The Quest...

• Last year I said we were on two journeys: law + tech
• Trying to reach the same goal:
  – Easy to use, Privacy-respecting, Secure Authorisation
On the legal side...
It’s the politics, stupid

• Draft Data Protection Regulation now deep in politics
  – Basic disagreement on what individuals want
  – Parliament & Council haven’t reached initial negotiating positions
  – >3000 amendments proposed
  – Privacy experts want to start again!

• And then PRISM
  – “No Personal Data release to countries that spy”
  – Errr... Plenty of those inside the EU!

• Federation needs unlikely to be heard in the noise 😞
Where now?
Back to basics

- Minimise data/processing
  - Whatever privacy law emerges, less is going to be better
- Minimise surprise
  - Happy users won’t complain to lawyers
- Reduce (regulatory) risk, don’t hope to eliminate it
  - Aim: benefit outweighs risk
Benefits of single identity may justify ePTID pain (Jens)
Services need (just) adequate and relevant data (Jens)
Zero-attribute authN (Remco)/Last-resort IdP (Marco)
  – Find out what SPs really need
Identify user only for accounting/audit (Marco)
  – Maybe it’s enough to know those policies/processes exist?
Negotiate access vs attribute provision (Jens)
Support VO-specific attributes (e.g. %FTE) (Heather)
Use “account” as a way for user to view/control data flow (Jens)
Allow users some control of policies (Jens)
Let communities define own location/access policies (Johannes)
‘Goldilocks’ complexity (Heather)

Silently “just working” => hard to excite users (Frank)
Willingly accept the risk of reliance on a person/entity/system to act [in way that helps] (Bob Cowles)
Entity categories as risk/benefit categories (pers.comm.)

Without clear law, this seems the only approach...
We’re progressing...
Enjoy the boat trip

Janet, Lumen House
Library Avenue, Harwell Oxford
Didcot, Oxfordshire
t: +44 (0) 1235 822200
f: +44 (0) 1235 822399
e: Andrew.Cormack@ja.net
b: https://community.ja.net/blogs/regulatory-developments