`

Identity Rights Agreements and Provider Reputation

IDENTITY COMMONS Position Paper

Kaliya Hamlin, Identity Woman & Identity Commons
Phillip J. Windley, Brigham Young University
Aldo Castaneda, The Story of Digital Identity

Abstract: *While decentralized, user-centric identity systems provide hope that useful, secure identity systems may be possible on the Internet, ensuring that user data is protected in these system requires more than a technical solution. In this paper, we describe a project underway at Identity Commons to create a framework within which users can express their protection preferences (called identity rights agreements). Part of this project will establish a reputation system for identity providers and relying parties that engenders trust and lowers user risk.*

The emergence of decentralized, user-centric identity systems for use on the Internet leads to numerous social trust and privacy issues surrounding how identity information is used. Daniel Solove has called the current state of privacy protection an "architecture of vulnerability." [Sol04] In recent years there as been some governmental action with regard to privacy, but for the foreseeable future privacy will rely much more on the actions of individuals and organizations along with social norms than it does on legislation.

User-Centric Identity Systems

In user-centric, decentralized identity systems, there are typically three parties to any identity transaction. The user is the person (or entity in a broad sense) whose identity attributes are the subject of the transaction. The identity provider is the party that holds the attributes and is supplying them to the relying party, the entity requesting the attributes for some use.

In a user-centric system, the identity provider only transmits those attributes that the user has specifically authorized in response to a specific request from a relying party. These user responses might be automatically provided in some circumstances according to rules the user has set up. The identity provider and the user could be under the control of the same entity in some transactions.

The goal of a user-centric identity system is to put users in control of their identity information. However, under current regimes, they have little control over what the relying party does with their identity attributes.

Identity Commons was formed in 2001 to address the social trust issues arising from digital identity. Following a discussion at the Internet Identity Workshop in October 2005 in Berkeley, California, Identity Commons has been focused on the development of Identity Rights Agreements and a Service Provider Reputation Network. Together, identity rights and service provider reputation can provide significant protection for user identity attributes.

Identity Rights Agreements

Identity Rights Agreements (IRAs) [Wind06] are a way for users to express their preference about how their personally identifying information is collected and used. At least initially, IRAs would be voluntary in the sense that they would not be enforced by a technology system. On the other hand, IRAs set up a framework where existing legal frameworks and contract law could be used to enforce them.

IRAs are patterned after the Creative Commons [CC05], which gives users an easy way to assert ownership of intellectual property (IP) and to selectively claim specific rights associated with that IP. Creative Commons (CC) uses a four layer stack to communicate the claims:

1. Easily recognizable logo
2. Human readable agreement
3. Legal document layer
4. Machine readable metadata

This stack provides superior usability because of layers one and two, but couples those in a structural way with the legal language and machine readable metadata. One key difference: CC is based on copyright law, whereas IRAs would be based on contract law.

Like CC, IRAs would come in a limited set of configurations. This limited set of configurations allows users to quickly and easily assert (or accept) a well-known and understood set of terms regarding the use of their data. For example, here is a potential spectrum of choices that might be represented by a set of standard identity rights agreements.

- Post publicly (broadcast)
- Share with anyone, but may not broadcast
- Share with partners with whom you have a legal contract to honor this agreement
- Share with no one
- Store encrypted
- Use for this purpose and destroy

The above are just examples. The Identity Commons community is working to gather requirements and legal advice for the initial set of IRAs. Still, the idea should be clear: a simple taxonomy of increasing protection requirements that users can assert about their identity data.

Ideally, each attribute associated with an identity would be able to be separately licensed. This is necessary because while most people are glad to have the URL of their Web site broadcast freely, they might choose to have their phone number kept by the relying party and want their SSN used and then destroyed or at least stored encrypted.

IRAs could be attached to identity attributes in a number of ways. Assume that the identity attributes are transmitted in XML. The attributes could be wrapped in an IRA envelop, the IRAs could be inserted as attributes to the XML tags, or the IRA could reference the XML tags by ID. All three of these, and perhaps others, will be needed to make IRAs compatible with various identity systems. We expect that user interfaces would make the XML detail invisible to the user, while allowing machine readability.

As discussed above, IRAs would have a human readable component linked to legal language and metadata. This would require that each level in the hierarchy have an identity of its own. Further, IRAs would be versioned to allow for future changes. We envision that each level in the hierarchy would be identified by a URI or XRI-based identifier. Here is an example:

```
uri:identityrights.org/ira1.0/level0
uri:identityrights.org/ira1.0/level1
...
uri:identityrights.org/ira1.0/level7
```

These names would be used to link together the various levels of the IRA stack.

`

Relying parties requesting identity information would receive back a standard response indicating the IRA associated with that identity data. Proceeding with the transaction would be interpreted as agreeing to abide by the IRA requirement. IRAs might be made legally binding by the use of electronic (not digital) signatures. The Uniform Electronic Transactions Act of 1999 [UETA99], which has been adopted by 28 states, makes users action (clicking on a Web page, for example) legally binding electronic signatures under certain circumstances.

Because IRAs contain metadata consistent with the desired protection level, it is conceivable that sophisticated negotiation engines could arise that would negotiate on behalf of a user and relying party when relying parties can't abide by the preference expressed by the user. These systems would be rule-based. For example, my default preference may be to have my SSN used and then destroyed, but I am willing to have it stored so long as it's encrypted. A relying party that can't provide the requested service without keeping the SSN could then negotiate with me, automatically, to store the encrypted SSN. Automatic negotiation is much more difficult without the standardization provided by IRAs or something like them [Thib00].

Service Provider Reputation Network

Contract law can only provide so much protection for identity rights because the courts can be an expensive and unwieldy place to enforce requirements. Infractions would have to be widespread and egregious before most wronged parties would be willing to sue. The second part of our proposal aims to create frameworks whereby social pressure, in the form of reputation, can be brought to bear on identity providers and relying parties.

In a user-centric identity system, one key question for users is "who to trust?" How can end users trust an identity provider to protect their personally identifiable information? Further, how do they know a relying party will honor IRAs?

The early innovators of user-centric identity services realize that fostering trust is a critical component to the market success of these new services. Identity Commons is working with these developers to create a Service Provider Reputation Network to support mutual accountability and best practices in this emerging space. Part of the need is to support trusted authentication of the sites that users are interacting with.

Service Providers who are part of this network would be bound to honor the IRA's they have with their users. IRAs could be enforced by a combination of technical and social means. Not abiding by agreements that you have signed would be grounds for negative remarks on your Identity Commons reputation, or ultimately expulsion from the Identity Commons list of approved service providers.

The community participating in developing trusted user-centric services includes YADIS (http://www.yadis.org), OpenID (http://www.openid.net), LID (http://lid.netmesh.org/), XRI-based i-names (http://www.xdi.org), MyXDI (URL http://www.ootao.com), and SXIP (http://www/sxip.org).

Conclusions

Protecting user identity data on the Internet requires more than technical solutions. Whatsmore, new legal solutions are likely to be a long time coming and may still not be satisfactory. We have described a project underway at Identity Commons to establish a standardized way for users to express their preferences with respect to how individual identity attributes are used by identity providers and relying parties. We have further described a reputation network that would help users decide who does and who does not abide by IRAs. We seek feedback on these ideas and help in defining these frameworks.

References

[CC05] Creative Commons, *Cultivating the Public Domain*, http://creativecommons.org/about/legal/cultivating

[Wind06] Windley, Phil, August 06, 2005 - Identity Rights Agreements http://www.windley.com/archives/2005/08/identity_rights.shtml

[Sol04] Solove, Daniel J. *The Digital Person*, New York University Press, 2004

[UETA99] *Uniform Electronic Transactions Act*, 1999, http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm

[Thib00] The following papers by Robert Thibadeau of CMU illustrate how a small set of widely-referenced agreements can dramatically simplify policy negotiation.
http://dollar.ecom.cmu.edu/p3pcritique/ (especially the very end)
http://yuan.ecom.cmu.edu/pspnote/