INTERNET-DRAFT J. Morris
Center for Democracy and Technology
D. Mulligan
Samuelson Law, Technology, and Public Policy Clinic
S. Kelin
Samuelson Law, Technology, and Public Policy Clinic
A. Davidson
Center for Democracy and Technology
draft-morris-geopriv-scenarios-00.txt November 2001
Expires May 2002

Framework for Location Computation Scenarios

Status of this Memo

Copyright Notice

Abstract

This document defines a framework for describing location computation scenarios. The framework is intended to be a starting point for a discussion of privacy and security issues for location-based services.

1. Introduction

Location-based services (applications that require geographic location information as input) are becoming increasingly common. The collection and transfer of location information about a particular target can have privacy implications. The ability to derive or compute a target's location, and access to the derived or computed location, are key elements of the location-based services privacy equation. Central to a target's privacy are (a) the identity of entities that have access to raw location data, derive or compute location, and/or have access to derived or computed location information, and (b) whether those entities can be trusted to know and follow the target's privacy rules. This document seeks to list location-computation scenarios and identify for each scenario which entities must be trusted to ensure a target's privacy.

2. Scope of This Document

The framework set out below assumes that "location information" is a relatively specific way of describing where a target is located and that the location information is either (a) derived or computed from information generally viewed as non-public, or (b) determined by a device that is not generally publicly addressable or accessable. For example, location information could include information calculated by triangulating on a wireless signal with respect to carriers' cell phone towers, or longitude and latitude information determined by a device with GPS (global positioning satellite) capabilities. The framework below also encompasses, for example, scenarios in which the non-mobile position of a target is derived from "caller-ID" or ANI (automatic number identification) information obtained by a service provider offering dial-in network access.

Excluded from the framework below is location information that is based on generally available information such as an IP or e-mail address. It is important to note that information like IP address can enable someone to roughly estimate a location. Commercial services exist, for example, that offer to provide rough location information based on IP address. Currently, this type of location information is less accurate and has a coarser granularity than the type of location information addressed in this document. This less accurate type of location computation still raises significant potential privacy and public policy concerns, but such scenarios are outside the scope of this document.

For the purposes of this document, "privacy rules" are rules that regulate an entity's activities with respect to location information, including, but not limited to, the collection, use, disclosure, and retention of location information. These rules must generally comply with fair information practices. For example, see the OECD (Organisation for Economic Co-operation and Development) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data at http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM. Specific parameters of these rules are outside the scope of this document, but they must be fully articulated in a separate document prior to creating location privacy technologies.

3. Framework

The framework to describe location computation scenarios has three attribute categories: mobility of the target, which entity has control over the raw data, and the site of the location computation.

The first attribute category, the mobility of the target, has two possible values: fixed or mobile. Because human beings are not inherently trackable, location-based services often use location information based on devices that people use or carry. In other words, the location of a target's device is often used as a proxy for the location of the target him/herself. In other scenarios, the desired location is that of the device itself, for example if a device is installed in a vehicle or other object to be tracked.

For purposes of this framework, what is relevant is not primarily the actual portability of a target device, but the method of the device's data connection. For example, a laptop computer using a wired data connection (including a dial-up connection through the public switched telephone network) typically indicates that the target is in a fixed location at the point of the location inquiry, while a laptop computer using a wireless data connection should be viewed as "mobile" even if the laptop is in fact not moving. Thus, the type of data connection can indicate a target's "mobility."

The other two attribute categories can be thought of as decision points that are related to steps in the location computation process. 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).

It is significant that the raw information from Step 1 and the computed location from Step 2 both provide information about the target's position. In Step 2, the raw data from Step 1 is transformed (and perhaps joined with external geographic or other data) into a more useful format. Because location information can be expressed in many formats, it is also possible that the location computed in Step 2 will be further transformed so that it is more useful to the requestor. After the target's location has been computed, the location is available to be used in a location service or otherwise served to a requestor (as discussed in Section 7 below).

The first decision point is who has control over the raw data (Step 1). There are two possible values: the target or the target's (wired or wireless) carrier network. 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 carrier (even though the user may have the ability to turn the cell phone, and thus the GPS reporting, off entirely).

The second decision point is the site of the location computation (Step 2). There are three possible values: the target's device, the carrier network of the target's device, or a third party who is neither the target nor the carrier.

There are two distinct decision points because the entity or device that controls the raw data may transmit it to a different entity before the location computation is performed. Although some initial implementions of location-based services may assume that a wireless carrier will perform the location computation, any framework to protect privacy should accommodate a model in which third parties receive raw locational data, derive or compute a location, and then serve or otherwise act on the location in accordance with a target's privacy rules.

4. Significance of Decision Points

To ensure privacy, the target must be able to set and communicate privacy rules. Furthermore, the privacy rules of the target must be honored both by entities with access to the raw data and by entities (if different) that perform the location computation (and

possibly by additional entities that later receive and/or re-serve the computed location).

The first decision point - who has access to and control over the raw data - is important because any entity with access to this raw data can likely determine the location of the target independent of the desires of the target. If the target has control over the raw data, the target (if given appropriate tools) can limit transmission of the raw data according to appropriate privacy rules. This would include situations in which raw data is generated by a GPS-enabled device controlled by the target, but also would include scenarios in which a target manually inputs his location into a device or location service. In contrast, if a carrier has access to or control over the location information (such as when the raw data is drawn from a wireless carrier's network), the carrier must know or learn - and follow - the appropriate privacy rules.

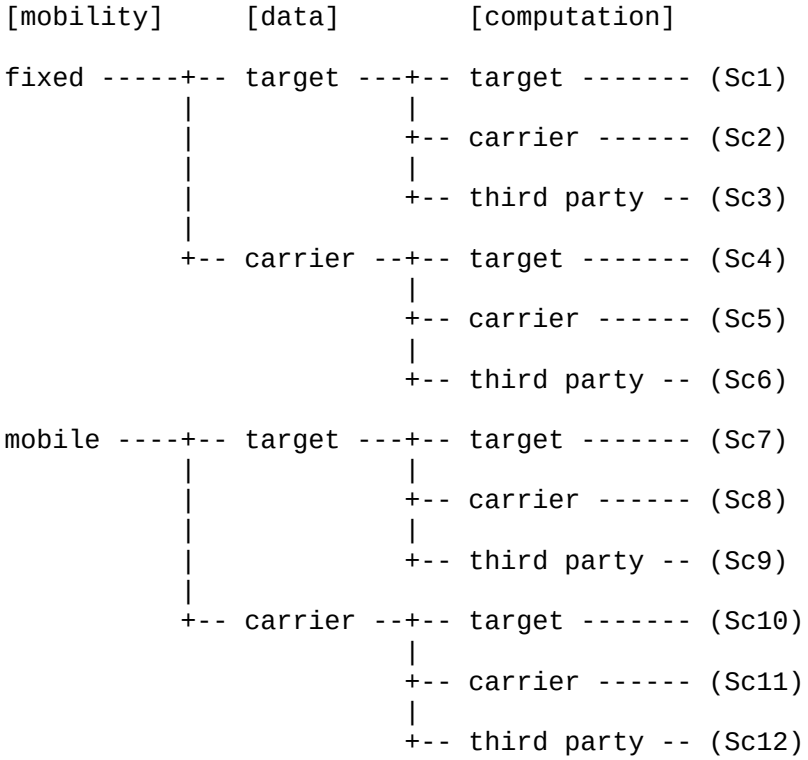
The second decision point - who performs the location computation - is equally important because, by definition, any such entity knows the target's location. If the target (or target's device) performs the location computation, the target (if given appropriate tools) can limit transmission of location information according to appropriate privacy rules. In contrast, if either a carrier or third party performs the location computation, the carrier or third party must know or learn - and follow - the appropriate privacy rules.

Together, the entities that control the raw data and perform the location computation determine who knows the target's location. Thus, these entities must protect the location information consistent with the privacy rules set by the target during all uses and disclosures.

5. Basic Scenarios

The three attribute categories and their possible values yield a total of 12 basic scenarios, as illustrated below. In the diagram, the following words stand for the following phrases:

```
mobility    - mobility of the target
data        - who controls or has access to raw location data
computation - who performs the location computation
carrier     - carrier network of the target's device
target      - the target or the target's device
Sc n        - scenario number
```



6. Examples of Scenarios

Of the 12 scenarios identified, some reflect well-known business and technical models that currently are being implemented. For example, Sc11 is where the location of a cellular telephone user is determined by the user's wireless carrier based on information in the carrier's network.

Other scenarios reflect plausible if less visible business models, such as Sc9 in which a target has a cellular telephone or other

device containing a GPS chip, and the target (or target's device) transmits the raw data to a third party, which returns the target's current street location.

Among the "fixed" mobility scenarios, for example, Sc3 would include a situation in which a target manually provides current location information and a third party returns driving direction to a particular retail establishment. Sc5 would include a possible business model in which a carrier provided highly localized targetted advertisements based on "caller ID" information drawn from a dial-in modem port.

Finally, certain scenarios, such as Sc4, do not reflect any readily apparent practical implementations but are included to ensure a complete analysis of the scenarios.

It is important to acknowledge that particular types or formats of location data cannot be easily categorized as always "raw data" or always "computed location information." For example, in Sc9, longitude and latitude data may be the "raw data" returned by a GPS device, and a third party may derive a street address from that raw data. But in Sc12, the raw data may be triangulation data available to a carrier through its network, and based on that raw data the carrier may compute longitude and latitude data to be provided to a law enforcement agency involved in a wilderness search and rescue. Moreover, as discussed below, computed location information may be further transformed into additional, perhaps more useful, location formats.

7. After the Location Computation

After the target's location has initially been computed, there are at least five possible outcomes:

(a) the transaction is complete (if, for example, the target wants to know its own location and the target computes the location, as in Sc10);
(b) the entity that computes the location transmits it back to the target, or transmits to the target other information (such as driving directions) that are based on the target's location;
(c) the entity that computes the location transmits it to a third party that makes immediate use of the information;
(d) the entity that computes the location stores it for later retrieval by the target or possibly a third party; or
(e) the entity that computes the location transmits it to a third party that in turn serves or stores the location information.

Once a location has been computed, it is available to be transmitted or served to a requestor. An entity that serves location information is known as a "location server." It is important to note that any entity can be a location server, including the target's device, the carrier, or a third party. To protect the privacy of the target, any location server must receive and follow the target's privacy rules when it stores location information and/or uses or discloses this information.

8. Implications

As discussed above, two critical elements of location computation scenarios are who controls the raw data and who computes or derives the location. If the target does not both control the raw data and perform the location computation, he or she must form a relationship (even if, in some cases, a very brief one) with at least one other entity, and privacy rules must control this relationship. Who these other entities are must be considered because different entities have different relationships with the target, face different technical constraints, and are subject to different legal considerations.

For example, a target who uses a computer to dial into a network (and most other wired connections) typically does so through an Internet Service Provider as the "carrier," and it is likely (but not certain) that the user has a pre-existing relationship with the ISP. In cases where there is a pre-existing relationship, technology may not be necessary to transmit privacy rules to that carrier. Instead, the target and carrier might reach a contractual agreement about privacy, and the target may first express privacy rules in an online or offline form that is stored by the carrier.

For wireless scenarios, a target typically (but not always) has a pre-existing relationship with a wireless carrier, but there may not be any direct relationship with the relevant carrier while a target is "roaming" away from the primary carrier's service area.

As for technical constraints, it is possible that a target's mobile device will be small, lightweight, and low on computing power. These characteristics may mean that the device cannot efficiently perform its own computations. Thus, to protect his or her privacy, the target would need to form a trusted relationship with his or her carrier or a third party, obligating them to compute the location and either provide it back to the target's device for serving or abide by the target's rules about privacy.

Carriers and others may be constrained by national or local laws regarding how they handle information. For example, in some relevant situations within the United States, "Customer Proprietary Network Information" (CPNI) rules require that telecommunications carriers obtain customer approval before using, disclosing, or permitting access to individually identifiable CPNI. See 47 United States Code Section 222 at http://www4.law.cornell.edu/uscode/47/222.html.

9. Possible Technologies to be Developed

It is not the purpose of this document to identify the specific technologies necessary to protect privacy of location information. But, in considering the framework set out above, the scenarios suggest a number of possible technological needs to protect a target's privacy and transmit a target's privacy rules. Those possible technological needs include:

(a) a method to transmit to a carrier that has access to raw location data the applicable privacy rules of the target;
(b) a method to transmit a target's privacy rules to an entity that computes or derives location; and
(c) a method to transmit a target's privacy rules to any subsequent entity (after the location computation is complete).

A single technology could be created to accomplish all three listed needs. It is also possible, however, that the first listed need (to protect privacy of raw data) could be accomplished by the

transmission of a more limited amount of data than might be required to accomplish the other needs. For example, if a privacy model permits other entities to receive and follow more complex privacy rules, then a carrier with access to raw data might need to receive only one instruction regarding what other entity should receive the raw data.

10. Conclusion

Scenarios are a good way to begin discussing the privacy issues of location-based services. To be useful, these scenarios should include the details of location computation, which can in turn suggest the specific entities that must receive and honor a target's privacy rules.

11. Security Considerations

This document does not introduce new security issues. The entire document, however, does address the need to protect the privacy and confidentiality of location information.

Authors

John B. Morris, Jr.
Center for Democracy and Technology
1634 I Street NW, Suite 1100
Washington, DC 20006
+1.202.637.9800
jmorris@cdt.org

Deirdre K. Mulligan
Samuelson Law, Technology, and Public Policy Clinic
Center for Clinical Education
Boalt Hall School of Law
Berkeley, CA 94720-7200
dmulligan@law.berkeley.edu

Sabra-Anne R. Kelin
Samuelson Law, Technology, and Public Policy Clinic
Center for Clinical Education
Boalt Hall School of Law
Berkeley, CA 94720-7200
sakelin@boalthall.berkeley.edu

Alan Davidson
Center for Democracy and Technology
1634 I Street NW, Suite 1100
Washington, DC 20006
abd@cdt.org

draft-morris-geopriv-scenarios-00.txt Expires May 2002