janet

Federated AAI and EU Law

Andrew Cormack
Chief Regulatory Adviser, Janet
@Janet_LegReg

The puzzle

- Federated AAI recognised as a Privacy Enhancing Tool
  - According to UK and Ontario Privacy Commissioners
  - Less information processed, more reliably
  - So privacy law ought to encourage its adoption
- Current EU law designed for world of 1995
  - Can’t design FedAAI to fit the law ☹
    - We tried that with cookie law ☹
  - Legal uncertainty may actually discourage adoption ☹

Problems with EU law (1995 Directive)

janet

- Doesn’t handle three-party relationships (user/IdP/SP)
  - And we’re already thinking of four or more (social Id, Virtual Orgs)
- Status of indirectly-linked identifiers is unclear
  - German courts even disagree with each other!
  - Some choices lead to impossible-to-fulfil duties!
- Correct basis for processing is unclear
  - Consent? Necessary for contract? Legitimate interests?
- Rules for exports from EEA are unclear
  - Member State formalities and approaches incompatibly different

The aim: accurate authorisation

janet

- Technically
  - Easy to use,
  - Privacy-respecting,
  - Secure
- Legally
  - With a clear basis,
  - That encourages privacy-protecting options
- How to get there?
  - National federations/international agreements (REFEDs, eduGAIN)
  - New draft *Data Protection Regulation* (2012-present)

On the legal side...

US public domain by NARA/Wikimedia Commons

It’s the politics, stupid

janet

- Draft *Data Protection Regulation* now deep in politics
  - Basic disagreement on what individual citizens want
  - Commission draft Jan 2012
  - Parliament response Oct 2013
    - After considering >3000 amendments to COM draft
  - Council haven’t published **initial** negotiating position
    - Seem to be aiming at 2015
  - Privacy experts want to start again!
- And then PRISM/Snowden
  - “No Personal Data release to countries that spy”
  - Errr... Plenty of those **inside** the EU!
- Federation needs unlikely to be heard in the noise ☹

Improvements in EU law (2013 Nov draft)?

janet

- Doesn't handle three-party relationships (user/IdP/SP)
  - And we're already thinking of four or more (social Id, Virtual Orgs)
- Status of indirectly-linked identifiers is unclear
  - German courts even disagree with each other!
  - Some choices lead to impossible-to-fulfil duties!
- Correct basis for processing is unclear
  - Consent? Necessary for contract? Legitimate interests?
- Rules for exports from EEA are unclear
  - Member State formalities and approach incompatibly different

Improvements in EU law (2013 Nov draft)?

- Still doesn't handle three-party relationships (user/IdP/SP)
- Recognises that indirectly-linked identifiers are different
  - And that impossible duties shouldn't be created
  - But much argument on what rules should apply
- Correct basis for processing still unclear
  - Consent? Necessary for contract? Legitimate interests?
- Rules for exports from EEA being argued
  - But differences between countries should be reduced
- Still can't design FedAAI to fit the law ☹

Beyond Europe

janet

- Things may not be so different
  - Many countries implementing EU-inspired laws
  - US FERPA/HIPPA may actually be more restrictive than EU
  - And spying doesn't just happen "over there"
- But EU law struggles to recognise that
  - Formal recognition of equivalent countries is slow
  - EU-US Safe Harbor can't cover public sector
  - Doesn't actually regulate spies (despite what you may have heard)

janet

Where now?

US public domain by Fish & Wildlife Service/Wikimedia Commons

Back to (privacy) basics

janet

- Minimise data/processing
  - Whatever privacy law emerges, less ought 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
  - Law often requires "appropriate"/"equivalent"/etc. anyway

Minimisation

- Choose the right attribute
- Service Providers
  - Do you need name/e-mail, or will a unique ID do?
  - Do you need it from the IdP or will self-asserted do?
    - Home-for-homeless/socialID only offer self-asserted anyway
- Identity Providers
  - Provide privacy-protecting values, so SPs can rely on them
  - Deal effectively with reported problems, so SPs don't have to
  - Populate real-world identities as some services do need them

Surprise

- Most users want authorisation to happen!
- Service providers
  - Only use attributes to provide requested services
  - Tell users/IdPs/federations what you do and don’t do
  - Unexpected processing makes both law and users unhappy
- Identity providers
  - Document your default release policy
  - Consider notification/consent tools so users can find out

Risk/Benefit

janet

- Federated education services benefit user and organisation
  - And protect privacy better than the alternative
- Service Providers
  - Try to fit the appropriate REFEDs (draft) service category
    - Collaboration: users need to recognise each other, R&E focussed
    - Library: need to assign users to licenses and save their choices
    - Association: just need to know it's a student/member/etc
    - ... (let us know if you aren't one of these)
- Identity Providers
  - Set reasonable default release policies: nice when things "just work"
  - Consider releasing more (needed) attributes for more R&E benefit
  - Accept reasonable level of compliance

Act local: Think global

- National solutions may look easier
  - Shared assumptions/culture/law
  - And some things don't cross borders (e.g. course codes?)
  - Or won't be of interest to outsiders (e.g. internal structures)
- But international is increasingly important
  - For research/education/work
  - Harmonisation/standardisation easier than translation
  - Find/develop/propose common approaches to common problems
    - "close enough", rather than "not invented here"
  - Should save effort now: will save pain in future

We’re progressing...

janet

Questions?

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