

Internet Draft  
Document: draft-cuellar-geopriv-scenarios-03.txt

J. Cuellar  
Siemens AG

J. Morris  
Center for Democracy & Technology

T. Kanai  
Fujitsu Laboratories

Expires in six months

Mar 2003

### Geopriv Scenarios and Use Cases

#### Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at  
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>.

#### Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

#### Abstract

This document describes location-based service scenarios for Geopriv. It complements the Geopriv Requirements document by providing a set of examples in which the Geopriv Location Object (LO) may be used. Thus this documents serves as a basis to discuss and analyze the security (authentication, authorization, integrity and confidentiality) and privacy issues and requirements associated with location-based services. To be useful, these scenarios include details of location computation, which helps to identify the entities involved on an abstract level and where privacy issues like control, consent, access, and security arise.

## Table of Contents

1. Overview.....	3
2. Conventions used in this document.....	4
3. Terminology.....	4
3.1. Foundational Definitions.....	4
3.1.1. Location Information (LI) and Sighting.....	4
3.1.2. The Location Object.....	5
3.1.3. Location Object vs. Using Protocol.....	6
3.1.4. Trusted vs. Non-trusted Data Flows.....	6
3.2. Geopriv Entities and Functions.....	7
3.2.1. Primary Geopriv Entities.....	7
3.2.2. Secondary Geopriv Entities.....	8
3.2.3. Geopriv Data Storage Functions.....	9
3.3. Privacy Rules.....	9
3.4. Identifiers, Authentication and Authorization.....	10
3.4.1. Identifiers.....	11
3.4.2. Authentication.....	11
3.4.3. Authorization.....	12
4. Three Frameworks to Classify Use Cases and Scenarios.....	12
4.1. Classifications "Push", "Pull", and "Translate/Query".....	13
4.1.1. Push Model.....	13
4.1.2. Pull Model.....	13
4.1.3. Translate/Query Model.....	14
4.2. Overlap of Geopriv Roles (Classif. A-1 through A-9).....	15
4.3. Initial Location Computation (Classif. B-1 through B-12).....	15
5. Services From a User Point of View.....	17
5.1. Network Management and Computer Services.....	18
5.1.1. Location Based Charging or Billing.....	18
5.1.2. Enhanced Call Routing.....	18
5.1.3. Ubiquitous computing applications.....	19
5.2. Emergency and Security Services.....	19
5.2.1. Emergency Call Services.....	19
5.2.2. Emergency Alert and other Public Safety Services.....	19
5.2.3. Evacuation navigation service.....	19
5.2.4. Location-based services to drivers.....	19
5.2.5. Tracking services for Security.....	20
5.3. Resource Management Services.....	20
5.3.1. Tracking services for Resource Management.....	20
5.3.2. Package Tracking.....	20
5.3.3. Taxi dispatch system - location of the customer.....	20
5.3.4. Taxi dispatch system - location of the taxi.....	21
5.4. Geographic Based Content Services.....	21
5.4.1. Navigation.....	21
5.4.2. City Sightseeing.....	22
5.4.3. Mobile Yellow Pages.....	22

5.4.4. Traffic Monitoring.....	22
5.4.5. Traffic jam information.....	22
5.5. Content Provider-Initiated Information Services.....	23
5.5.1. Location Dependent Content Broadcast.....	23
5.6. Entertainment and Community Services.....	23
5.6.1. Mobile Communities or Locate a Person.....	23
5.6.2. Gaming.....	23
5.6.3. Rendezvous service.....	23
6. Scenarios.....	23
6.1. Scenario 1.....	24
6.2. Scenario 2.....	24
6.3. Scenario 3.....	25
6.4. Scenario 4.....	26
6.5. Scenario 5.....	27
6.6. Scenario 6.....	28
6.7. Scenario 7.....	29
6.8. Scenario 8.....	31
7. Implications and Conclusions.....	32
8. Security Considerations.....	32
9. Acknowledgements.....	32
10. References.....	32
11. Author's Addresses.....	33
12. Full Copyright Statement.....	33

## 1. Overview

Location based systems are an emerging field, and all possible services or relationships cannot be identified or even imagined today. Over the next few years, location based services and applications are likely to come in a huge array of shapes, sizes, structures, paradigms, and approaches. This document attempts to articulate the range and types of applications that are possible using location services, although the use cases and scenarios below are unavoidably incomplete.

This document includes 4 main sections below. Section 3 contains terminology and definitions, largely drawn from the similar section in the Geopriv Requirements draft. Section 4 advances three different and incomplete (individually or collectively) analytical frameworks with which to consider Geopriv uses and scenarios. Section 5 lists, and briefly discusses, a range of possible use cases. Section 6 looks at a subset of these use cases diagrammatically, in an effort to identify the entities and data flows involved.

## 2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC-2119].

## 3. Terminology

The terminology and definitions detailed below include both (1) primary or essential terms used in the Requirements document, and (2) secondary terms that provide additional detail about the usage model envisioned for the Geopriv Location Object.

Most of the definitions below are drawn directly from the Requirements Document. The focus of that document, however, is on the requirements for the Geopriv Location Object. This document, in contrast, looks more broadly at Geopriv scenarios and data flows. It thus uses some additional terms not used in the Requirements Document. These additional terms are indicated by a "Not in Requirements Document" designation.

### 3.1. Foundational Definitions

#### 3.1.1. Location Information (LI) and Sighting

The focus of the Geopriv working group is on information about a Target's location that is NOT based on generally or publicly available sources, but instead on private information provided or created by a Target, a Target's Device, or a Target's network or service provider. Notwithstanding this focus on private location information, the Geopriv Location Object could certainly be used to convey location information from publicly available sources.

##### Location Information (LI):

A relatively specific way of describing where a Device is located.

In general, Location Information is (a) derived or computed from information generally not available to the general public (such as information mainly available to a network or service provider), (b) determined by a Device that may be not generally publicly addressable or accessible, or (c) input or otherwise provided by a Target.

As examples, LI could include (a) information calculated by triangulating on a wireless signal with respect to cell phone towers, (b) longitude and latitude information determined by a Device with GPS (global positioning satellite) capabilities, (c) information manually entered into a cell phone or laptop by a Target in response to a query, or (d) automatically delivered by some other IP protocol, such as at device configuration via DHCP.

Excluded from this definition is the determination of location information wholly without the knowledge or consent of the Target (or the Target's network or access service provider), based on generally available information such as an IP or e-mail address. In some cases information like IP address can enable someone to estimate (at least roughly) a location. Commercial services exist that offer to provide rough location information based on IP address. Currently, this type of location information is typically less precise and has a coarser granularity than the type of location information addressed in this document. Although this type of location computation still raises significant potential privacy and public Policy concerns, such scenarios are generally outside the scope of this document.

Within any given location-based transaction, the INITIAL determination of location (and thus the initial creation of Location Information) is termed a Sighting:

Sighting:

The initial determination of location based on non-public information (as discussed in the definition of Location Information), and the initial creation of Location Information.

Some variant of the sighting information is included in the Location Object. Abstractly, it consists of two separate data fields:

(Identifier, Location)

where Identifier is the identifier assigned to a Target being sighted, and Location is the current position of that Target being sighted. Not all entities may have access to exactly the same piece of sighting information. A sighting may be transformed to a new sighting pair:

(Identifier-1, Location-1)

before it is provided by a Location Generator or Location Server to another Location Recipient (for instance, another Location Server). In this case, Identifier-1 may be Pseudonym, and Location-1 may have less accuracy or granularity than the original value.

### 3.1.2. The Location Object

A main goal of the Geopriv working group is to define a Location Object (LO), to be used to convey both Location Information and basic privacy-protecting instructions:

Location Object (LO): This data contains the Location Information of the Target, and other fields including an identity or pseudonym of the Target, time information, core Privacy Rules, authenticators, etc. Most of the fields are optional, including the Location Information itself.

Nothing is said about the semantics of a missing field. For instance, a partially filled object MAY be understood implicitly as the request to complete it. Or, if no time information is included, this MAY implicitly mean "at the current time" or "at a very recent time", but it could be interpreted in a different way, depending on the context.

### 3.1.3. Location Object vs. Using Protocol

The security and privacy enhancing mechanisms used to protect the LO are of two types: First, the Location Object definition MUST include (optional) fields or mechanisms used to secure the LO as such. The LO MAY be secured, for example, using cryptographic checksums or encryption as part of the LO itself.

Second, the "using protocol" (that is, the protocol that uses the Location Object) may also provide security mechanisms to securely transport the Location Object.

The "using protocol" is the protocol that uses (creates, reads or modifies) the Location Object. A protocol that just transports the LO as a string of bits, without looking at them (like an IP storage protocol could do), is not a using protocol, but only a transport protocol. Nevertheless, the entity or protocol that caused the transport protocol to move the LO is responsible of the appropriate distribution, protection, usage, retention, and storage of the LO based on the rules that apply to that LO.

The security mechanisms of the Location Object itself are to be preferred. The using protocol has to obey the privacy and security instructions coded in the Location Object and in the corresponding Privacy Rules regarding the transmission and storage of the LO in order to ensure that the rules established by the Rule-Maker are observed. Other requirements on the using protocol are out of the scope of this document. <Open Issue: "One Message" Transfer Issue. The requirements discussed in this document do not preclude a single message/packet transmission of location, but this is not an explicit requirement>.

### 3.1.4. Trusted vs. Non-trusted Data Flows

Location information can be used in very different environments. In some cases the participants will have longstanding relationships, while in others participants may have discrete interactions with no prior contractual or other contact.

The different relationships raise different concerns for the implementation of Privacy Rules, including the need to communicate Privacy Rules. A public Rule Holder, for example, may be unnecessary in a trusted environment where more efficient methods of addressing privacy issues exist. The following terms distinguish between the two basic types of data flows:

**Trusted Data Flow:**

A data flow that is governed by a pre-existing contractual relationship that addresses location privacy.

**Non-trusted Data Flow:**

The data flow is not governed by a pre-existing contractual relationship that addresses location privacy.

### 3.2. Geopriv Entities and Functions

The entities of a Geopriv application or transaction may be given explicit roles:

#### 3.2.1. Primary Geopriv Entities

Certain entities and roles are involved in most (and in some cases all) Geopriv transactions:

**Target:**

The entity whose location is desired by the Location Recipient. In many cases the Target will be the human "user" of a Device or an object such as a vehicle or shipping container to which the Device is attached. In some instances the Target will be the Device itself.

**Device:**

The technical device the location of which is tracked as a proxy for the location of a Target.

A Device might, for example, be a cell phone, a Global Positioning Satellite (GPS) receiver, a laptop equipped with a wireless access Device, or a transmitter that emits a signal that can be tracked or located. In some situations, such as when a Target manually inputs location information (perhaps with a web browser), the Target is effectively performing the function of a Device.

**Rule Maker (RM):**

The individual or entity that has the authorization to set the applicable Privacy Rules for a potential Geopriv Target. In many cases this will be the owner of the Device, and in other cases this may be the user who is in possession of the Device. For example, parents may control what happens to the location information derived from a child's cell phone. A company, in contrast, may own and provide a cell phone to an employee but permit the employee to set the Privacy Rules.

**Location Recipient (LR):**

An individual or entity who seeks to receive location data about a Target.

A Location Recipient may act in one or more of the following more specialized roles: as the Location Generator, a Location Server, or as a Viewer:

**Location Generator (LG):** The LG is an element responsible for creating the Location Object for a specific Target. LGs publish Location Objects to Location Servers. The manner in which the Location Generator learns of Location Information is outside the scope of the Geopriv protocol.

**Location Server (LS):**  
The LS is an element that receives publications of Location Objects from Location Generators and may receive subscriptions from Location Recipients. The LS applies the rules (which it learns from the Rule Holder) to LOs it receives from LGs, and then notifies LRs of resulting LOs as necessary.

Some location tracking scenarios may involve a Target, Device, or Device user performing the function of a Location Server.

**Viewer (Viewer):**  
An individual or entity who receives location data about a Target and does not transmit the location information or information based on the Target's location (such as driving directions to or from the Target) to any party OTHER than the Target or the Rule Maker.

### 3.2.2. Secondary Geopriv Entities

Certain entities and functions are present or involved in only a subset of Geopriv transactions:

**Unintended Target [Not in Requirements Document]:**  
A person or object tracked by proximity to the Target. This special case most frequently occurs if the Target is not a person. For example, the Target may be a rental car equipped with a GPS Device, used to track car inventory. The rental company may not care about the driver's location, but the driver's privacy is implicitly affected. Geopriv may or may not protect or affect the privacy of Unintended Targets, but the impact on Unintended Targets should be acknowledged.

**Data Transporter:**  
An entity or network that receives and forwards data without processing or altering it. A Data Transporter could theoretically be involved in almost any transmission between a Device and a Location Server, a Location Server and a second Location Server, or a Location Server and a Viewer. Some location tracking scenarios may not involve a Data Transporter.

**Access Provider (AP):**  
The domain that provides the initial network access or other

data communications services essential for the operation of communications functions of the Device or computer equipment in which the Device operates. Often, the AP -- which will be a wireless carrier, an Internet Service Provider, or an internal corporate network -- contains the LG. Sometimes the AP has a "dumb" LG, one that transmits Geopriv LOs but does not use any part of the Geopriv Location Object. Other cases may not involve any AP, or the AP may only act as a Data Transporter.

Service Initiator [Not in Requirements Document]:

Entity that initiates the service and submits a request to disclose the Location Information to the Location Recipient. In most cases, this entity will overlap with one of the other Geopriv entities, such as the Target, the Rule Maker, or the Location Recipient.

### 3.2.3. Geopriv Data Storage Functions

Within the Geopriv framework, certain data may be stored in various functional entities:

Rule Holder (RH): The RH is an element that houses Privacy Rules for receiving, filtering and distributing Location Objects for specific Targets. A LS may query an RH for a set of rules, or rules may be pushed from the RH to an LS. The rules in the Rule Holder are populated by the Rule Maker.

Private Rule Holder [Not in Requirements Document]:

A non-public Rule Holder used to store private (authenticated, but not signed) or public (signed) Rules, identifiers, keys, and perhaps also requests. A Private Rule Holder could be operated by a Device, a Location Server, or a third party service provider.

Public Rule Holder [Not in Requirements Document]:

A public repository where signed Rules are stored.

Location Storage:

A Device or entity that stores raw or processed Location Information, such as a database, for any period of time longer than the duration necessary to complete an immediate transaction regarding the LI.

The existence and data storage practices of Location Storage is crucial to privacy considerations, because this may influence what Location Information could eventually be revealed (through later distribution, technical breach, or legal processes).

### 3.3. Privacy Rules

Privacy Rules are rules that regulate an entity's activities with respect to location and other information, including, but not limited to, the collection, use, disclosure, and retention of location information. Such rules are generally based on fair information practices, as detailed in (for example) the OECD Guidelines on the Protection of Privacy and Transporter Flows of Personal Data [OECD].

**Privacy Rule:**

A rule or set of rules that regulate an entity's activities with respect to location information, including the collection, use, disclosure, and retention of location information. In particular, the Rule describes how location information may be used by an entity and which transformed location information may be released to which entities under which conditions. Rules must be obeyed; they are not advisory.

A full set of Privacy Rules will likely include both rules that have only one possible technical meaning, and rules that will be affected by a locality's prevailing laws and customs. For example, a distribution rule of the form "my location can only be disclosed to the owner of such credentials and in such accuracy" has clear-cut implications for the protocol that uses the LO. But other rules, like retention or usage Rules, may have unclear technical consequences for the protocol or for the involved entities. For example, the precise scope of a retention rule stating "you may not store my location for more than 2 days" may in part turn on local laws or customs.

The Privacy Rules of the Rule Maker regarding the location of the Target may be accessible to a Location Server in Private or Public Rules Repositories, or they may be carried by the Location Object, or they may be presented by the Location Recipient as capabilities or tokens:

**Public Rule [Not in Requirements Document]:**

A Rule, digitally signed by the Rule Maker, and stored in a Rule Holder for the use of one or several Location Servers.

**Private Rule [Not in Requirements Document]:**

An authenticated Rule, consented by the Rule Maker, and stored in Private Rule Storage for the private use of a limited set of Location Servers.

**Geopriv Token [Not in Requirements Document]:**

A token or ticket issued and secured (authenticated or signed) by the Rule Maker to a Location Recipient, expressing the explicit consent of the Rule Maker to access his location information. This Geopriv Token is thus, logically, a rule of the Rule Maker.

### 3.4. Identifiers, Authentication and Authorization

This subsection introduces terms and concepts used in the Requirements Section.

### 3.4.1. Identifiers

Anonymity is the property of being not identifiable (within a set of subjects). Anonymity serves as the base case for privacy: without the ability to remain anonymous, individuals may be unable to control their own privacy. Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together. Unlinkability requires that entities are unable to determine whether the same user caused certain specific operations in the system. [ISO99]: A pseudonym is simply a bit string which is unique as ID and is suitable to be used for end-point authentication.

#### Unlinked Pseudonym:

A pseudonym where the linking between the pseudonym and its holder is, at least initially, not known to anybody with the possible exception of the holder himself or a trusted server of the user. See [Pfi01] (there the term is called Initially Unlinked Pseudonym)

The use of Unlinked Pseudonyms is necessary to obtain anonymity. But also it is necessary to change the used pseudonyms regularly, because identifying the user behind an unlinked pseudonym can be very simple.

In order to remain anonymous, an entity may use private identifiers. Private identifiers convey less information than public identities, because they are meaningful to a smaller number of entities and in use for a shorter duration. Thus if A discloses a private identifier to B, B is less likely to associate this information with a known individual or entity than if a public identifier was disclosed.

#### Short-lived Identifier [Not in Requirements Document]:

An identifier that is used only for one or a limited number of "sessions".

Using protocols should be able to handle LOs with identifiers, LOs without identifiers, and LOs with pseudonyms. The identity of the requester may be irrelevant in some cases, whereas the identity of the Target may be irrelevant in others.

#### Entity-Identifier [Not in Requirements Document]:

The names used by the Geopriv entities to identify, authenticate or authorize themselves to other entities. Rules also use entity-identifiers to express which Location Recipients may receive which transformed sighting information.

### 3.4.2. Authentication

The word authentication is used in different meanings. Some assert that authentication associates an entity with a more or less well-known identity. This basically means that if A authenticates another entity B as being "id-B", then the label "id-B" is not a pseudonym, but a persistent or at least linkable identity of the entity. In this case, the label "id-B" is called a publicly known identifier, and the authentication is "explicit":

#### Explicit Authentication:

The act of verifying a claimed identity as the sole originator of a message (message authentication) or as the end-point of a channel (entity authentication). Moreover, this identity is easily linked back to the real identity of the entity in question, for instance being a pre-existing static label from a predefined name space (telephone number, name, etc.).

### 3.4.3. Authorization

#### Authorization

The act of determining if a particular right, such as access to some resource, can be granted to the presenter of a particular credential.

Depending on the type of credential, authorization may imply Explicit Authentication or not.

## 4. Three Frameworks to Classify Use Cases and Scenarios

There are many different ways to conceptualize or classify the possible Geopriv scenarios. Among the possible approaches can be:

- A. How is the location information transaction being triggered: is it a "push" or a "pull" model, or a "query" to translate a location or find a location in a context?
- B. What are the relevant entities, devices, and roles, and how do they interrelate and (often) overlap?
- C. What entity first has control over the initial sighted data, and over the initial computation and distribution of the location information?

These three classifications are discussed briefly in this section.

A fourth approach to considering the full range of possible Geopriv scenarios is to analyze the use cases from the user's perspective, looking at what service is being provided from the point of view of the user. A range of these use cases are described in Section 5, with references back to the three classification schemes discussed in this section.

None of these classifications alone is fully sufficient to identify the full range of possible location services. Other ways to consider the possible uses and scenarios are discussed in Section 7.

#### 4.1. Classifications "Push", "Pull", and "Translate/Query"

One classification of scenarios is according to who is the Service Initiator and whether the service triggering is done on demand or on subscription mode, and if the Rule Maker is granted positioning consent or not. A Target, Rule Maker, Location Recipient, or another party may trigger the actions, depending on the service being provided. They may be triggered on demand or as a periodical subscription (periodical updates). Also it is possible for location services to support conditional positioning. Under these conditions, an application that is granted conditional positioning authorization must notify and obtain positioning authorization from the Rule Maker of the Target prior to performing the positioning process. The Rule Maker is able to accept or reject the positioning attempt.

In Japan for instance, all major mobile carriers provide the following types of well-known commercial services:

1. "Here I am!" (Subscribers may send their location information to other subscribers or to Internet users via e-mail or other means.)
2. "Where is he/she?" (Carriers tell users where someone is located.)
3. "Where am I?" service (Carriers tell subscribers where they are located on a map.)

Those three correspond roughly to 3 query modes described below: Push Model, Pull Model, and Translate/Query Model. Note that many scenarios will involve both Push and Translate, or both Pull and Translate.

##### 4.1.1. Push Model

In the Push Model, the Target typically acts as the Location Initiator (instead of responding to a request). For example, after locating himself, the Target may send his location to the Viewer or another Location Recipient. Similarly, the Target may ask a Location Generator to locate the Target and transmit the location to a Viewer or other Location Recipient.

##### 4.1.2. Pull Model

In the Pull Model, a Viewer or other Location Recipient wants to know where a given Target is, and thus is the Service Initiator. As one example of the Pull Model, a Location Server:

1. receives Location Information from the Location Generator or from another Location Server,
2. receives, directly or through a repository or a trusted third party, the Privacy Rules associated with the Target,
3. accepts services requests from Location Recipients (including other Location Servers),
4. matches the location request to the Rules for the Target and processes the Location Information accordingly, and
5. returns Location Information (sometimes filtered) of the Target.

#### 4.1.3. Translate/Query Model

Those are services where some entity (such as a Target or other Location Recipient) provides Location Information and obtains a function of that information as response. For instance, he may want to translate a location from one format to another (say from coordinates to civil), or to see in a map where certain coordinates are, or given the distance from a point to 2 or more fixed locations, to find the possible locations of the point.

This service may be invoked by a mobile Target that knows where he is, or where he plans to be this afternoon, but needs additional information about the location or needs the location in a different format.

In one example, a Target knows his location (say, using a GPS chip), but not in the form that he needs it (say, as a street address). In this case, the Target asks an external Location Server to translate the information to a street address or position on a map. The Location Server obtains the location from the Location Generator (which is the Target itself), converts the Location Information to the requested form, and sends it back to the Location Recipient (also the Target).

## 4.2. Overlap of Geopriv Roles (Classif. A-1 through A-9).

In many Geopriv scenarios the different entities can overlap. Sometimes a Device is a proxy for a Target, and sometimes the Device is the Target. In some cases, the Rule Maker and the Target are the same individual or entity; in other cases, they are different. If the Target/Device knows his location (through GPS, for example), the Target/Device may also be the Location Generator. If the Target's Device has the capabilities and bandwidth, that Device may serve as the Location Server, or may rely on an external Location Server.

The following is an admittedly incomplete breakdown of different overlaps among the Geopriv roles (where LS stands for Location Server, LG for Location Generator, and Sinitiator for Service Initiator):

A-1: LS = RM = Target = LG / Viewer = SInitiator  
 A-2: LS = RM = Target / LG / Viewer = Sinitiator  
 A-3: LS / RM = Target = LG = Viewer = SInitiator  
 A-4: LS / RM = Target = LG / Viewer = SInitiator  
 A-5: LS / RM = Target / LG / Viewer = SInitiator  
 A-6: LS / RM / Target / LG / Viewer / SInitiator  
 A-7: LS / RM = Viewer = SInitiator / Target = LG  
 A-8: LS = RM = Target = SInitiator / LG / Viewer  
 A-9: LS = LG / RM = SInitiator / Target = Viewer

For instance in group A-1 there are 2 physical entities (one entity is the Location Server, Rule Maker, Target and Location Generator, while the other entity has the roles of Viewer and Service Initiator). In A-5 there are 4 different physical entities (only the Rule Maker and the Target are the same). The A-6 group has different entities playing the 6 roles.

Where possible in the use cases and scenarios in Sections 5 and 6 below, the classifications A-1 through A-9 will be given for each use case or scenario.

## 4.3. Initial Location Computation (Classif. B-1 through B-12)

The location computation process contains two steps: 1) obtaining raw data about the Target's location, and 2) deriving or computing the Target's location using this raw data. One example of such a location computation process is signal triangulation. The raw data (Step 1) includes the direction a cell phone is from certain cell towers and where those cell towers are located. Given this information, one can compute the cell phone's location (Step 2).

Thus two important questions raised by the initial location computation scenarios are (a) which entity has control over the raw data, and (b) the site of the location computation. On the first question (who has control over the raw data), there are two main

likely answers: the Target's Device or the Target's (wired or wireless) Access Provider (AP). In this framework, if the Target cannot control the dissemination of the raw data (such as with a cell phone that transmits information from a GPS chip to the wireless carrier without regard to the user's preferences), then the correct value would be the AP.

For the second question (the site of the initial location computation), there are three main likely answers: the Target's Device, the AP of the Target's Device, or a third party who is neither the Target nor the AP.

In considering the use cases and scenarios set out later in this document, it is important to consider which entities have access to the raw data, to ensure that those entities comply with the relevant Privacy Rules.

In addition to the two questions raised in this classification, there is value in noting a third question: whether the scenario involves a Device (and Target) that are mobile or fixed. Although in many (perhaps most) the functioning of the Geopriv Location Object will not depend on whether a scenario is fixed or mobile, in considering the scenarios it is instructive to acknowledge the existence of the fixed scenarios.

The three questions and their possible values yield a total of 12 basic scenarios, as illustrated below:

mobility	- mobility of the Device
raw data	- who controls or has access to raw location data
computation	- who performs the location computation
AP	- Access Provider for the Target's Device
Target	- the Target or the Target's Device
>	- direction of raw data flow
>>	- direction of processed location data flow

[Class]	[mobility]	[raw data]	[computation]
B-1	fixed	target -->+--	target ----->>
B-2	fixed		+-- AP ----->>
B-3	fixed		+-- third party -->>
B-4	fixed	AP ----->+--	target ----->>
B-5	fixed		+-- AP ----->>
B-6	fixed		+-- third party -->>
B-7	mobile	target -->+--	target ----->>
B-8	mobile		+-- AP ----->>
B-9	mobile		+-- third party -->>
B-10	mobile	AP ----->+--	target ----->>
B-11	mobile		+-- AP ----->>
B-12	mobile		+-- third party -->>

In general, classifications B-1 through B-6 could apply in any use case or scenario involving a fixed location, and B-7 through B-12 could apply whenever a mobile location is involved. Thus, these classifications are not useful for distinguishing between different use cases and scenarios.

Instead, these classifications are important to consider when assessing the security and privacy of the initial stages of any Geopriv transaction. In designing the Geopriv protocol, it is important that it be effective in all of these cases under this classification scheme.

## 5. Services From a User Point of View

There is a huge diversity of possible location based services that may be offered. This section describes a sample of the possible location services, grouping them into rough and somewhat arbitrary categories. Many of the services listed below will be commercial services offered by network access providers or third parties.

Where possible, the most appropriate classification designations from Section 4 above are offered for each use case. In some cases, the classifications offered are not the only possible classification for

the service. <Note: This classification is significantly incomplete in this draft.>

## 5.1. Network Management and Computer Services

Most wireless service providers (which act as the Access Providers in the Geopriv context) already use extensive location based services for internal operations, such as location assisted handover, traffic and coverage measurement, O&M related tasks, network planning, network QoS improvements, improved radio resource management, etc. Assuming that the information is entirely internal within a single network, privacy implications are likely governed by laws or contract, and many of the location services would be outside of the scope of Geopriv.

### 5.1.1. Location Based Charging or Billing

This location based service can be used to charge users (for example, for wireless access) depending on their location. Different rates may be applied at country clubs, golf courses, or shopping malls. This service may apply also for instance to business groups, which obtain preferential rates within corporate campuses. In many cases, subscribers should be notified of the zone or billing rate currently applicable, and be notified when the rate changes. Depending on implementation, this type of service may or may not come within the scope of Geopriv.

This service could arise with either the Push or Pull Models, and most likely in classifications A-1, 2, 4, 5, or 8.

### 5.1.2. Enhanced Call Routing

This service allows user calls to be routed to the closest service client based on the location of the originating and terminating point of the call. The user may for instance dial a feature or service code to invoke the service (\*GAS for closest gas station, etc). ECR services may be offered, for example, through menu driven access that allows users to interactively select from a variety of services.

If the implementation of the location based aspects of this service is entirely within a single wireless network provider, then this service may not utilize Geopriv. Even within one network, however, Geopriv may offer an effective way to implement this type of service. Similar forms of this service offered by third parties are discussed below.

This service could arise with either the Push or Pull Models, and most likely in classification A-8.

### 5.1.3. Ubiquitous computing applications

The determination of access to bandwidth, devices and information sources and sinks can utilize location information. The location can provide information about the devices that are available to the user, which allows determination of what will be an effective means of communicating with him/her.

This service could arise with either the Push or Pull Models, and most likely in classification A-8.

## 5.2. Emergency and Security Services

### 5.2.1. Emergency Call Services

This location based service supplies location information to an emergency service provider to assist them in their response. This service is mandatory in some jurisdictions, for instance in the United States for mobile voice providers (E911 service).

This service could arise with either the Push or Pull Models, and conceivably in almost any of the classifications A-1 through A-9.

### 5.2.2. Emergency Alert and other Public Safety Services

Emergency Alert Services are used to notify subscribers within a specific geographic location of emergency alerts, including tornado or flooding warnings, evacuation instructions, police information broadcast, etc.

This service could arise with either the Push or Pull Models, and conceivably in almost any of the classifications A-1 through A-9.

### 5.2.3. Evacuation navigation service

In case of an emergency in a hotel, such as fire, the hotel initiates a navigation service to tell its customers about the evacuation routes. Each room has a mobile Device, similar to a PDA, with positioning functionality. A customer leaves his room along with the PDA. The system obtains customer's current location through the PDA and displays the safest evacuation route on it. The hotel is the Service Initiator, and both the Target and Viewer are the Device.

This service could arise with either the Push or Pull Models, and most likely in classification A-9.

### 5.2.4. Location-based services to drivers

Assistance for vehicle breakdown (Emergency Roadside Service) and personalized information on traffic conditions. This service may be

used in complement to an enhanced call routing service, which calls the nearest Emergency Roadside Service of a certain type and delivers the location information of the Target to the Roadside Service. This could be used for the purpose of dispatching service agents.

This service could arise with either the Push or Pull Models, and most likely in classification A-8.

#### 5.2.5. Tracking services for Security

The Rule Maker wants to protect his car with a location provider anti-theft device or to track the position of his children (or a pet). The network may provide the last known location and timestamp. If information is unavailable in real-time, a reason may be provided.

This service could arise most likely under the Pull Model, but most probably under scenarios other than classifications A-1 through A-9.

### 5.3. Resource Management Services

#### 5.3.1. Tracking services for Resource Management

This service allows the tracking of location and status of specific service group users. One example is a supervisor in the role of Rule Maker and main Location Recipient who manages a delivery service and needs to know the location and status of employees. The supervisor may also be able to relay messages to the employees or other people involved in the service (for instance, customers). Another example is an enterprise tracking the location of vehicles (cars, trucks, etc.) and use location information to optimize services (Fleet Management).

This service could arise most likely under the Pull Model, and most likely in classification A-6.

#### 5.3.2. Package Tracking

A delivery company (Rule Maker) launches a service to notify a customer 'C' (Viewer) about a package 'B' (Target) that it is now at the closest hub. The sighting might be triggered by an employee of the delivery company, or by the sender or the receiver of the package.

This service could arise with either the Push or Pull Models, and most likely in classification A-6.

#### 5.3.3. Taxi dispatch system - location of the customer

A customer calls a taxi company for a taxi by his cellular. A dispatch operator initiates their taxi dispatch system to find the most appropriate taxi. First, the system obtains customer's current location from a Location Generator (maybe a cellular carrier). Then it searches the closest and available taxi based on location information that he has. When it finds one, it displays a map around the customer to the taxi driver.

This service could arise most likely under the Pull Model, and most likely in classifications A-1, 2, 4, or 5.

#### 5.3.4. Taxi dispatch system - location of the taxi

After a customer calls a taxi company for a taxi and the dispatch operator already knows his location, it searches the closest and available taxi based on location information. This is an particular example of a Target Information Disclosure Service. This kind of service inputs Location Information and outputs a Target ID (or processed information). In our case the Location Server should have a functionality to obtain a Target ID (a taxi) by using the Location Information of the customer. When it finds a taxi, it displays a map around the customer to the taxi driver

Note: the location of the customer is sent or the taxi, but the location of the taxi is sent (by LG) to the Operator, the taxi knows his own location.

This service could arise most likely under the Pull Model, and most likely in classifications A-1, 2, 4, 5, or 7.

#### 5.4. Geographic Based Content Services

Location based information services allow subscribers to access information for which the information is filtered and tailored based on the location of the requesting user. Subscribers will likely initiate service requests on demand, but such services may be triggered automatically when certain user-set conditions are met.

##### 5.4.1. Navigation

The purpose of the navigation application is to provide directions to guide the target to his/her destination. Depending on the context this could be driving or walking directions, traffic update, public transport services, or others. The information may be in the form of plain text, SMS messages, symbols with text information (e.g. distances and turns), voice, or symbols on a map display.

For example, a user is driving a car with a navigation Device which can access to the Internet. He initiates an online navigation service from the Device to get the fastest route to his destination.

The online system obtains his location with the Device. Then searches traffic information around him and finds the fastest route. And it shows a direction on his Device.

This service could arise most likely under the Translate/Query Model, and most likely in classification A-3.

#### 5.4.2. City Sightseeing

City Sightseeing would enable the delivery of location specific information to a tourist. Such information might describe historical sites, providing navigation directions between sites, facilitate finding the nearest museum, bank, airport, bus terminal, restroom facility, etc.

This service could arise most likely under the Translate/Query Model, and most likely in classification A-3.

#### 5.4.3. Mobile Yellow Pages

Mobile Yellow Pages services provide the user with the address and phone number of the nearest location of a certain type or all locations within a chosen area (e.g. all Chinese restaurants within three kilometers).

The information can be provided to the users in text format (e.g. name of the restaurant, address and telephone number) or in graphical format (map showing the location of the user and the restaurants).

This service could arise most likely under the Translate/Query Model, and most likely in classification A-3.

#### 5.4.4. Traffic Monitoring

Mobiles in automobiles on freeways may be sampled to determine average velocity of vehicles.

This service could arise most likely under the Pull Model, and most likely in classifications A-1, 2, 4, or 5.

#### 5.4.5. Traffic jam information

This is a particular case of an Area Information Disclosure Service. This service type, a variant of the Target Information Disclosure Services, comprehends services which input Area information, instead of Location, and output a Target ID (or processed information).

A traffic information system inputs area information (e.g. location with range) to a Location Server. Then the Location Server returns number of targets which are within the area right now.

This service could arise most likely under the Pull Model, but most probably under scenarios other than classifications A-1 through A-9.

## 5.5. Content Provider-Initiated Information Services

Another form of location based information services can transmit information to users based on their location, but at the request or initiation of entities other than the user. Users will likely need to subscribe or opt in to the services (and thus the services are in some ways user initiated). The delivery of such services may be triggered automatically when certain user-set conditions are met.

### 5.5.1. Location Dependent Content Broadcast

The main characteristic of this service category is that the network automatically broadcasts information to terminals in a certain geographical area. The information may be broadcast to all terminals in a given area, or only to members of specific group (perhaps only to members of a specific organization). The user may disable the functionality totally from the terminal or select only the information categories that the user is interested in. An example of such a service may be localized advertising; merchants could broadcast coupons and advertisements to people passing by.

This service could arise most likely under the Push Model, but most probably under scenarios other than classifications A-1 through A-9.

## 5.6. Entertainment and Community Services

The services in this subsection could arise with either the Push, Pull, or Translate/Query Models, and conceivably in almost any of the classifications A-1 through A-9.

### 5.6.1. Mobile Communities or Locate a Person

Find friends or share my position with my friends and interact

### 5.6.2. Gaming

Play games based on players's location.

### 5.6.3. Rendezvous service

A user initiates a rendezvous service from his cellular. The system obtains his current location from a Location Generator, maybe a cellular carrier. The system sends his friend an e-mail to describe how to reach him.

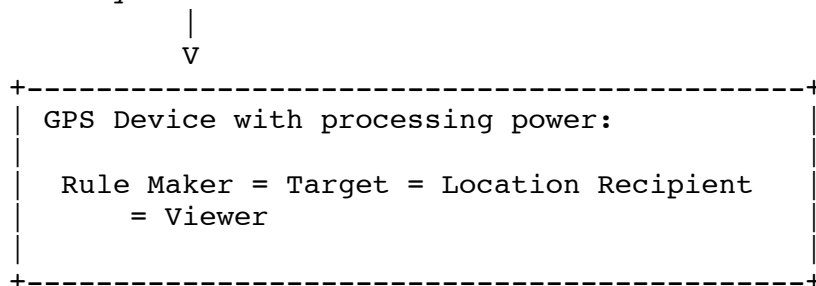
## 6. Scenarios

## 6.1. Scenario 1

## Target Seeks Own Location with GPS Device with Computing Power

In this very simple example, the Target wishes to know his/her location using GPS, and has a device that is capable of processing the raw data to determine a useful location. The location is derived as follows: the device receives transmissions from GPS satellites, and internally computes and displays the location. This is a wholly closed system.

One Way GPS Satellites



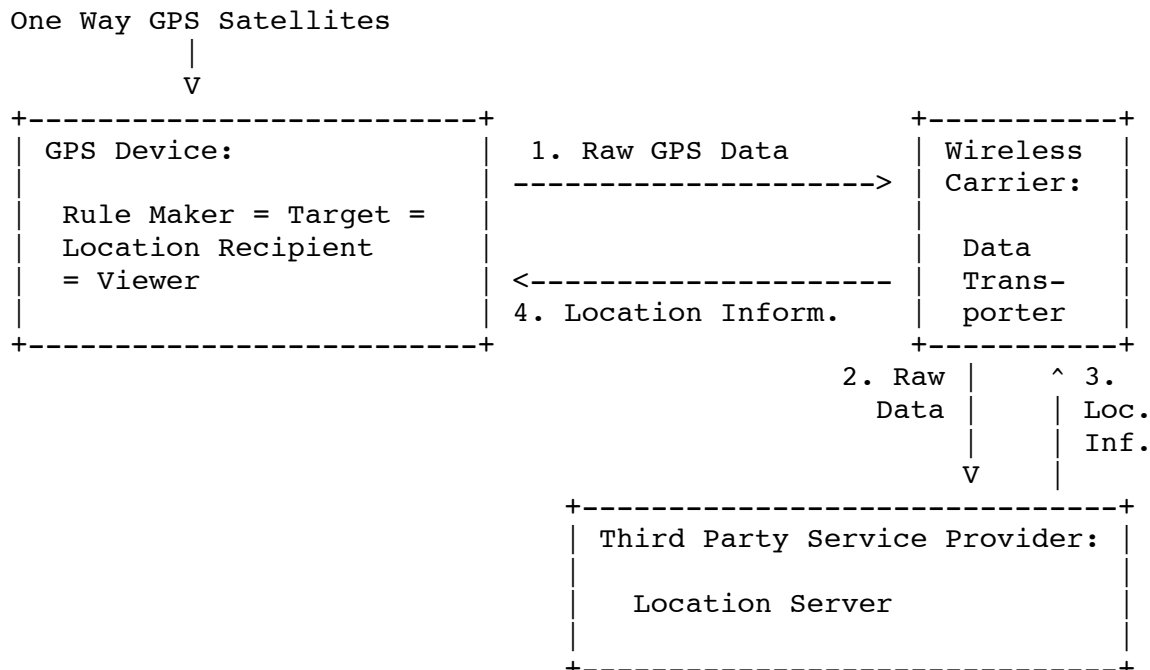
In this closed system no external entity is granted access to location information. This minimizes the privacy concerns. But, because the device can be lost, stolen or accessed through legal process, questions about data retention and data security remain. What information is stored on the device? For how long? What security protects it?

This scenario could arise most likely under the Translate/Query Model, but most probably under scenarios other than classifications A-1 through A-9.

## 6.2. Scenario 2

## Target Seeks Own Location with GPS Device with No Computing Power

In this example (an instance of B-8 or B-9), usable Location Information is computed by an outside entity based on GPS data. In this example, the outside entity is NOT the wireless carrier providing network access, but is instead a third party. The location is derived as follows: the Device receives GPS transmissions, and sends (using the wireless carriers network, which acts as a simple Data Transporter) the raw data to a third party Location Server. That server processes the data and sends it back to the Device. The third party Location Server may or may not store the Location Information for later use in accordance with the Privacy Rules set by the Rule Maker.



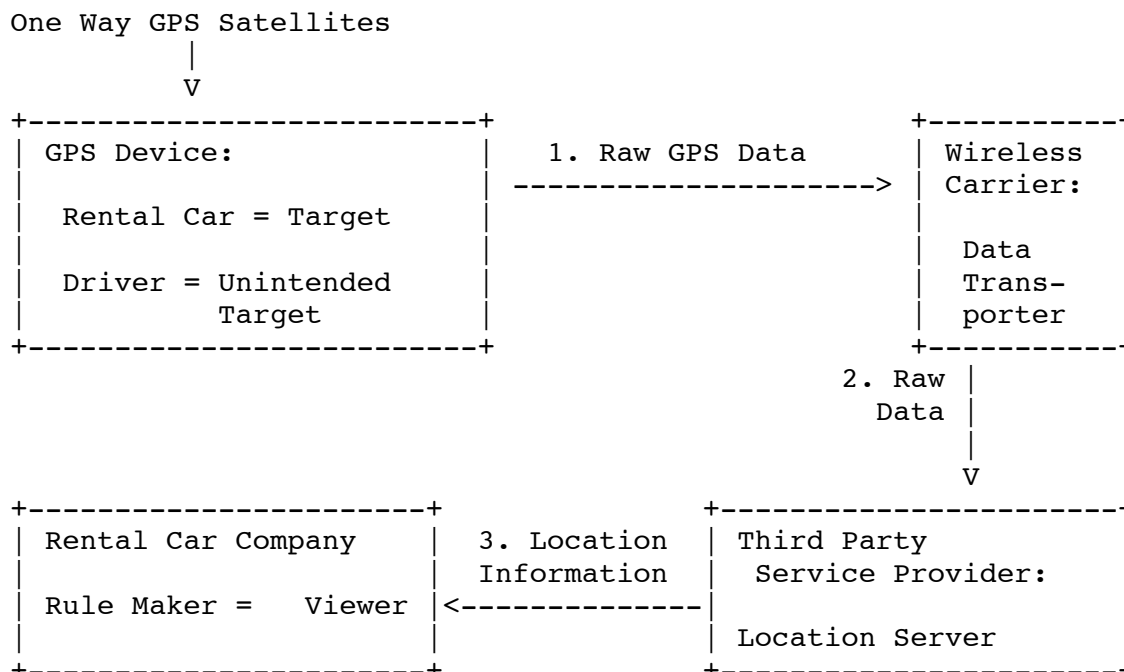
The same concerns raised in Scenario 6.1 (about the security of information contained in the Device) remain. A host of additional concerns are raised, including about the security of information as it passes through the Data Transporter. The most significant additional concerns are about the third party Location Server, including the length of data retention, the ability to reuse and disclose, and the security of any data storage.

This scenario could arise most likely under the Translate/Query Model, but most probably under scenarios other than classifications A-1 through A-9.

### 6.3. Scenario 3

#### Fleet Owner Seeks Location of Rental Cars with GPS Device

In this example (an instance of classification B-9), a rental car company wants to track its vehicles using GPS, solely for purposes of fleet management (and not as a service to the rental customer). The Target is the rental car and the Unintended Target is the driver. The location of the Target (and the Unintended Target as well) is derived as follows: the rental car receives GPS transmissions, and on a regular basis transmits the raw GPS data via a wireless network to a third party Location Server, which in turn determines the Location Information in a useful format and forwards that LI to the car rental company.



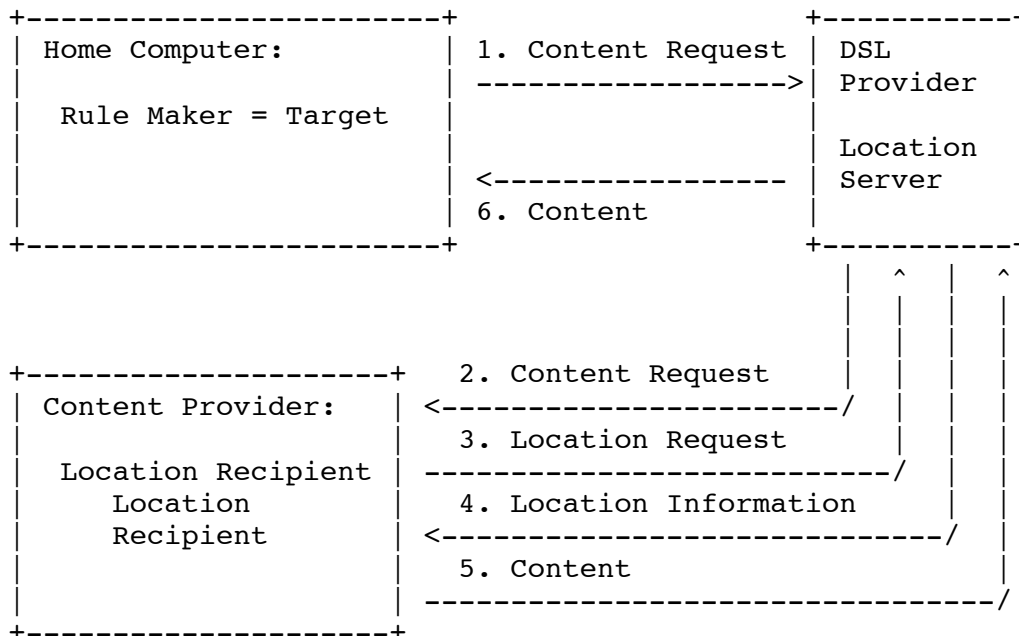
All of the same concerns raised in Scenario 6.2 are raised here, plus additional concerns (in particular concerning the threat to the privacy of the Unintended Target, the car rental customer driving the rental car). That threat is reduced (but far from eliminated) if the information transmitted to the third party Location Server does not carry any identifier related to the customer/driver. In general, the threats to the Unintended Target are outside the scope of Geopriv, but the risk to the Unintended Target nevertheless warrants note.

This scenario could arise most likely under the Pull Model, and most likely in classification A-6.

#### 6.4. Scenario 4

##### Target in Fixed Location Purchases Regionally Restricted Content

In this example (an instance of classification B-5), the Target has in his or her home a desktop computer continuously connected to the Internet over a wire-line DSL connection. The Target seeks to purchase certain audio or video content from a World Wide Web based content provider. For contractual or legal reasons, the content provider will only sell the content to users located in a particular country or region. The content provider (as the Location Recipient) requests that the Target's Access Provider (the Target's DSL ISP) provide the Target's Location to the content provider.



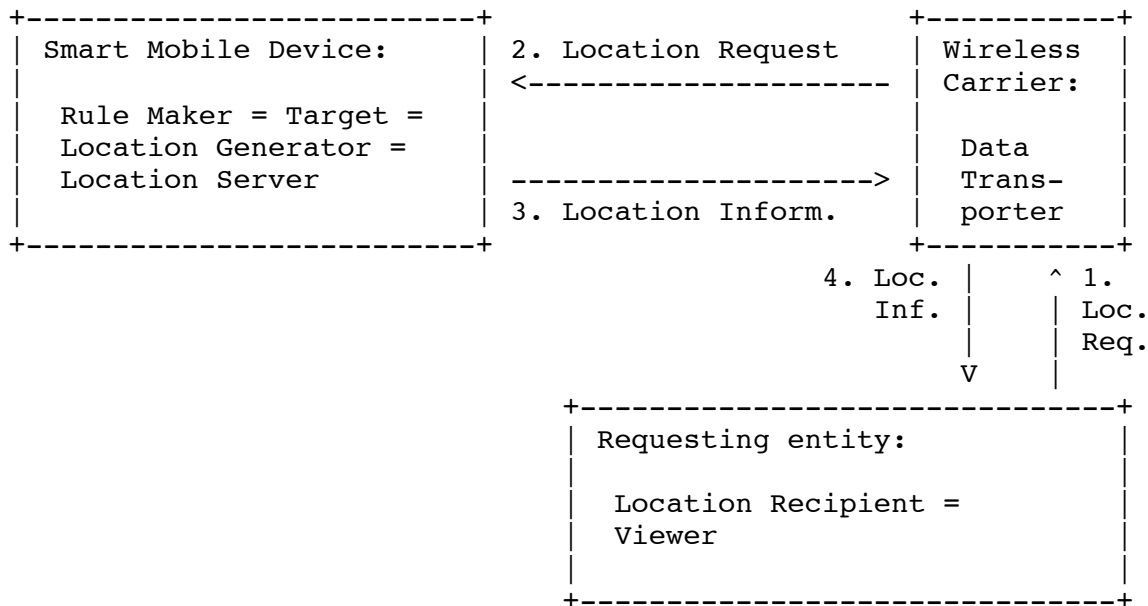
This scenario could arise with either the Push or Pull Models, and most likely in classifications A-1, 2, 4, 5, or 8.

### 6.5. Scenario 5

Third Party Seeks Location of Target with Device with Computing Power and Location Awareness

In this case, a mobile node (laptop or handheld) is at the same time is the Target, Rule Maker, Location Server, and Location Generator. The mobile node knows or discovers its own position using a GPS mechanism, a manual input from the user, or a co-located sensor that recognizes the relative position of some active badges or other reference points. An application running in the mobile node delivers its location to some Viewers.

A Viewer that wants to know the position of the mobile node sends a Location Requests to the application running on the mobile node. After authenticating the Location Recipient, the application checks which Rule rule matches, translates the location information to the appropriate form and sends back this Filtered Location Information to the Viewer.



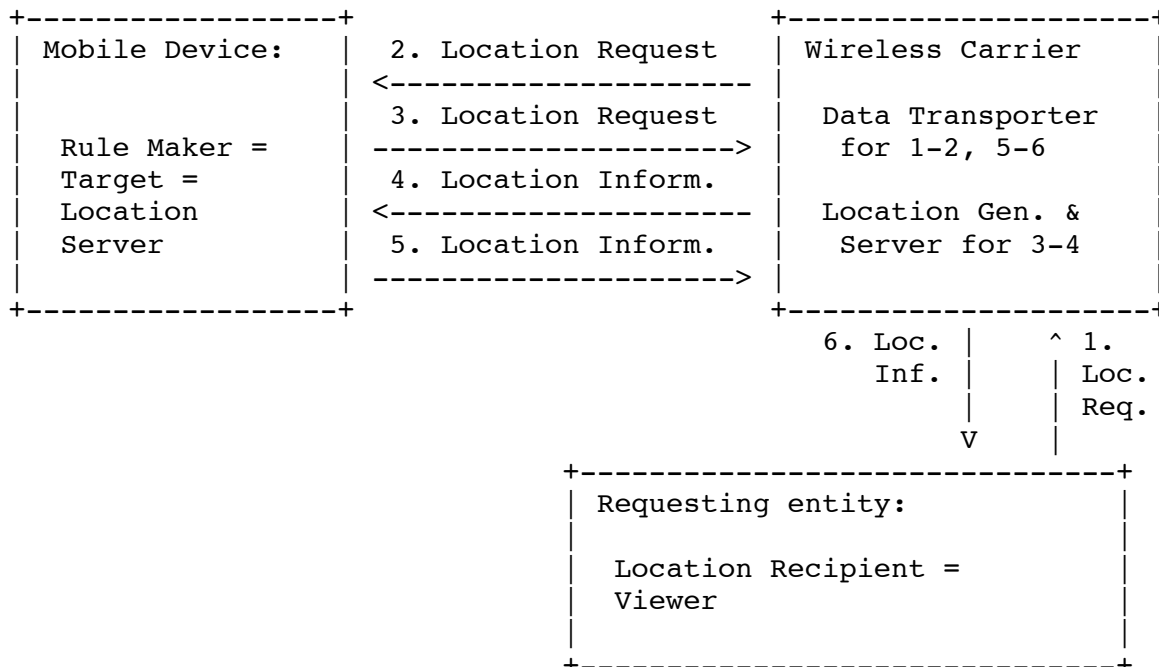
Notice that in this case the Rules are only for internal use of the mobile node and as such do not have to be standardized. Only the interface to the Viewers has to be standardized. The Location Recipient, however, must obey the Rule Maker's Privacy Rules, which are either conveyed or referenced in the Location Object

This scenario could arise most likely under the Pull Model, and most likely in classifications A-1 or 4.

### 6.6. Scenario 6

Third Party Seeks Location of Target with Device with Computing Power But No Location Awareness

This scenario is very similar to the prior one, but instead of the mobile node discovering his position by himself, it requests its wireless carrier (its Access Provider) to determine the location of the mobile note (the Device), and send it back to the mobile node for service to the Viewer.



Notice that in this scenario no Location Recipient exists, besides the Rule Maker and the Viewers served by the Rule Maker. Thus, the Rule Maker is in full control of its private information.

There is a significant privacy concern raised by the uncertainty of how the Rule Maker makes sure that the Location Generator (here, the Access Provider) does not provide location information to other location recipients. Either the AP is aware of the full Rules of the owner, or a default (set by law, contract, or protocol design) prohibits disclosure. A precise requirement should be formulated to guarantee this privacy protection.

Another concern is that, depending on the sensing infrastructure and its trusts relationships to the user, authenticating the supplied location information is difficult for the following reasons:

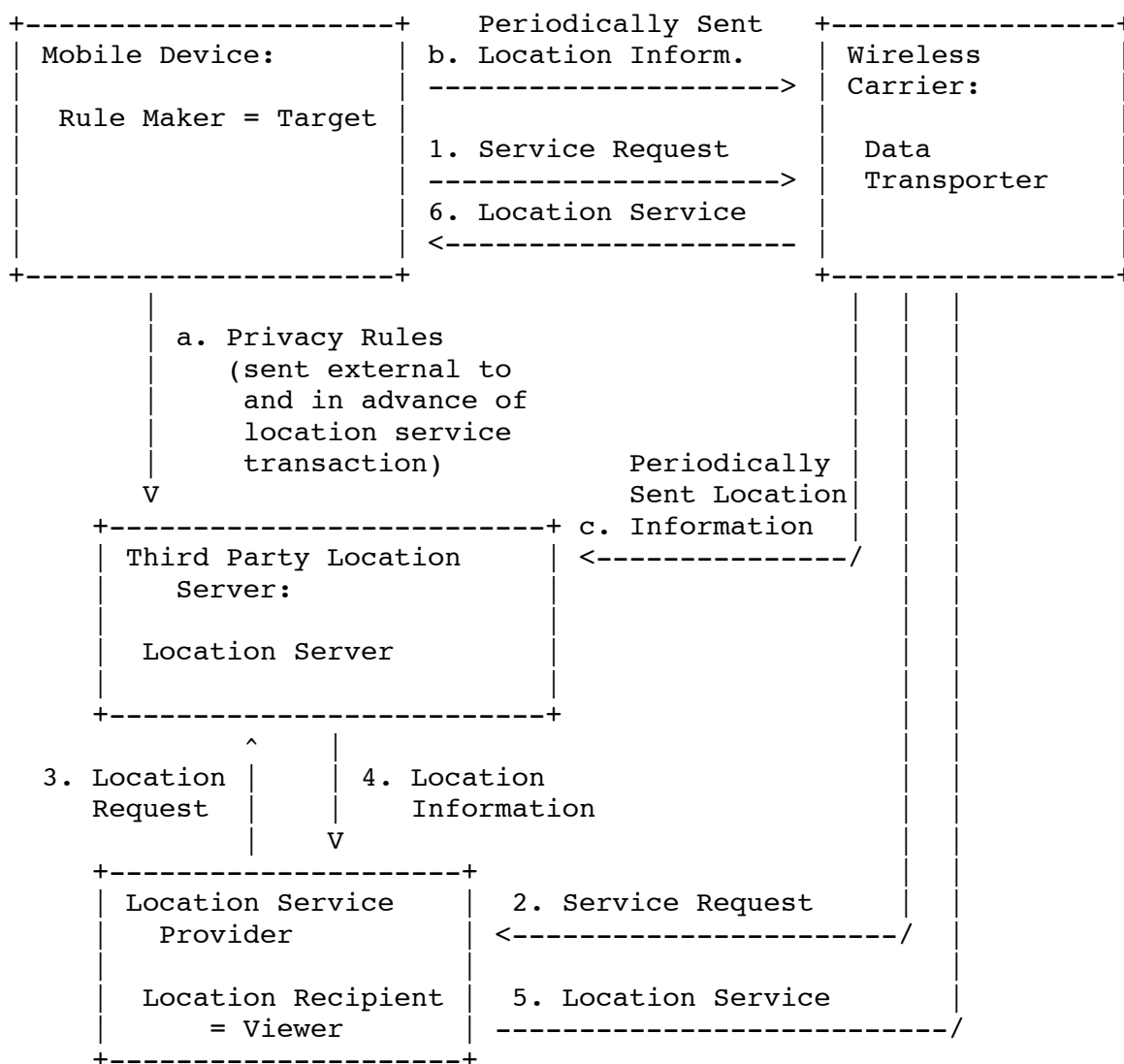
- o some sensor systems only detect active badges that can be removed from the mobile object they represent.
- o sensor systems are not equipped with proper keys or key distribution software.

This scenario could arise most likely under the Pull Model, and most likely in classifications A-2 or 5.

### 6.7. Scenario 7

Target with Location Aware Device Using Third Party Location Server to Obtain Location Based Service From a Fourth Party Service Provider

In this case, a mobile node (laptop or handheld) is at the same time is the Target, Rule Maker, Location Server, and Location Generator. The mobile node knows or discovers its own position using a GPS mechanism, a manual input from the user, etc., and periodically sends that location to a third party Location Server with which the Rule Maker has a prior contractual arrangement. The Target sends the Location Server its Privacy Rules in advance. When the Target then seeks a location service, it requests the service from the service provider. The service provider requests the Target's location from the Location Server, and then fills the Target's request for a service.

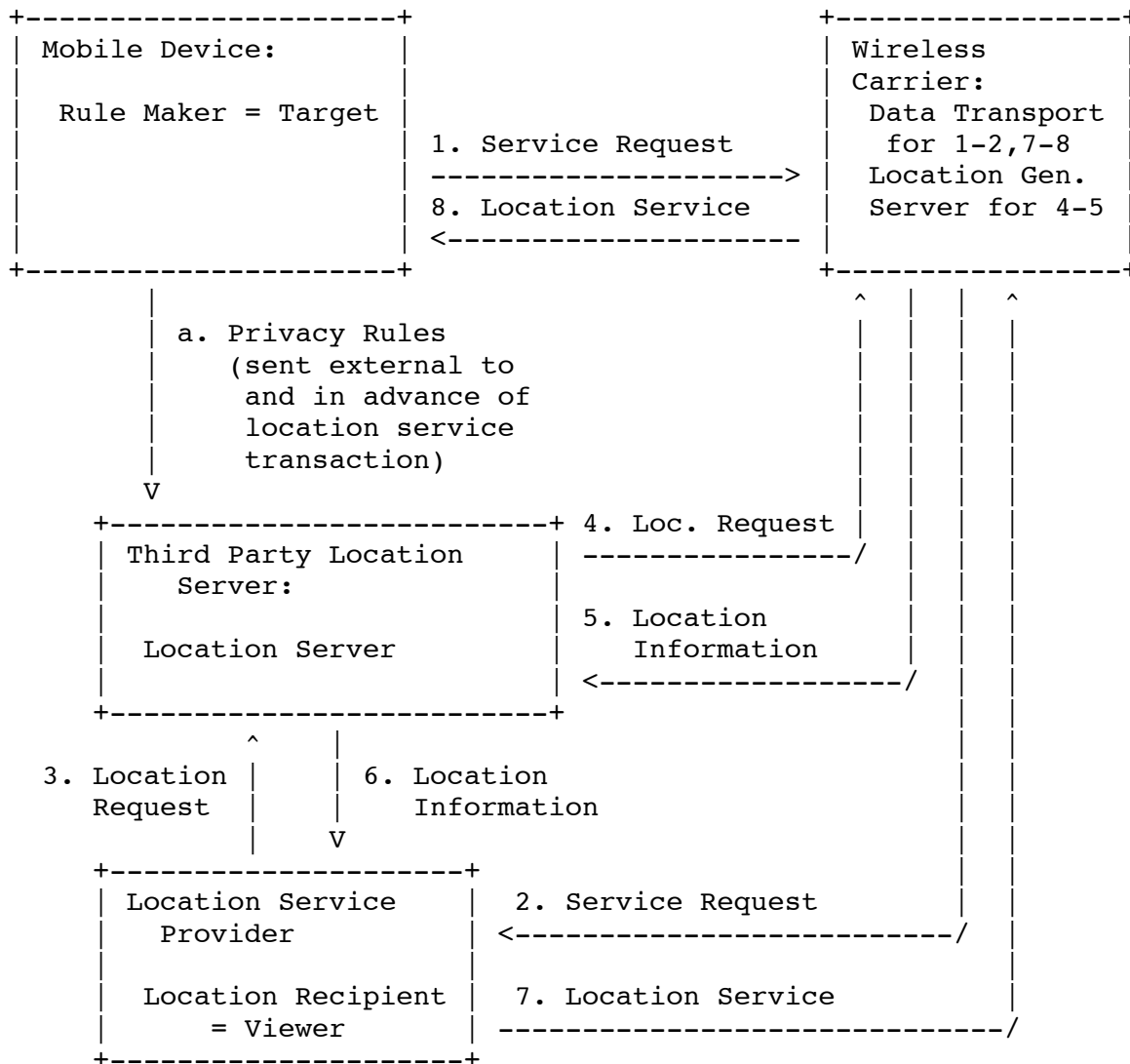


This scenario could arise most likely under the Pull Model, but most probably under scenarios other than classifications A-1 through A-9.

6.8. Scenario 8

Target with Non-Aware Device Using Third Party Location Server to Obtain Location Based Service From a Fourth Party Service Provider

This final scenario is the same as the prior scenario except that the Target's Device does NOT know its location and must instead have its Location Server ask for its location from the Target's Access Provider:



Note that the Access Provider also acts as a Location Server to provide the initial Location Sighting to the third party Location Server, which then in turn fills the request for location.

This scenario could arise most likely under the Pull Model, but most probably under scenarios other than classifications A-1 through A-9.

## 7. Implications and Conclusions

Critical privacy issues illustrated by the location computation scenarios are who controls the data and how, who computes or derives the location information, and who stores uses and discloses the data.

All examples apart from the closed system represented by Scenario 1 present many privacy issues. The more entities involved, the more difficult it is to make sure the Privacy Rules of the Rule Maker are implemented. In cases where there is a pre-existing relationship, technology may not be necessary to transmit Privacy Rules. Instead, the Rule Maker and AP might reach a contractual agreement about privacy. But, the Rule Maker will not always have a contractual relationship with the AP or all involved entities. In some instances the Target will have no choice but to use a single AP. Sometimes "a chain" from the AP to other entities to enforce the Privacy Rules may work. Therefore, technologies that address these issues must be developed.

Entities may be constrained by national or local laws regarding how they handle information. For example, in some relevant situations within some countries, "Customer Proprietary Network Information" (CPNI) rules require that telecommunications carriers obtain customer approval before using, disclosing, or permitting access to individually identifiable CPNI.

## 8. Security Considerations

The purpose of the Geopriv Location Object is to allow a Rule-controlled disclosure of location information for location services. The information carried within the Location Object is secured in a way compliant with the privacy and security Rules of the Rule Maker, but other information, carried in other objects or headers are in general not secured in the same way. The scenarios included in this draft can serve to illustrate security concerns that must be addressed by Geopriv.

## 9. Acknowledgements

Important elements of this draft were inspired by a prior scenarios draft by Kenji Takahashi and his colleagues.

## 10. References

[ISO99] ISO99: ISO IS 15408, 1999, <http://www.commoncriteria.org/>.

[OECD] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, <http://www.oecd.org>.

[Pfi01] Pfitzmann, Andreas; K<sup>o</sup>hntopp, Marit: Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology; in: H Federrath (Ed.): Designing Privacy Enhancing Technologies; Proc. Workshop on Design Issues in Anonymity and Unobservability; LNCS 2009; 2001; 1-9. Newer versions available at <http://www.koehntopp.de/marit/pub/anon>

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

## 11. Author's Addresses

Jorge R. Cuellar  
Siemens AG  
Otto-Hahn Ring 6  
81730 Munich  
Germany  
Email: [jorge.cuellar@mchp.siemens.de](mailto:jorge.cuellar@mchp.siemens.de)

John B. Morris, Jr.  
Director, Internet Standards, Technology & Policy Project  
Center for Democracy and Technology  
1634 I Street NW, Suite 1100  
Washington, DC 20006  
USA  
Email: [jmorris@cdt.org](mailto:jmorris@cdt.org)

Tsuyoshi Go Kanai  
Fujitsu Laboratories, Ltd.  
64 Nishiwaki, Okubo-cho,  
Akashi 674-8555  
Japan  
Email: [kanai.go@jp.fujitsu.com](mailto:kanai.go@jp.fujitsu.com)

## 12. Full Copyright Statement

Copyright (C) The Internet Society (date). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

Expires in six months

Mar 2003

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.