Internet Draft
Document: draft-morris-geopriv-core-02.txt
Expires December 2003

J. Morris
Center for Democracy
and Technology

D. Mulligan
Samuelson Law, Technology,
and Public Policy Clinic

J. Cuellar
Siemens AG

June 2003

Core Privacy Protections for Geopriv Location Object

Status of this Memo

Copyright Notice

Abstract

The working group has generally agreed that the Geopriv Location Object MUST be able to contain a limited set of Privacy Rules. This Internet-Draft suggests the set of Privacy Rules that the authors believe should be includable in the Location Object.

Table of Contents

1. Overview and Notes on Revisions

The authors believe that there exists working group consensus that that the Geopriv Location Object (LO) MUST be able to contain a limited set of Privacy Rules. This document suggests the set of Privacy Rules that the authors believe should be includable in the Location Object.

The threshold question of whether the LO should contain any Privacy Rules was discussed at IETF-55 in Atlanta. A brief explanation as to why a limited set of Privacy Rules should be includable in the LO is set out in Section 5 below.

The -00 version of this document was discussed at IETF-55 in Atlanta. The -01 version significantly reorganized the proposed rules, and was discussed at IETF-56 in San Francisco. This -02 version refines the Privacy Rules proposal based on in person and mailing list discussion. The main changes from the -01 version are:

* the prior draft placed the proposed privacy elements into two categories: "Human- AND Machine-Readable Privacy" (including elements that can be distributed to any of the entities in a Geopriv transaction) and "Machine-Readable Privacy Elements" (including elements that can only be sent from one Location Server to another Location Server). Concern was raised by the idea of "human readable" elements, and these categories have been changed to respond to the concerns raised.

* the prior draft proposed that rules could be made specific to individuals (Element D, for example, "give my location to my mother at any time, but give my location to my boss only at these certain times), AND, separately, specific to presenters of a credential

(Element E, for example, "give my location to anyone who presents XYZ credential). A concern was expressed about the difficultly of establishing identity independent of a credential. In other words, assuming the absence of a credential (which is permitted with Element E), verifying an identity (as in Element D) would be very difficult. To address this concern, the old Element D has been eliminated. The old Element E has been modified to suggest that in designing the Location Object, it is possible that a concept of "identity" may be used merely as an index into a table of credentials, but such a use of "identity" would not be a requirement for the Location Object.

2. Conventions used in this document

Terms with initial capitals (such as, for example, "Location Object," "Privacy Rule," and "Viewer") have the same meaning as defined in the Geopriv Requirements document, draft-ietf-geopriv-reqs-03.txt.

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 [1].

3. Privacy Rules to be Includable in a Geopriv Location Object

This section details two groups of core elements of Privacy Rules that should be expressible in the Geopriv Location Object. For each of the core elements (designated as Elements A through L), a more precisely stated "rule" is also provided, with Elements D through L being stated in a permissions table as part of a single rule. Section 4 below contains some additional substantive discussion of these elements.

Note that some of the elements and rules discussed below are phrased in terms of prohibitions ("do not disclose except to . . ."), but could probably as effectively be phrased in terms of permissions ("permitted to disclosed only to . . . ").

3.1. Widely Distributable Privacy Elements and Rules

This first group of privacy elements and resulting rules represent the most basic Privacy Rules, and can be transmitted between and among any of the entities in a Geopriv transaction.

Two different forms of this first group would be defined - a compact form suitable for low bandwidth applications, and a more verbose default form that could possibly be transmitted to the Viewer (i.e., the final recipient of Location Information). This latter approach would permit, for example, the return of a Location Object in

response to a HTTP request from a web browser.

The three privacy elements in this group are:

Element A: Requirement that external privacy rules be followed

Element B: Limitation on length of data retention

Element C: Limitation on any retransmission or further disclosure

The following expresses these three broad elements in more precise language:

Rule 1: Do not retransmit or further disclose my location information except in full compliance with the privacy rules located at [url/uri]. (Element A)

Rule 2: Do not retain my location information [past xyz time+date OR longer than xyz duration]. (Element B)

Rule 3: Do not retransmit or further disclose my location information. (Element C)

3.2. LS-to-LS Privacy Elements and Rules

The second group of Privacy Rules that can be contained in a LO is intended for use in transmissions between Location Servers.

The authors believe that, taken together, Elements A - L would allow the expression of a very high percentage of users' complete set of Privacy Rules, and thus in many cases could obviate the need for reference to any external set of Privacy Rules.

The privacy elements in this group are:

Element D: [deleted]

Element E: Permission to disclose only to someone presenting a specified key (for instance, a shared key or the private key corresponding to a particular public key), or a special type of credential (an e-token to be defined).

Element F: Requirement that the granularity/precision of location information be reduced

Element G: The ability to provide additional Privacy Rules for specific requestors or groups of requestors

Element H: The ability to define a time until which a permission is valid

Element I: The ability to define a geographical area for which the permission is valid ("if I am in area x then you can tell y my location")

Element J: The ability to define a repeatable time window (such as weekdays during office hours) during which a permission is valid

Element K: The ability to require that express consent of the Target/Rule Maker be obtained prior to disclosing location

Element L: The ability to require that notice be provided to the Target if location is provided

Elements E through L can be expressed in the form of a single permissions table:

Rule 4: Do not retransmit or further disclose my location information EXCEPT in accordance to the following permissions table:

Credent/Ident	Accuracy	Policy	Valid	LocRes	TimeRes	Consent	Notice
xyz1 [id1]	uvw1	p1	v1	r1	t1	c1	n1
xyz2 [id2]	uvw2	p2	v2	r2	t2	c2	n2
xyz3 [id3]	uvw3	p3	v3	r3	t3	c3	n3
xyz4 [id4]	uvw4	p4	v4	r4	t4	c4	n4

where

xyz Credential: allows for wildcards and "no additional credential required beyond [abc] identity" (Element E)

[id] A non-required possible identity label that can be used to provide an index into the credential table (for example, "here is my xyz credential, and you will locate that credential indexed by [id] in your table")

uvw Accuracy: has one of the following values (Element F):
A = no granularity change required

B = 10 kilometer radius (or within lat/long quadrant)
C = 100 kilometer radius (or within larger quadrant)
D = local or municipal civil designation (e.g., city)
E = state or regional civil designation (e.g., state)
F = national designation (e.g., country)
G = time zone

p Policy: pointer to the privacy rules/policy that must be followed for this specific Location Seeker (Element G)

v Validity: this permission is valid until time v (Element H)

r Location Restriction: r represents a region where this permission applies (for instance, if I am in Munich, then it is OK to pass this information) (Element I)

t Time Restriction: this permission is only valid within the recurring time window t (for instance, only during working hours may my boss obtain my location) (Element J)

c Consent Bit: ask me for permission in real time (and let the Location Seeker abc wait until I tell you) (Element K)

n Notification Bit: send me a notification if you send this Location Information to Location Seeker abc (Element L)

4. Additional Discussion of Proposed Privacy Elements and Rules

The following are additional comments and explanations of the above privacy elements and rules:

a. Rules 1 - 3 should be expressible in both a compact form and a form that would be intelligible to a human viewer. Rule 4 is primarily intended to be read by Location Servers that have sufficient intelligence to process the rules. When sending Location Information to an ultimate Viewer, it is possible that the Geopriv Location Object (LO) itself would need to contain human-readable information (for example, if the LO is sent to a Viewer using SMTP or HTTP). This approach is analogous to the full and compact versions of privacy policies under P3P.

b. Element C and Rule 3 could possibly be omitted as a separate flag or field, because a "do not distribute" instruction should be a

fundamental default for the Geopriv Location Object. Nevertheless, there is value in having an express "do not redistribute" indicator, especially to emphasize that instruction to an ultimate Viewer (who, as discussed above, may well be a human receiving the LO essentially directly).

c. To be clear, the proposal of making specific Privacy Rules includable in a Location Object does NOT mean that all of the proposed privacy rules would be transmitted in every Location Object within a given location transaction. It is quite possible that a LO at an early stage of a location transaction might carry full specifics on Rules 1 - 4. But a later stage of the same location transaction (say, from a Location Server to an ultimate Viewer) might

only carry Rules 1 - 3 (which would be the only rules directly applicable to the Viewer).

5. Reasons to Include Privacy Rules in Location Object

It is not the purpose of this Internet-Draft to explain in full the reasons why a limited set of Privacy Rules should be includable in the Location Object. A brief discussion, however, may assist a reader who is unfamiliar with past working group discussions on the topic.

A critical question that faced the Geopriv working group was whether the Location Object (LO) to be designed should include fields for particular privacy-protecting rules, or instead should simply refer to an external set of privacy rules. The three most plausible answers to this question would be:

(1) "Entirely External" -- the LO should only contain a URI reference to an external set of privacy rules that must be followed by any recipient of the LO.

(2) "Limited Internal" -- the LO should contain a limited set of rules that cover the great bulk of likely privacy situations (as well as the ability to include a URI reference to an external set of privacy rules if more robust rules are needed, or external rule storage is preferred).

(3) "Full Internal" -- the LO should be defined to be able to contain a full, robust, and potentially complex set of privacy rules.

The "Full Internal" option would yield the most complex LO, would be

the most complex to define and implement, and may not be consistent with the goal of enabling the use of the Geopriv LO on constrained devices or with limited bandwidth.

The "Entirely External" approach would be the quickest for the working group to accomplish, and if fully implemented in the marketplace this approach could give end users a great deal of control and flexibility in the protection of Location Information. Under this approach, however, privacy protection would heavily depend on marketplace developments wholly external to the work of Geopriv, and thus may not fulfill the mission of the working group as defined by its charter.

Certain working group participants (including the authors here) argued that the most effective way to ensure that users have some privacy control is for the Location Object to be able to carry a limited number of privacy rules. In discussions at IETF-55 in Atlanta, the working group agreed to pursue the "Limited Internal"

approach, although the group did not determine the precise elements to be included in a "Limited Internal" approach. It is to this latter question that this document is addressed.

Note that the "Limited Internal" approach is effectively a superset of the "Entirely External" approach, so that both of those models could be implemented in appropriate situations even if the LO can carry a larger set of rules. Thus, where a particular location service application in fact offers users robust and effective means to create and maintain an external set of privacy rules, that application could simply transmit the URI/URL of those external rules in the Location Object. But where an application lacks robust and effective external rule servers, the "Limited Internal" approach would allow a core set of rules to be carried with the LO.

6. Additional Suggested Requirement for Location Object

This section is retained here to avoid losing track of the proposal made below (which could be incorporated in the definition of the LO).

The -00 version of this document proposed one element (the original Element G described below) that was decided to be useful, but not actually a "privacy rule." The apparent consensus was to instead designate the proposed functionality simply as a feature to be included in a final definition of a Geopriv Location Object. The resulting proposal is that the LO should be able to contain the following instruction:

> Promptly transmit my location to [abc] individual or entity,

along with [xyz] instruction (where the contents of [xyz] are NOT defined by Geopriv except for technical parameters such as maximum size).

Although this proposal does not itself directly advance a privacy objective, it would greatly facilitate the future development of privacy protecting (and other) business models. It would also promote the ability of a Target to bypass the location services offered by a Location Generator (such as a wireless carrier) in favor of location services offered by a competitive third party.

7. Security Considerations

Security is, of course, is a core goal of the Geopriv working group. The questions addressed in this Internet-Draft -- what privacy rules should be includable in the Geopriv Location Object -- have significant security implications, most directly on the security of the privacy rules themselves. The inappropriate disclosure of some privacy rules could itself harm privacy, and thus a decision to include some privacy rules in the Location Object could expose those rules to a higher chance of security (and thus privacy) violation.

On the other hand, if including rules in the Location Object increases the likelihood that those privacy rules would in fact be known and followed, then the added security risk of transmitting those rules may be outweighed by the added privacy protection afforded.

8. Acknowledgements

We wish to thank Jon Peterson for his constructive criticism of the proposals advanced in the prior version of this document.

9. References

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

10. Author's Addresses

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

USA http://www.cdt.org

Deirdre K. Mulligan
Samuelson Law, Technology and Public Policy Clinic
Boalt Hall School of Law
University of California
Berkeley, CA 94720-7 Email: dmulligan@law.berkeley.edu
USA

Jorge R Cuellar
Siemens AG
Corporate Technology
CT IC 3
81730 Munich Email: Jorge.Cuellar@siemens.com
Germany

11. Full Copyright Statement