Privacy Stew and Stewardship

Ken Klingenstein
Internet2
Topics

• Privacy Stew – what’s happening
  - GDPR update
  - Privacy Shield demise
  - Canadian public identity initiatives – DIACC and Notice/Consent
  - COVID-19 tracing and privacy
  - Consent-informed attribute release – CAR
    - Relevance to Seamless Access proposed bundles

• Privacy Stewardship – how to deal with it
  - How does an institution chart a course
    - Figuring out what’s important
  - Half-role of a Chief Privacy Officer
    - Figuring out who’s responsibility it is
  - Building Privacy Partnerships
TERRITORIAL SCOPE
EU Establishments
Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.

PERSONAL DATA
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
- task in the public interest
- legitimate interests

RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

RIGHTS OF DATA SUBJECTS
Access and Rectification
Purpose Specification and Minimization
Right to Erasure
Right to Data Portability
Transparency
Automated Decision Making

SENSITIVE DATA
Religious or Philosophical Beliefs
Political Opinions
Sex Life
Health

EFFICACY JUDICIAL REMEDIES
Compensation for material and non-material harm.

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.

INTERNATIONAL DATA TRANSFER
Adequate Level of Data Protection
Model Contractual Clauses
Privacy Shield
Binding Corporate Rules (BCRs)

EUROPEAN DATA PROTECTION OFFICER (EDPO)
Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.

WORLDWIDE OVERSIGHT
If likely to result in a high privacy risk Æ notify data subjects and notify supervisory authorities no later than 72 hours after discovery.

WORKFORCE AWARENESS TRAINING BY PROF. DANIEL J. SOLOVE
www.teachprivacy.com
GDPR (General Data Protection Regulation) update

- Emergence of both “basis for release” and “purpose of use” as key issues
  - Basis for release creates institutional compliance requirements
    - Documenting basis: contract, consent, national security, legal actions, etc.
  - Purpose of use is an SP requirement and needs taxonomies
    - Interactive Advertising Bureau (IAB redux) has one; R&E needs a different one

- Major clarification of issues in May
  - Abuse of legitimate interest
  - Poorly done consent and cookie walls
  - Coarse grain too coarse

Privacy Shield Demise

- Privacy Shield was a kludge to replace a hack
  - The original agreement Safe Harbor, covered transfer of EU data to US
  - Corporate employees, customer, social use cases covered
  - Struck down by EU several years ago, replaced in the US with PrivacyShield
- Privacy Shield struck down by ECJ
  - Shrems II
  - Core reason was concern for protection against US gov access
  - Impacts a lot
- Remedies not great
  - Standard contract clauses
  - Encryption upon encryption
DIACC and the Pan-Canadian Trust Framework

- Canadian approach to public digital identity
- Modeled after NSTIC effort within NIST in the US but learned from that experience
- Trustmark is voila!
- Impressive list of identity providers, SP’s lining up
- In early rollout right now, but enfolds major existing infrastructure
- Explicit notice/consent requirements
  - https://diacc.ca/interoperability/notice-consent-overview-conformance-draft-recommendations/
Pan Canadian Trust Framework

Figure 2. Pan-Canadian Trust Framework Model Visual Draft
Consent will normally be sought. While data protection laws allow for data to be collected without consent in certain circumstances, these circumstances do not typically apply to digital identity solutions.

Consent will always be “opt-in” (i.e., the Subject must perform an action to provide consent).

Notice and consent must take place at the time of transaction that it applies to;

Consent can be only for the transaction in progress (i.e., one time); or be given for a period of time (i.e., subscription services).

Withdrawal of consent applies to future transactions where consent has been given for a period of time.

Consent will always be explicit, and in language that is easily understood.

Digital identity solutions will provide obvious and straightforward means for the Subject to manage consents, preferably in one place.

COVID-19 and Privacy

- Rapid adoption of new (cloud) services
- Many with sub-optimal Data Protection and Intellectual Property clauses
- But we couldn’t have stayed open without them
- Which risk is worse?
- Gartner idea (EUNIS 2020 conference): Future arrived 57 months early
- Contact-tracing has its own unique privacy issues
Consent–Informed Attribute Release (CAR)

- Joint effort of Internet2 and Duke University, emerging from an NSTIC grant on Scalable Privacy
- Effective end-user management mechanisms in-line and self-serve (personal privacy console)
- Effective enterprise management of both presentation and policy formulation
- Unexpected compliance benefits
- Open source software (Apache style license)
- “will work for attributes” – original Shib T–Shirt
Research-r-Us (We Are Your People) is requesting access to your personal information.

**Review and edit what you provide to this site**

Edit Amber’s presets:

- Permit
- Deny

- Display Name: Annie E.
  To personalize our pages for your viewing

- Email Address: ugrad@mail.amber.org
  To contact you about events and offers you may be interested in

- Federated Affiliations: student@amber.org
  To establish your research relationship with your organization (required)

- Federated Principal Name: ugrad@amber.org
  To uniquely identify you in our database

- Official Name: Ann Elk
  To track your real identity in our partners’ databases

**Requested information held by:**

Amber IDP

R&S R US

Research-r-Us (We Are Your People)

We serve the Research Needs of Scholars

Research-r-Us (We Are Your People)’s privacy policy

- Don’t show this screen the next time I log into Research-r-Us (We Are Your People)

Save and Continue ➔ Cancel ❌
Faculty — limited access content UI

ContentRUs (The Content People) is requesting access to your personal information.

Review what you provide to this site

Update your settings:

- Permit
- Deny

- Departmental Fund code: 12130100 (School of Law)
- Departmental Fund code: 12171555 (Sociology)
- Display Name: Professor Godel
- Email Address: iamfaculty@avalonmail.com

Requested information held by:
Amber IDP

CONTENTRUS

ContentRUs (The Content People)
ContentRUs Content Management Service (LLC)
ContentRUs (The Content People)'s privacy policy

Don't show this screen the next time I log into ContentRUs (The Content People)

Save and Continue  Cancel
Self-service consent UI
An API view
Privacy Stewardship

- Players
- Process
- Partnerships
Players

- Legal and Compliance
- Chief Privacy Officer/CISO
- Central IT
- Registrar
- Libraries?
CPO Responsibilities

Graph from “The Evolving Landscape of Data Privacy”, Educause 2020
Process (thanks to Educause quick survey 11/10/20)

- **Reviews** vendor contracts to ensure that terms and conditions protect institutional data
- **Provides** privacy education training and awareness across the institution
- **Develops** institutional privacy-focused programs and policies related to federal, state, and local regulatory guidelines
- **Monitors** compliance with acts and regulations (e.g., HIPAA, FERPA, GDPR)
- **Conducts** regular privacy reviews to identify privacy-related vulnerabilities
- **Serves** as the centralized contact and authority for privacy issues
- **Supports** technology related to privacy
Three new seamless access bundles under discussion
- Authentication only, anonymous authorization, pseudonymous authorization (personalization/state)

“standards” process
- Seamless Access WG
- Refeds Schema WG
- Federation and IdP adoption
- Contract Language WG in Seamless Access

Concern about metrics and usage statistic attributes
CAR and Seamless Access Entity Categories

- Entity Categories are really Attribute Bundles
- Possible uses of bundles
  - Preconfigure IdP release w/o consent
  - Recommend to user with consent
  - Notice and transparency
- Can address Refeds feedback about including access and metrics in the same bundle via required/optional
Discussion

- In which privacy processes do you have a role on campus?
- Which privacy processes should you have a role in on campus?
  - What do libraries bring to the table?
- Learning the languages of each other
- How to get involved
  - E.g. how do open shelves relate to contact tracing