Emerging Standards in User Consent

Resolving Privacy Challenges Through Innovation

Nick Taylor | Director - Customer Engineering | @nicktaylor
Top three organizational challenges

1. Complying with privacy laws and regulations

2. Complex and fragmented consent experiences that plant consumer doubt about your trustworthiness

3. Can’t enable consumer-controlled data sharing across cloud, mobile, and IoT sources
To build lasting trusted digital relationships, stakeholders need to meet in the middle

**Risk perspective**

“Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. …

In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller…”

**Business perspective**

*We value personal data as an asset*

Our *customers’* wishes have value

Our customers have their *own reasons* to share, not share, and mash up data, which we can address as value-add
The EU General Data Protection Regulation: it’s different this time

• GDPR applies to every organization selling to or monitoring anyone in the EU
• GDPR has a firm deadline (May ‘18), high penalties (4% of global turnover), and high aspirations
• Digital teams need to take the GDPR challenge in hand to ensure a triumph vs. a tragedy
• Providing customers with data sharing controls goes beyond compliance to bilateral digital trust and the ultimate service stickiness

• PSD2 asks for explicit user consent too - the tide is turning
The holistic view

Single view of the consumer

- Lifecycle management of a user profile and their data sharing preferences
- Secure storage of profile data
- Anonymised syncing of profile data and connector based integration to third-party systems

Giving the consumer a single view of their consents

- ToS and privacy policy capture at registration and authentication time
- Social sign-in
- Social registration
- Social consent management

Giving the consumer control over their consents

- Interoperable, user-driven, proactive and reactive sharing flows
What’s the latest on User Managed Access (UMA)?
Key benefits to users

• Sharing, unsharing, and editing of sharing preferences allowed at any time, **without external influence**
  • Not just opt-in or opt-out when asked
  • A selective sharing paradigm for an IoT landscape that demands it
• Possible to offer a service that **centralizes sharing preference management** across data services for user convenience
  • The central service **doesn’t see any of the data**
  • Data is fed fresh from each individual service
• The user can **selectively share** whatever “grain” of access each data service offers
  • Such as read vs. write, or weight vs. fat mass
Key benefits to service operators

• A permission model that **scales for user growth**
• Enables living up to a promise of **transparency** and building trusted digital relationships
• Enables addressing new **regulations** that demand freer choice in consent
User Managed Access 2.0

• Evolving UMA - feature parity but easier to use

• Closer to OAuth, OpenID Connect, and other familiar technologies
  • OAuth server deployers should find it easier to adopt: it’s mainly an extension OAuth grant
  • Developers should find it easier to work with: it’s mainly OAuth

• Readier for IoT, scale, and disconnected-service use cases
  • And it is extensible where needs are yet unknown

• Readier for wide ecosystems
  • Bob doesn’t need to provide any claims (e.g., “log in”) to Alice’s authorization server until just before he tries to access her protected resource
UMA 2.0 Timeline

Dec 2015: UMA V1.0.1 Recommendations published
Q1 2016: 2.0 roadmap themes discussed and decided
Early Q2 2016: Major decision-making begun
May 2016: Spec editing begun
Jan 2017: Completed editing of key design issues
Mar 2017: Completed editing of follow-on issues
Apr 2017: Completed spec refactoring
Thank you!