Position Paper on "P3P and the Privacy of Location Information"

W3C Workshop on the Future of P3P

John B. Morris, Jr.
Director, Internet Standards, Technology & Policy Project
Center for Democracy & Technology
jmorris@cdt.org

This paper gives a brief overview of the on-going work of the Geopriv working group of the Internet Engineering Task Force (IETF), solely from the perspective of one (very active) participant in the working group. It also discusses some of the key issues that the working group has faced or must face in the future, including the question of whether and how to utilize P3P within the Geopriv context.

I. Background on the Geopriv Working Group

The Geopriv working group was created in 2001 to address the need for privacy protection of geographic location information (for example, in the context of a service that can determine the location of a particular individual or device). According to its Charter [1], the "primary task of this working group will be to assess the authorization, integrity and privacy requirements that must be met in order to transfer [location] information, or authorize the release or representation of such information through an agent."

According to the charter, the working group has an ambitious mandate: "For reasons of both future interoperability and assurance of the security and privacy goals, it is a goal of the working group to deliver a specification that has broad applicability and will become mandatory to implement for IETF protocols that are location-aware."

The working group started slowly, but is nearing completion on its initial "requirements" document. It will be considering that document, as well as documents addressing threats and scenarios, at the meeting of the working group at the November 2002 IETF.

II. Geopriv's "Location Object" and the Possible Role of P3P

Assuming the Geopriv working group continues in its current direction, the initial design work of the group will be on a "location object," a defined envelope that contains location information (in one or more formats), and certain user-defined privacy rules (and/or a reference to external privacy rules).

A critical but as yet unresolved issue facing the working group is whether the Location Object (LO) should include fields for particular privacy-protecting rules, or instead should simply refer to an external set of privacy rules. An individual (non-WG) Internet-Draft [2] recently submitted to the working group offers four plausible answers to this question, labeled somewhat arbitrarily as follows:

- "Entirely External" -- the LO should only contain a reference to an external set of privacy rules that must be followed by any recipient of the LO.
- "Bare Bones Internal" -- the LO should contain at most one or two rules that specify, for example, that the location information shall not be retained past xyz date (or longer than xyz duration), along with a URI reference to an external set of privacy rules that must be followed by any recipient of the LO.
- "Limited Internal" -- the LO should contain a limited set of rules (say, 4 to 7 rules) that cover the bulk of likely privacy situations (as well as the ability to include a reference to an external set of privacy rules if more robust rules are needed, or external rule storage is preferred).
- "Full Internal" -- the LO should be defined to be able to contain a full, robust, and potentially complex set of privacy rules.

It is unlikely that the working group would adopt the "Full Internal" approach. Among the other three approaches, the Center for Democracy & Technology has advocated for the "Limited Internal" approach that would allow certain privacy rules to be carried with the location information.

If the Geopriv working group adopts something akin to the "Limited Internal" approach, the next question to arise will be the format of (a) the limited internal rules, and (b) the external privacy rules. A major consideration for the working group is the size of the Location Object itself. One goal of the working group is to allow the Geopriv work product to support scenarios with devices that have extremely low computational power and/or that send and receive information using very low bandwidth. Among the possible scenarios, for example, would be very simple and small devices that wirelessly transmit a signal (which can be located by wireless networks) at designated intervals.

Because of the desire to support highly constrained devices, it is likely that any privacy rules carried by the Geopriv Location Object will be implemented with as few bits as possible. Thus, it is a reasonable prediction that the working group will not adopt P3P to control the format of internal rules.

Externally stored Geopriv rules, however, are a different matter. The Geopriv working group is not looking to reinvent any wheels, and thus it is likely that the group will seriously consider whether P3P should be used for externally stored privacy rules.

III. Specific Privacy Issues Raised by Location Information

The nature of geographic location information, and privacy concerns about such information, raise some challenging issues. Complicating the challenge is the fact that in certain narrow situations (e.g., emergency telephone calls placed over cell phone networks) carriers in some countries have legal obligations to deliver location information regardless of the preferences of the users. Of the many issues that the Geopriv working group is confronting, two might be of particular interest to the P3P workshop.

Granularity of location information: Among the possible location-focused privacy rules are possible rules about how precise a location should be distributed. For example, there may be situations where a user would not want her precise location disclosed, but would be willing to have her time zone disclosed. One proposal [2] to the Geopriv working group, for example, suggests that a user be able to reduce the granularity or specificity of location information along the following line:

A = no granularity change required
B = 10 kilometer radius (or within a defined latitude/longitude quadrant)
C = 100 kilometer radius (or within larger defined 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

Privacy of Privacy Rules: Another issue being considered by the Geopriv working group is an arguable need to be able to keep certain privacy rules private. Thus, although privacy rules might be conveyed along with location information in a Location Object, in some cases it may be appropriate (depending on the intended recipient) to strip out certain privacy rules. For example, a user might have three hypothetical privacy rules stating:

1. No one may retain my location information for longer than one day.
2. Business Acquaintance X can be told my specific location weekdays and my current city on weekends
3. Business Acquaintance Y can be told my current city on weekdays and no information on weekends.

The simple articulation of these rules, however, can disclose private information about the user's business relationships (and certainly the user would not want Business Acquaintance Y learning that he is disfavored relative to X). Thus, it may be appropriate for a trusted intermediary location server to receive all of the policies, but only forward policy 1 (along with the relevant location information) to either X or Y.

References:

[1] IETF Geopriv Working Group Charter, http://www.ietf.org/html.charters/geopriv-charter.html.

[2] "Core Privacy Protections for Geopriv Location Object," http://www.ietf.org/internet-drafts/draft-morris-geopriv-core-00.txt.(work in progress).