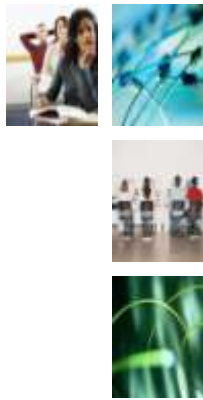


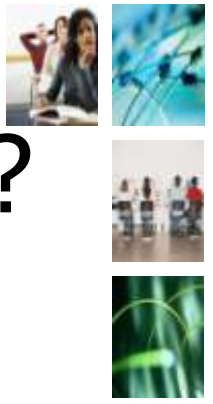
Federated Identity and Data Protection Law

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



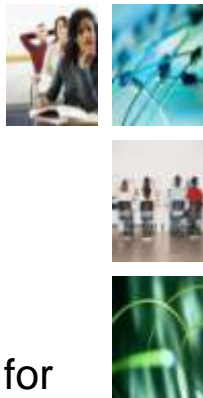
Which Law?

- 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



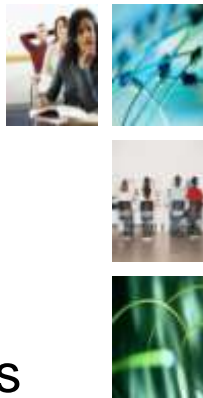
What does it mean for FAM?

- 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...



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 - Must allow consent to be withdrawn at any time;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.



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