand what risks may be associated with such disclosures.

LOC-AID does not dictate the form, placement, terminology used or manner of delivery of notices. We do provide tools, and we can provide recommendations. You may use written, electronic or oral notice so long as mobile end users have an opportunity to be fully informed of your information practices. We'll check on you from time to time, even 'mystery shop' your application, to make sure you are following these requirements. 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 location (LBS) portion must be conspicuous.

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

Also, you must inform users how long any location information will be retained, if at all.

Did you pass the test above?¹ If you are using location information to create aggregate or anonymous data by removing or permanently obscuring information that identifies a specific device or user, you must nevertheless provide notice of the use.

What If My Users Want To Stop Location Queries?

Sometimes a customer may want to completely stop the location aspects of your mobile application, but keep the application running. That's fine. LOC-AID provides tools that allow end users to deactivate location requests in ways that do not interrupt their service. This is an important feature for many mobile users. But make sure your customers know how to do this (or we will help you do it). You must inform users how they may terminate the location requests and permissions, and the implications of doing so. You also must ensure that any privacy options or controls available to users to restrict use or disclosure of location information by or to others are explained to users.

¹ The answer to this test is "both."



Take the Test: You've developed a killer social networking service that includes a way for the users to establish permissions for when, where and to whom his or her location information will be disclosed. What do you need to include about **notice** in your user statement about this feature?

- edit location settings
- who can locate you
- what they can see
- all of the above

Answer: All. The notice to the user could include a statement to the effect:

“You control who will receive your location information. In ‘settings’ on the menu, you can select contacts you wish to block or enable all the time, or you can select a manual option to review a list of contacts each time you disclose your location.”

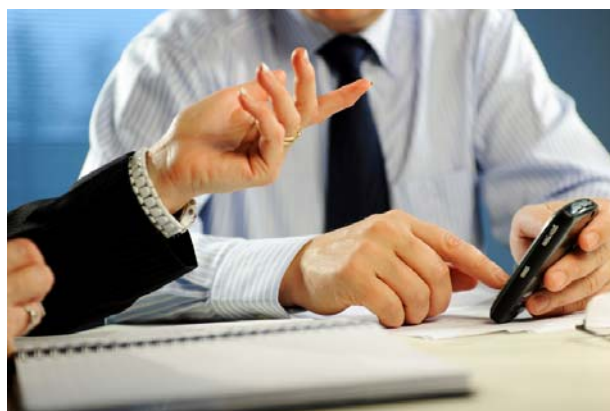
What About Periodic Reminders?

A great idea. LOC-AID offers reminder packages if you'd prefer us to send SMS reminders on your behalf. It is good practice to periodically remind your mobile end users when their location information may be shared with others and of the users' location privacy options, if any. The terminology used, timing and frequency of such notice depends on the nature of your application and brand. LOC-AID expects developers to send more reminders when the service involves frequent sharing of location information with third parties, and fewer reminders, if any, when the service involves one-time, user-initiated concierge service calls (e.g., locating a nearby service).

Do I Also Notify Account Holders?

Yes, in most cases. In some circumstances, account holders (as opposed to users) may control the installation and operation of the location-based service on the application. This is often the case in family accounts, or when mobile users are under a certain minimum age.

In addition to providing notice to the account holder, you still must ensure that notice is provided to each user or device that location information is being used by or disclosed to the account holder or others. Once again, the content, timing and frequency of such notice depends on the nature of your application and brand. LOC-AID can help you develop the notification messaging and frequency.



What Level of Consent Does LOC-AID Require?

LOC-AID Privacy Principle #2 is CONSENT. You must obtain mobile end user consent to the use or disclosure of location information before initiating a location query. Except in the circumstances described below where consent is obtained from account holders or business and the end users are informed of such use or disclosure, you must gain consent. But all consents are not created equal: the form of consent may vary with the type of service, but in all cases you must demonstrate and prove that you have legitimately and faithfully acquired end user consent for every location request you make. You, not the wireless carrier, bears the burden of establishing that consent to the use or disclosure of location information has been obtained before initiating a location fix.

As in the case of NOTICE, the LOC-AID privacy requirements do not dictate the form, placement, terminology used, or manner of obtaining consent as long as the consent is informed and based on notice consistent with the requirements set forth in the LOC-AID Terms of Service and Privacy Policies.

What Types Of Consent Are Acceptable?

Consent takes many forms. Here's a few:

- ✓ **Implicit Consent.** Consent may be implicit, such as when users request a service that obviously relies on the location of their device. Notice may be contained in the terms and conditions of service for a location-based service (LBS) to which users subscribe.
- ✓ **"Click Consent".** Your mobile end users may manifest consent to LBS terms and conditions electronically by clicking "I accept" on your website, in response to an email or SMS message or within your application.
- ✓ **Verbal Consent.** Another acceptable consent form can be acquired verbally by authorizing the disclosure to a customer service representative, through an IVR system or any other system reasonably calculated to confirm consent, so long as you retain documentation of the consent action.
- ✓ **Opt-In Consent.** Opt-in mechanisms must be explicit and actionable, as in the case of a single or double opt-in process. Pre-checked boxes that automatically opt users in to location information disclosure, or, choice mechanisms that are



It's OK to keep track of your employees. Let's say your application is used by businesses for managing field workers who are always on the go. You could satisfy your LOC-AID notice obligation by having the company give direct notice to each device that location information is being provided. Or, pursuant to a contractual obligation between you and the business, the employer could inform its workers that it will receive user location information.

buried within a lengthy privacy policy or a uniform licensing agreement ordinarily would be insufficient to express user consent.

When Would I Require Account Holder Consent?

Almost always. In some cases, where the actual user is different than the account holder, an account holder may control the installation and operation of LBS (e.g., business account holder utilizing LBS for fleet management; parental account holder providing phones for childrens’ use). Under these circumstances, the appropriate consent may be obtained solely from the account holder. As noted above, however, you still must ensure that notice is provided to each user or device that location information is being used by or disclosed to the account holder or others.

Can My End Users Revoke Their Consent?

Absolutely, and at any time. And you must make it easy for them to do it. You must allow users to revoke their prior consent to use or disclose location information to all or specified groups or persons. Where technically feasible, you may provide for selective termination or restriction of a location service upon account holder request. An account holder may revoke or terminate all or a portion of any users’ consent to location requests as well. But note that LOC-AID does not dictate terms of service that you must offer to users with regard to location services, nor do we dictate any technical implementation for terminating or restricting a location service on your application.

Account Holder Consent Examples:



Business Monitoring

A business buys your app to track employee locations to provide for rapid response repair service, just-in-time delivery, or fleet management.



Public Safety

You work with a public safety organization to provide monitoring compliance with terms of supervised release and house arrest, terms of bail for bondsmen, protecting public officials on duty, or military force movements.



Parental Controls

You offer a service to notify parents when a child arrives at or leaves a designated place.



Family Safety

You offers a family safety feature to locate family members in an emergency or other specified circumstances.

LOC-AID Information Security Requirements

Privacy and security fit together like a hand in glove at LOC-AID. We demand the highest levels of information and data security from its location developer partners. We must. The carriers do, and so should you. Therefore, you must employ reasonable administrative, physical and/or technical safeguards to protect a mobile end user's location information from unauthorized access, alteration, destruction, use or disclosure. You should use contractual measures when appropriate to protect the security, integrity and privacy of user location information.

Retention and Storage of Location Information

As a general policy, you should retain mobile end user location information only as long as business needs require, and then you must destroy or render unreadable such information on disposal. If it is necessary to retain location information for long-term use, where feasible, you should convert location information to aggregate or anonymized data.

Reporting Abuse

You should provide a resource for users to report abuse and provide a process that can address that abuse in a timely manner.



Compliance with Laws

You must comply with applicable laws regarding the use and disclosure of location information, and in particular, laws regarding the protection of minors. In addition, it is recommended that you comply with applicable industry best practices and model codes.

Location-Enablement Education

In addition to any notices required under these requirements, as a LOC-AID Location Development Partner you may be asked from time to time to undergo a certification process to confirm your understanding of LOC-AID privacy requirements. In addition, from time to time LOC-AID may announce various education campaigns to inform developers and their mobile end users regarding the responsible use of location-enabled applications and LBS

and the privacy and other risks associated with the disclosure of location information to unauthorized or unknown third parties. All entities² involved in the delivery of LBS, including wireless carriers, device manufacturers, operating system developers, application aggregators and storefront providers, should work to educate users about the location capabilities of the devices, systems, and applications they use as well as to inform them of the various privacy protections available.

Best Practices

LOC-AID is committed to the development, implementation and maintenance of responsible and meaningful privacy controls. We work closely with industry, developer and advocacy groups to develop policies, regulations, procedures and best practices for privacy and location management. LOC-AID sits on the CTIA's WIC Leadership Council. We actively helped craft the CTIA LBS Best Practices.



² LOC-AID thanks the CTIA and other members of the wireless industry in helping to create these location developer requirements. LOC-AID welcomes all input and review from LBS stakeholders on these policies. If you wish, you can provide relevant comments to Rip Gerber directly at rgerber@loc-aid.com.

Reference to the CTIA Guidelines is made throughout. Please note that revised 2010 Guidelines will be presented to the CTIA Board of Directors for their approval and adoption at the Board's March 23, 2010 meeting. Upon Board approval a final copy will be publically available on CTIA's Website. For further information please contact **Kate Kingberger, Director, Wireless Internet Development, CTIA – The Wireless Association**, 1400 16th St NW; Suite 600, Washington, DC 20036. E-mail: kkingberger@ctia.org

LOC-AID's Privacy Promise

We at LOC-AID thank you for your business, and your innovative mobile applications. Our business is to help you location-enable your application and your mobile business. For LOC-AID, Location Matters™.

Our business is all about helping you to be successful. We partner with wireless carriers and mobile developers in providing location-based services, and our Privacy Vault™ approach and security policies also apply to our partners, in every application we location-enable. LOC-AID provides location-based services through a network-based gateway with the world's largest and most respected carriers. Our gateway, the LOC-AID Xchange™, enables companies to locate mobile devices, but only with the corresponding permission-level approved for a particular application, campaign or query on the mobile device. These permission standards are rigorous and surpass all industry standards and internally-developed guidelines within the wireless carriers. Privacy levels in LBS services are driven by '3 Ps': the person, the purpose and the permission level.

In some cases, the company will secure a trusted relationship with a mobile user, whereby the end-user permission level, or opt-in provisioning, is acquired and managed directly by the developer, mobile content provider or mobile application company.

In other cases, the privacy levels are directly managed by the end user, the mobile consumer, on the device or through a website.

In ALL cases, LOC-AID ensures the highest levels of privacy are achieved and protected.

We encourage you to visit the respective wireless carrier websites in your market to learn more about mobile location privacy and security. LOC-AID has created a separate document for your easy reference: [LOC-AID CARRIER PARTNER PRIVACY NOTICES](#).



About LOC-AID Technologies

LOC-AID operates the world's largest mobile location data gateway and manages the most secure, privacy-protected platform for wireless providers including Verizon Wireless, Sprint, America Movil, TelCel, Bell Mobility, AT&T and TELUS. Based in San Francisco, CA, with offices across North America, LOC-AID simplifies and manages the complex technical and approval interfaces of location-based services (LBS) for mobile developers. LOC-AID also offers a portfolio of location-enablement services including geo-fencing, geo-coding, map appends and location analytics.

For more information, visit www.loc-aid.com

© 2010 LOC-AID Technologies, Inc.