Privacy and Services

INTERNET®

Topics

- Privacy, consent, anonymization, etc.
- EU Privacy directive
- OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) TC

kjk@internet2.edu

Privacy

- Includes spills, user consent, stateful privacy, active privacy management, anonymization, etc.
- Complicated greatly by international considerations and weak US national laws
- Complicated greatly in loosely coupled and federated engagements

kjk@internet2.edu

Federated Identity and Data Protection Law

Andrew Cormack, Eva Kassenaar,
Mikael Linden,
Walter Martin Tveter

INTERNET2®

Which Law?

- Directive 95/46/EC
  - Processing of personal data allowed when
    - Required to perform contact with data subject, or
    - Required to satisfy legal duty, or
    - If data subject gives free, informed consent
      - And does not withdraw it
  - Different conditions apply to each of these
- NB National laws may vary this a bit

kjk@internet2.edu

What does it mean for FAM?

- FAM can be a good thing
- ***IF*** it satisfies the relevant conditions
  - Which look like good practice anyway…
  - See next two slides
    - Which use RFC-speak…
    - And not too much law-speak…

kjk@internet2.edu

Identity Providers

- Must identify which services are necessary for education/research
  - Must consider whether personally identifiable information is necessary for those services, or whether anonymous identifiers or attributes are sufficient;
  - Must inform users what information will be released to which service providers, for what purpose(s).
  - May release that necessary personally identifiable information to those services;
- May seek users' informed, free consent to release personal data to other services that are not necessary for education/research
  - Must inform users what information will be released to which service providers, for what purpose(s);
  - Must maintain records of individuals who have consented;
  - Must allow consent to be withdrawn at any time;
  - Must only release personal information where consent is currently in effect.
- Should have a data processor/data controller agreement with all service providers to whom personally identifiable data is released.
- Must ensure adequate protection of any data released to services outside the European Economic Area.

kjk@internet2.edu

Service Providers

- Must consider whether personally identifiable information is necessary for their service, or whether anonymous identifiers or attributes can be used;
  - Should obtain that information from home organisations;
  - Should have a data processor/data controller agreement with all home organisations from whom personally identifiable data is obtained;
  - If no such agreement is in place, must inform users what personal information will be obtained, by which service providers, for what purpose(s).
- May request personal information from users
  - Must inform users what information will be released to which service providers, for what purpose(s);
  - Must ensure that users who do not provide information are not unreasonably disadvantaged;
  - Must maintain records of individuals who have consented;
  - Must allow consent to be withdrawn at any time;
- Must cease processing data when consent is withdrawn

kjk@internet2.edu

Some particular thickets

- Inconsistency of PII
- IP addresses
- EPTID

kjk@internet2.edu

OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) Technical Committee

- Enterprises, including the healthcare enterprise, need a mechanism to exchange privacy policies, consent directives and authorizations in an interoperable manner. At this time, there is no standard that provides a cross-enterprise security and privacy profile. The OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) TC will address this gap.

kjk@internet2.edu

- The need for an XSPA profile has been identified by the security and privacy working group of the Healthcare Information Technology Standards Panel (HITSP). HITSP is an ANSI-sponsored body charged with identifying standard building blocks that can be leveraged to implement common healthcare use cases. The XSPA profile will require the participation of subject matter experts in several areas, including WS-Federation, SAML, WS-Trust, and possibly others noted below.

kjk@internet2.edu

- These functions will at a minimum support the HITSP Access Control Transaction Package specification TP20, including those access control capabilities required to support the HITSP Manage Consent Directive Package specification TP30. This includes the support of reliable and auditable methods to identify, select and confirm the personal identity, official authorization status, and role data for the subjects, senders, receivers and intermediaries of electronic data; data needed to convey and/or enforce permitted operations on resources and associated conditions and obligations; and reasonable measures to secure and maintain the privacy and integrity of that data from end to end.