EU
General Data Protection regulation (GDPR)

Background

- EU Privacy Laws have been advanced (compared to the US) but chaotic
  - 28 states interpreting a high-level EU directive
  - Applied to EU wide interactions, with local exceptions
  - Blunt instrument with little force
- Then Google, Facebook and the cloud
- Then Snowden
- Dec 2015 – Final adoption of EU General Data Protection Regulation (GDPR)
  - Effective in Jan 2018
  - Regulation, not directive (i.e. MUST, not SHOULD)

Key points

- Applies to all EU states
- Applies to all entities worldwide that have EU customers or clients (!)
- Potentially massive fines (4% of global revenue)
- Revocable consent
- “Clearly” informed consent
- Right to be forgotten
- Right to data portability between IdP’s
- Sets age of consent from 13 to 16 (allows local exceptions)

Some implications

- IaaS
  - Data processors share responsibilities with data controllers (e.g. VM providers may need to know what's in the VM)
  - 72 hour breach notification to authorities
- Implementing the right to be forgotten
  - Managing backups and use of metadata
- Implementing "clearly" informed, revocable, fine-grain consent
- Stricter sense of PII, including race and national origin

More implications

- Risk based requirements on companies to perform data protection assessments on full data life-cycle
- Almost one-stop shopping for multi-jurisdictional resolutions
- BAE++ (back-end contracts need to be approved by data controller)
- Data Protection Officers (~CPO) required with SME (small to medium enterprise) exceptions
- Safe Harbor 2.0 being discussed by EU-US now

GDPR and Scalable Consent

- GDPR
  - requires consent “to be freely given, specific, informed and unambiguous" and expressed affirmatively "either by a statement or by a clear affirmative action.
    - Freely given not available for employees; unclear for students
    - Information must be in clear and plain language
  - Requires user to be able to decline/revoke consent
  - Must be purpose-driven; change of purpose requires reconsent
- Scalable Consent
  - TIER related effort, catalyzed by NIST funding, to implement an architecture and code (internals and UI) to support multiprotocol consent
  - Targets are both Shib IdP and stand-alone components
  - May address much of the GDPR requirements when coupled with federation-level services (metadata, etc.)

GDPR Takeaways

- A “HIPPA/FERPA/FISMA” class object now on the radar
- Sets a high bar globally for data protection
- Very early in the deploy cycle; uncertainties abound
- Significant impacts on campus IT
  - infrastructure (consent support, reengineered storage and backups, etc)
  - policy (data protection officers, risk assessments, etc)
- Good resource: https://secure.wisegateit.com/member/resource/show?id=18345

  (and its federated!)