InCommon and Global Federation Update
InCommon

- Growth in use and robustness
- Robustness of infrastructure and beginnings of self-service federation management
- Agency use – NSF (CC*) and NIH
- Carefully expanding the trust model – the balance of more trust vs. higher barriers
  - MFA
  - Baseline Expectations
- Dynamic metadata slowly rolling out; affects discovery interface
- Attribute release and R&S continue to be vexing problems
- Other activities – IdP of Last Resort, Steward program – moving forward but needing business models
International Dimensions

• EduGAIN and interfederation growth/issues
• SirTfi for Security and Incident Handling
• Snctfi Activity for Collaboration-scale authorization
• Bridging cultures and regulatory regimes
  – Compensating controls
  – GDPR
Snctfi and VO authorization policies

• Allows a cluster of related resources to present a consistent management of the cluster to the federated R&E world.
  – Each of members of the cluster can be assumed to adhere to assertions about the cluster (e.g. incident handling, data minimization, etc.)
  – Requires a set of internal policies for compliance
• https://wiki.geant.org/display/AARC/Snctfi
Federated OIDC

- OIDC (and Oauth) were developed as bilateral protocols for mobile and light trust apps
- Now showing value in multilateral situations
- Client registration becomes the key step
GDPR (General Data Protection Regulation)

- Created by EU to manage data protection uniformly across the EU
  - Is binding for every member EU nation
  - With many global impacts
- Covers a vast waterfront of issues from tracking to attribute release to right to be forgotten to data breaches to . . .
- Consists of a set of rules (Articles) and then example interpretations of the rules in key areas (Recitations)
- Penalties of up to 4% of global revenue
- Identifies six reasons for attribute release, including contract, consent, national security, legal actions, etc.
  - Specifies when consent is not to be used, when it should be used, the quality of the consent, etc.
- It affects many, perhaps most, US institutions.
EU Establishments
Non-EU Establishments or organizations
Other goods or services or engaging in monitoring within the EU

Lawful Processing
Collection and processing of personal data must be for “specified, explicit and legitimate purposes”
- with consent of data subject or necessary for
  - performance of a contract
  - compliance with a legal obligation
  - to protect a person’s vital interests or task in the public interest
  - legitimate interests

Consent
Consent must be freely given, specific, informed, and unambiguous.

Responsibilities of Data Controllers and Processors
Data Protection Officer (DPO)
Designate DPO for a activity involves regular monitoring or processing large quantities of personal data.

Record of Data Processing Activities
Maintain a documented register of all activities involving processing of EU personal data.

GDPR
www.teachprivacy.com

Enforcement
Fines
Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies:
compensation for material and non-material harm

International Data Transfer
Adequate Level of Data Protection
Privacy Shield
Model Contractual Clauses

Data Breach Notification
Provisional data breach: “where each of the following conditions is met: (a) and (b) and (c): (a) the operation involves personal data; (b) the data subject’s and the data controller’s personal data; (c) the data controller has not taken appropriate and necessary measures to prevent the breach from occurring”
If likely to result in a high privacy risk: notify data subjects and if likely to result in a high privacy risk: notify data subjects no later than 72 hours after discovery.

Rights of Data Subjects
Right not to be subject to a decision based solely on automated processing, including profiling.

TeachPrivacy
Worldwide awareness training by Prof. Daniel J. Solove

Please ask permission to reuse or distribute
Some gnarly details

• PII and Sensitive PII
  – Almost everything is PII – from IP address to persistent identifiers
    • Some identifiers are not e.g. ePTID
  – Sensitive PII
    • Religious, ethnic, sexual, health, trade-union membership, etc.
    • Requires special handling in everything from protection to presentation

• Research data use
• Right to be forgotten
  – Cloud based backups
• “This call may be recorded…”
• Data breach notifications
  – 72 hours
• Data protection officer and individual data protection training