Trusted Intermediaries as Privacy Agents

Jim Fenton <fenton@cisco.com>
Cisco Systems, Inc.

Users have different expectations with respect to privacy on the Internet. A disclosure of a particular piece of information that may be perceived by one user as an assault on their privacy might be considered entirely appropriate to another. The current methods we have for managing our personal information on the Internet do not lend themselves to that situation well; it usually falls on the user to review a (frequently lengthy) Privacy Policy and determine whether that policy is consistent with their wishes. More often than not, the user has to decide to accept a Privacy Policy they haven't had a chance to read and understand fully, or has to trade their privacy for the utility of a service they want to use. This is one of the central principles of a concept known as Vendor Relationship Management (VRM).

Trusted intermediaries could provide a way for users to manage their personal information, including data managed by third parties (such as their credit score), in a manner they control. The intermediary would provide a way for the user to store their preferences regarding the disclosure of specific information about them, including the terms under which the information can be reused and repurposed. For example, a user might allow a particular merchant to record their address for purposes of purchasing a new automobile, but might not allow them to share that address with companies offering related accessories such as seat covers.

Another function that can be provided by a trusted intermediary is the disassociation of attributes about a user from other identifying information about them. An intermediary trusted by the user, and also trusted as a "fair broker" of attributes by the relying party, can make assertions about the user (e.g., that he or she is an adult) without actually disclosing who the user is. This is important for use cases such as those that involve whistle-blowing and anonymous crime reporting.

In order to support this mediated flow of information from an attribute provider to a relying party, standard formats need to be created for the representation of common information about users as well as for the terms of use that the user and /or the attribute provider want to impose on how that information is used. For example, a user might want to limit the dissemination of information on his or her age, or a credit agency might want to limit the reuse of an attribute asserting the user's credit score, since charging for that information is part of the revenue model for the attribute provider.

More broadly, internet protocols are sometimes described as "privacy enhancing". Privacy is really a social condition, well out of the scope of those of us that are involved with protocol development. The best we can do is to consider privacy needs and provide the capabilities to support privacy in protocols we develop. However, it is a societal decision whether, when, and how to use these capabilities.