



## Locaid® Privacy Policy for Location Aggregation Services

This Privacy Policy for Location Aggregation Services (“Policy”) and Frequently Asked Questions (“FAQs”) found on our website at [www.Locaid.com](http://www.Locaid.com) are incorporated by reference into our Terms of Use. Locaid operates as an aggregator for location based services by which it brings together – or operates as an information gateway for – wireless carriers (“Carriers”) and the providers of wireless applications and content (“Providers”). Locaid’s customers are businesses, not consumers.

Locaid provides location-based services through a network-based gateway with the world’s largest and most respected Carriers. Our gateway, called the Locaid Xchange Gateway™, 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.

Our location aggregation services obtain location information from multiple sources, but primarily from direct connections to Carrier network infrastructures.

### Benefits of Our Services

Our services benefit location-based service (“LBS”) software developers and providers by providing access to location data from multiple operators and other sources with a single business arrangement and single network connection.

Our services benefit Carriers by:

- 1) ensuring compliance with all applicable privacy laws, standards and regulations;
- 2) enforcing Carrier policies regarding provision and use of location information (for example, enforcing consistent terms and conditions of use, robust subscriber notices, opt-in verifications) and
- 3) helping to ensure efficient billings and timely invoice payments associated with location-based services.

Locaid transmits to LBS application providers the location data of individuals who purchase and use mobile location services (“Mobile Location Users”). We also allow LBS application developers and content providers to access to location information for subscribers across multiple Carrier platforms.

Thus, Locaid facilitates the support of many more location-enabled applications than any individual Carrier could support on its own. Without this kind of service, application providers would have to negotiate with and connect to each and every

Carrier, hindering rapid application deployment across a broad base of mobile users.

### Our Approach to Managing Privacy Protections

In addition to our own privacy and data protection policies, Locaid provides the services in full compliance with the legal and regulatory obligations that apply to our carrier partners, as well as generally accepted “best practices” developed by various industry organizations such as the Cellular Telecommunications and Internet Association (CTIA), an international nonprofit membership organization founded in 1984, representing all sectors of wireless communications – cellular, personal communication services and enhanced specialized mobile radio. This Policy describes our understanding of applicable legal and industry standards in the U.S. and EU.

### Our Commitment to Mobile User Privacy

Locaid’s permission standards are rigorous and are created and maintained with the intent to surpass all industry standards. The privacy levels upon which we insist are driven by “3 Ps:”

1. the person;
2. the purpose; and
3. the permission level.

There are two primary ways these permission standards work:

- a trust relationship is established with a Mobile Location User, whereby the User permission level, or opt-in provisioning, is acquired and managed directly by the software developer, mobile content provider or mobile application provider; or
- in other cases, the privacy levels are directly managed by the Mobile Location User, or that's User's designated representative, either the device or through a website.

In ALL cases, Locaid ensures the highest levels of privacy are achieved and protected.

Locaid is thoroughly familiar with applicable U.S. federal and state laws, as well as applicable foreign laws. In addition, Locaid is a member of leading associations that have developed industry best practices to protect mobile user privacy, including the Cellular Telecommunications and Internet Association (CTIA).

Locaid's privacy regime is comprised of three critical elements:

1. We have implemented a robust internal privacy and data security regime described in more detail below.
2. The strength of our privacy regime is based on our fundamental belief that protecting Mobile Location Users' privacy - and taking care to ensure that they are fully informed and aware of how information related to their use of LBS may be used with their consent—is critical.
3. Our privacy regime incorporates applicable U.S. and international legal requirements for protecting subscriber privacy with respect to location information. For example, Locaid is fully aware of, and complies to the extent applicable, with the Customer Proprietary Network Information ("CPNI") federal statute and accompanying Federal Communications Commission ("FCC") regulations.
4. Locaid contractually requires third-party LBS application providers to implement and enforce adequate privacy protections for subscriber location information and adhere to the requirements of Locaid's privacy regime.

## The Types of Personal Information We Obtain about Mobile Location Users

As explained above, when an Mobile Location User (an individual) purchases or subscribes to an LBS application, we provide location information to our LBS application partners through our mobile location gateway.

Locaid collects only the following data about Mobile Location Users:

- mobile number or alias code for mobile number;
- The x and y location coordinates related to a mobile number or code at a given time; and
- A date/time stamp related to the location of a particular mobile device.

## Disclosures of Location Information

There are only two circumstances under which Locaid discloses Mobile Location Users' location information:

- to an application provider for the specific LBS application the Mobile Location User purchased, subscribed to or authorized;
- to a public safety answering point, emergency or medical personnel or law enforcement personnel, as permitted or required by law.

## Notice and Consent Regime

Locaid contractually requires application developers and providers to fully inform Mobile Location Users about the nature and degree of the location-based service which the Mobile Location User has purchased, subscribed to, or has otherwise agreed to as a result of their contractual relationship with the application provider or developer, and the circumstances under which call location information, mobile telephone number(s) and any other personal data may be disclosed to third parties.

Although Locaid is not itself a Carrier subject to specific Carrier legal requirements, as a matter of best practice, we verify that the notice and consent regimes of our partners:

- are comprehensible and not misleading;
- are clearly legible, in sufficiently large type, and in an area/manner readily apparent to the Mobile Location User;
- explain that the Mobile Location User has the right, and the Carrier has the duty, to protect the confidentiality of CPNI, the



Get your Location API now at: <http://developer.loc-aid.com/getit>



Get your Location  
API now at: [http://  
developer.loc-aid.com/  
getit](http://developer.loc-aid.com/getit)

- Customer Proprietary Network Information;
- list the types of personal information (including location information and CPNI data as defined under U.S. law), the specific entities that will receive such data (after consent has been obtained), the purposes for which such data will be used, and sufficient information to enable the Mobile Location User to make an informed decision whether to permit the use or disclosure of, or to grant access to, his or her location information;
  - inform Mobile Location Users that they must affirmatively consent to allow for the requested usage, disclosure and/or access of his or her location information, after having been notified and informed of these rights;
  - indicate the steps the Mobile Location User must take in order to grant or deny access to location information;
  - indicate to the Mobile Location User that the denial of consent will not affect the provision of any services which he or she already receives.
  - be close to the solicitation for consent, and the statement of privacy rights to which the Mobile Location User is entitled under applicable FCC CPNI rules (for U.S. subscribers) or EU Directives and Member State laws (for EU subscribers);
  - state that any approval or denial of approval for the use of personal information in connection with the Location-Based Service (LBS) service will remain valid until the Mobile Location User affirmatively revokes or limits such approval or denial; and
  - provide regular reminders to Mobile Location Users that their personal data is being accessed and that consent may be suspended or withdrawn at any time.

### Certification and Training

Locaid will comply with any applicable certification requirements as set forth in the

FCC's CPNI rules.<sup>1</sup> In addition, Locaid will provide training to its personnel regarding the use and disclosure of personal data and CPNI and establish an "express disciplinary process" for the improper use and disclosure of personal data and/or CPNI.<sup>2</sup>

### Safeguarding Location Information – Data Protection and Security

Locaid ensures that data is protected and secure:

- We maintain location information data only so long as it is needed to provide services to the provider or until it is no longer needed to be retained for legal purposes;
- Except for the provision of location information to mobile application or content providers, we do not sell or share location information to anyone for any purpose;
- We implement encryption or other appropriate security controls to protect location information when stored or transmitted by Locaid; and
- We require non-Locaid companies, including service providers acting on our behalf, to protect all personal information they receive from us, in a manner consistent with this Policy.
- As a best practice and consistent with our adherence to FCC CPNI regulations for location information, we will notify subscribers if we become aware of a security breach resulting in unauthorized access to, use or disclosure of that subscriber's individually-identifiable CPNI (including subscriber mobile telephone numbers, email addresses and call location information).<sup>3</sup>
- We adhere to the Federal Trade Commission's ("FTC") baseline security requirements for the retention and handling of customer data.

In cases where U.S. state or federal laws or foreign laws require that individuals affected by data security breaches be notified, our LBS privacy and security regime will include the requisite notifications.

### Abuse of Location Tracking

Locaid will contractually require its location application partners to use technologies which allow users to turn location tracking on and off easily and to implement "double opt-in" measures (i.e., solicit consent at the time of subscription to a LBS, as well as at the beginning of a particular session). We will also require automatic log-out from the LBS application when the application session expires.

<sup>1</sup> 47 C.F.R. § 64.2009(e).

<sup>2</sup> Id. § 64.2009(b)-(c).

<sup>3</sup> 47 C.F.R. § 64.2011.

## Preventing Harm to Mobile Location Users

We understand that there is always a possibility for misuse of location information by persons with malicious intent - such as stalkers, predators, and those who engage in domestic violence. We will continue to work with our partners to identify best practices and policies to minimize such risks.

Likewise, we will work with Carriers to identify and prevent minor children from subscribing to services in accordance with a Carrier's policy. For example, a Carrier may have a policy that only the authorized account owner of record (for a family plan, for example) may opt-in or activate location services, thereby overriding any attempted "opt-in" by a minor child in possession of the mobile device.

## Changes to this Privacy Policy and Contacting Locaid

Locaid reserves the right to change this Policy at any time. If so, we will post the new Policy on our Web site.

Please visit our website at [www.Locaid.com](http://www.Locaid.com) for more information about our location data use practices. You can also email us at [privacy@Locaid.com](mailto:privacy@Locaid.com), or write to us at LOCAID Privacy Policy, 4 Embarcadero Center, Suite 1900, San Francisco, CA 94111.

For any questions about your service or account not related to privacy, please contact us at [cs@loc-aid.com](mailto:cs@loc-aid.com).



Get your Location API now at: <http://developer.loc-aid.com/getit>

## About Locaid

Locaid is the world's largest Location-as-a-Service (LaaS) company. We operate a location privacy platform that allows mobile developers to locate over 350 million devices for enterprise authentication, fraud management, consumer location services and opt-in mobile marketing. Locaid locates smartphones, feature phones, tablets and any mobile device on leading wireless carriers including América

Móvil, AT&T, Rogers, Sprint, T-Mobile and Verizon Wireless. Locaid also helps shape and enforce location privacy policies via leadership roles on governing associations including the CTIA, MMA and IAPP. The largest financial institutions, mobile marketers, M2M platforms and mobile service providers get network location from Locaid. Location Matters.™ You can locate us at <http://www.loc-aid.com>

