Informed Consent and Privacy Management

End-users of online services are dependent on multiple players for preservation of the privacy of their personal information. In particular,

- IdPs and APs must release personal information only to authorized SPs, and
- Authorized SPs must not misuse the information they receive.

Informed consent is crucial to the process used to authorize SPs to receive personal information.

Central to the design of a privacy manager is how to operationalize informed consent. Informed Consent is a widely considered topic in other contexts, with deep discussions in bioethics, research, and legal systems. (See, for example, http://depts.washington.edu/bioethx/topics/consent.html.) In all those cases, the conversations focus on the complexities and subtleties of the issues, aimed at the sophisticated practitioner. When informed consent is applied to the electronic release of information by a user on the Internet, the issues and approaches are quite different. If only by scale issues, complexities and subtleties are to be avoided; at least initially broad and simple tools must be crafted for the mass markets.

Several related concepts are within the scope of this discussion:

Warnings – messages provides by applications or operating systems that are binary both in nature (e.g. continue or not) and in successive layout. They represent a very broad category of HCI.

Consent – messages typically targeted to an end-user to gain permission to release information to a third party. The information is frequently personal information. Consent is often selective – release of small number of attributes may be needed for one service, whereas a different bundle of attributes may be needed for a related but distinct service.

Notifications –A message sent to a user, informing them that a transaction has taken place. They may be triggered by class of event, by preset time, or by dynamic issues. Notifications do not stop an event from happening.

Audit/Penalities/Policing – Users want to know that the IdP's are playing by the rules, else why bother thinking about consent. There needs to be a set of consequences for miscreants so that users can trust that consent and privacy management are meaningful actions.

Downstream reuse - Research has shown that users are more concerned with inappropriate "downstream" use of released information than with the length of time that information can be retained by the initial relying party. However, the understandings of "downstream" are unclear. A set of autonomous applications hosted at a single portal may be a single pool of proper use or inappropriate downstream use, depending on a set of clues given to the user.

Avoiding Consent

When is it not required?

When is it not consent but merely a condition of use for a service? Typically a rich legal issue and out of scope for this document but critical in ecosystem practices.
Where and when is notification separate from consent required?

Sequencing and structuring Informed Consent for a Privacy Manager

a. A priori and or static elements

1. RP presentations need to present their information with clarity and understanding of the choices

e.g. UK Code of Good Practices – see the examples in http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_NOTICES_COP_FINAL.ashx

+ 2. RP Certifications and standards in place

e.g. Research and Scholarship certification – see https://spaces.internet2.edu/display/InCCollaborate/Research+and+Scholarship+Category

+ 3. IdP participation/certification/etc in place

e.g opt-in IdP mechanisms in the above Research and Scholarship certification

4. Others?

b. Run-time/transaction components

Default setting (by product, by enterprise setting, etc)

+ A basic consent screen with information about what is being released (possible triggers?)

+ A "tell me more" capability that provides third-party metadata to inform the user in their decision (Note – what are other suggested sources – do all come in via metadata or local feedback and prior use or other hints?

+ A revocation of consent mechanism (where and how)

+ An optional process of notification settings – timing, modalities, exceptions, etc

+ An optional process of downstream use settings on released information, etc. How to deal with or represent the fuzzy perimeters of downstream.

+ Others?

c. Post-transaction options

Setting preferences, authorizations at an UMA authz server, etc

Others?