Privacy Stew and Stewardship

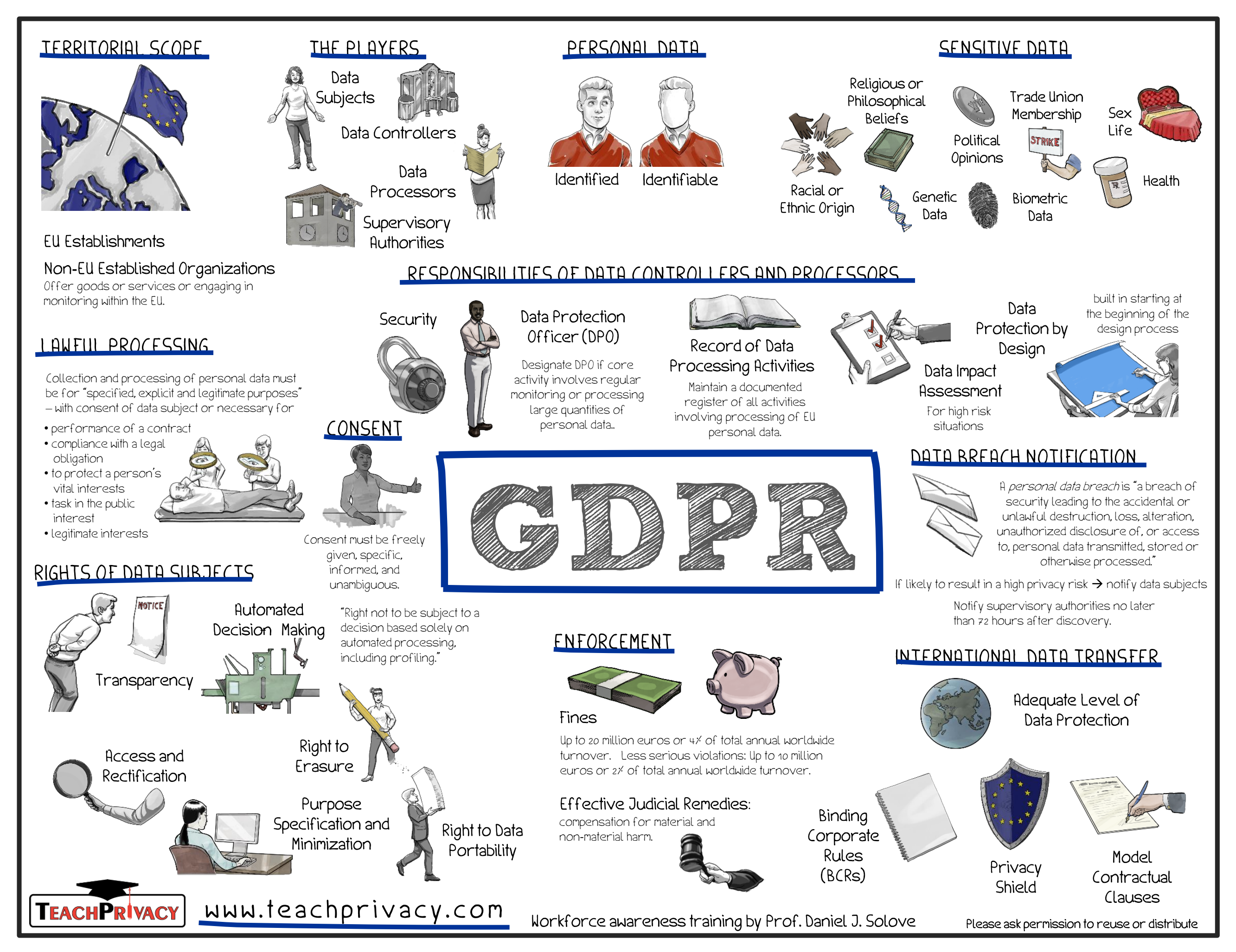
Ken Klingenstein

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

Daniel Solove One-Pager



TERRITORIAL SCOPE

EU Establishments

Non-EU Established Organizations

Offer goods or services or engaging in monitoring within the EU.

THE PLAYERS

Data Subjects

Data Controllers

Data Processors

Supervisory Authorities

PERSONAL DATA

Identified

Identifiable

SENSITIVE DATA

Religious or Philosophical Beliefs

Political Opinions

Trade Union Membership

Sex Life

Racial or Ethnic Origin

Genetic Data

Biometric Data

Health

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

Security

Data Protection Officer (DPO)

Designate DPO if core 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.

Data Impact Assessment

For high risk situations

Data Protection by Design

built in starting at the beginning of the design process

CONSENT

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

GDPR

DATA BREACH NOTIFICATION

A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS

Transparency

Automated Decision Making

"Right not to be subject to a decision based solely on automated processing, including profiling."

Access and Rectification

Right to Erasure

Purpose Specification and Minimization

Right to Data Portability

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

Binding Corporate Rules (BCRs)

Privacy Shield

Model Contractual Clauses

TEACHPRIVACY

www.teachprivacy.com

Workforce awareness training by Prof. Daniel J. Solove

Please ask permission to reuse or distribute

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
- https://bbbprograms.org/media-center/insights-blog/insights/2020/09/01/what-the-edpb-says-about-art.-49-derogations

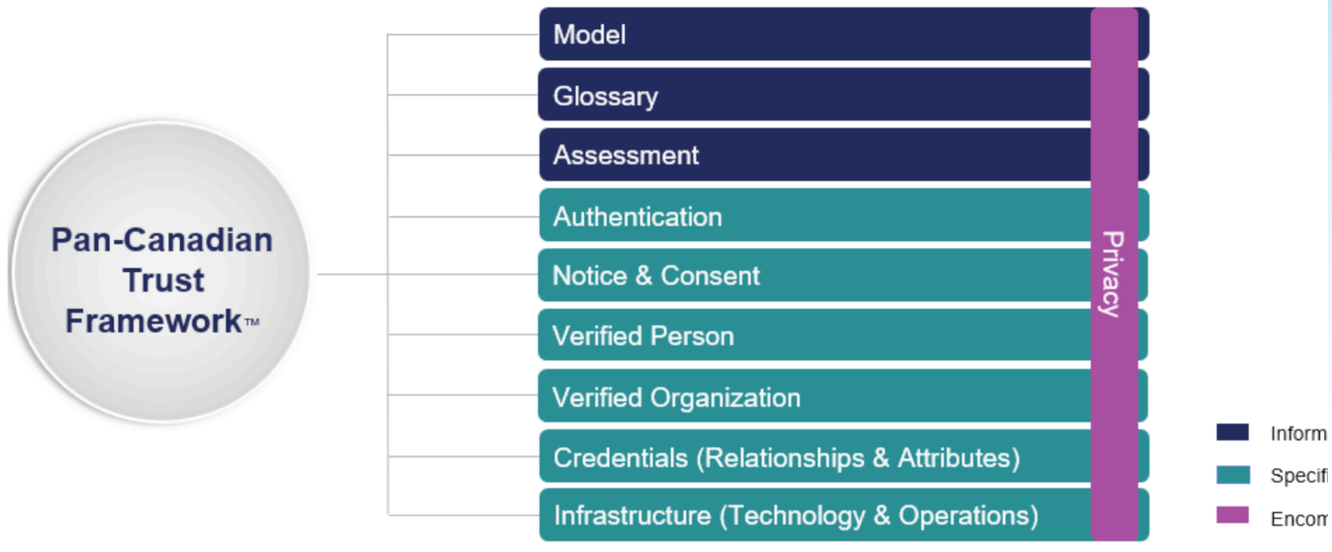
Privacy Shield Demise

- 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/
  - https://diacc.ca/wp-content/uploads/2019/08/Notice-and-Consent-Component-Overview-Draft-Recommendation-V1.0.pdf

Pan Canadian Trust Framework



Pan-Canadian Trust Framework™

Model

Glossary

Assessment

Authentication

Notice & Consent

Verified Person

Verified Organization

Credentials (Relationships & Attributes)

Infrastructure (Technology & Operations)

Privacy

■ Inform

■ Specifi

■ Encom

Figure 2. Pan-Canadian Trust Framework Model Visual Draft

DIACC Notice and Consent

- 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.
- https://diacc.ca/wp-content/uploads/2020/09/PCTF-Notice-Consent-Component-Conformance-Criteria-Final-Recommendation_V1.0.pdf

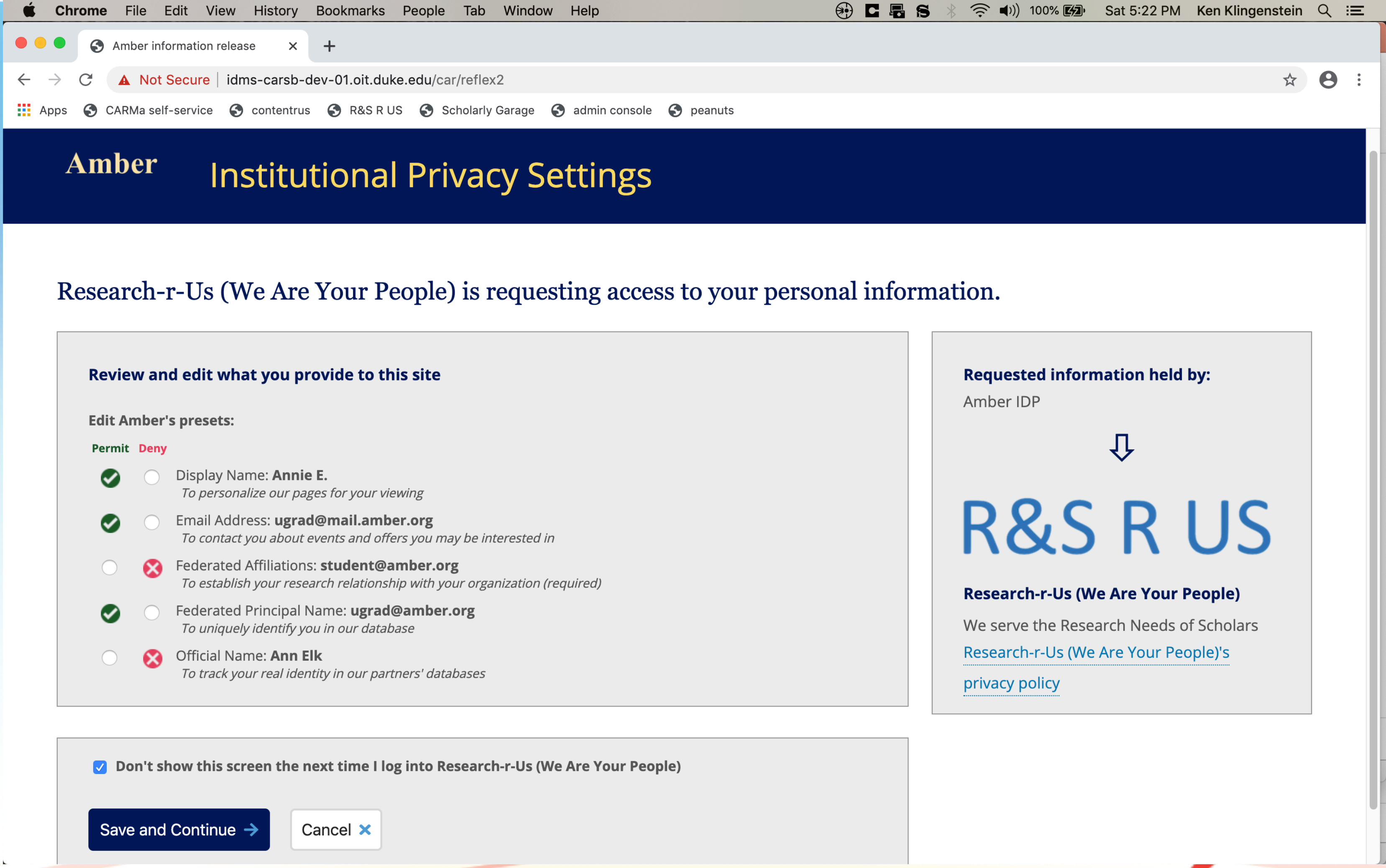
COVID-19 and Privacy

- 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

Basic undergrad consent UI



Amber Institutional Privacy Settings

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

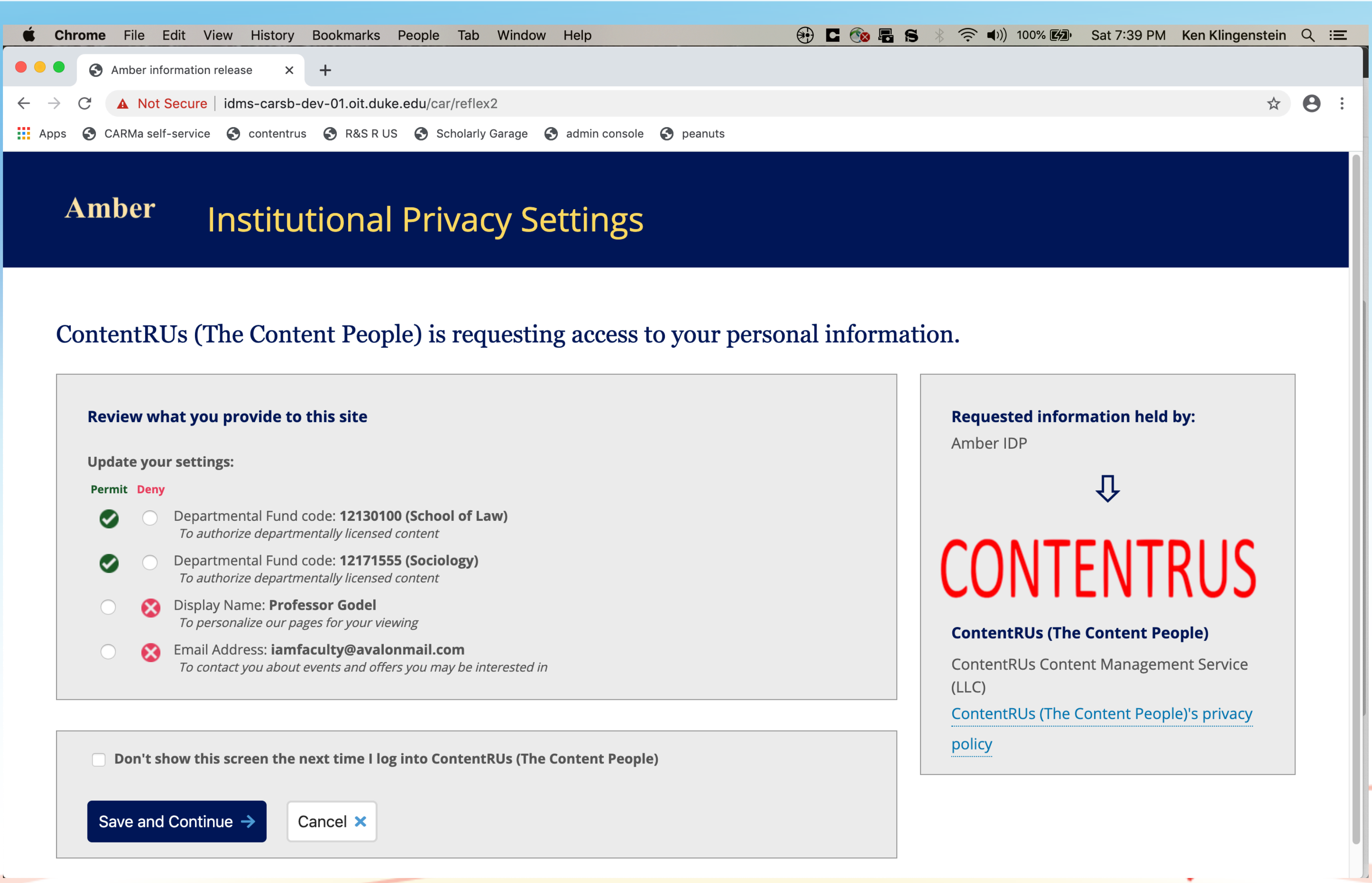
Research-r-Us (We Are Your People)

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)**

Faculty – limited access content UI



Chrome File Edit View History Bookmarks People Tab Window Help
100% Sat 7:39 PM Ken Klingenstein
Amber information release
Not Secure | idms-carsb-dev-01.oit.duke.edu/car/reflex2
Apps CARMa self-service contentrus R&S R US Scholarly Garage admin console peanuts

Amber Institutional Privacy Settings

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)** *To authorize departmentally licensed content*
✓	○	Departmental Fund code: **12171555 (Sociology)** *To authorize departmentally licensed content*
○	☒	Display Name: **Professor Godel** *To personalize our pages for your viewing*
○	☒	Email Address: **iamfaculty@avalonmail.com** *To contact you about events and offers you may be interested in*

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

Save and Continue → Cancel ✕

Requested information held by:

Amber IDP

⇩

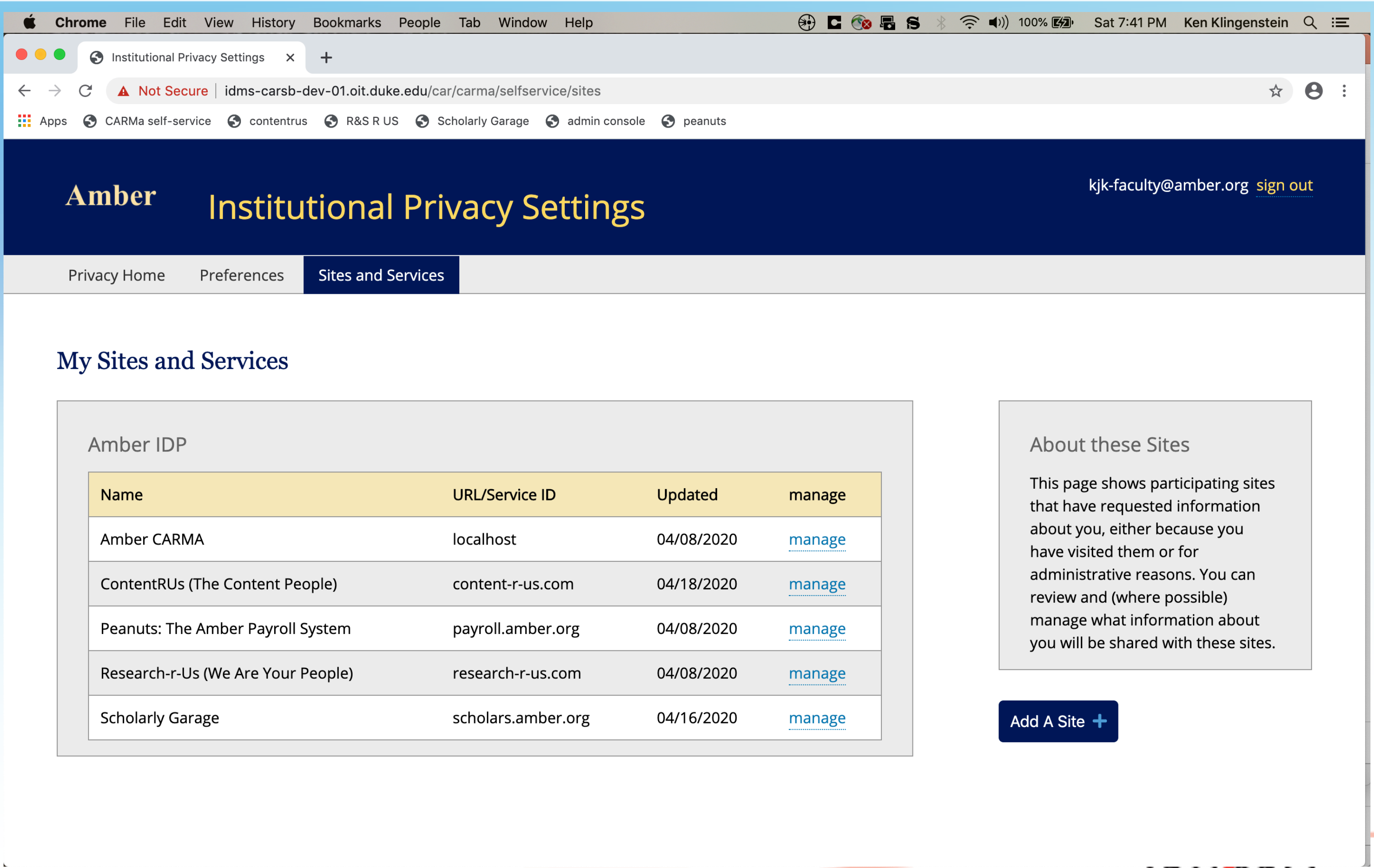
CONTENTRUS

ContentRUs (The Content People)

ContentRUs Content Management Service (LLC)

ContentRUs (The Content People)'s privacy policy

Self-servic e conse nt UI



Chrome File Edit View History Bookmarks People Tab Window Help
100%
Sat 7:41 PM
Ken Klingenstein
Institutional Privacy Settings
Not Secure
idms-carsb-dev-01.oit.duke.edu/car/carma/selfservice/sites
Apps
CARMa self-service
contentrus
R&S R US
Scholarly Garage
admin console
peanuts

Amber

Institutional Privacy Settings

kjk-faculty@amber.org sign out

Privacy Home | Preferences | Sites and Services

My Sites and Services

Amber IDP

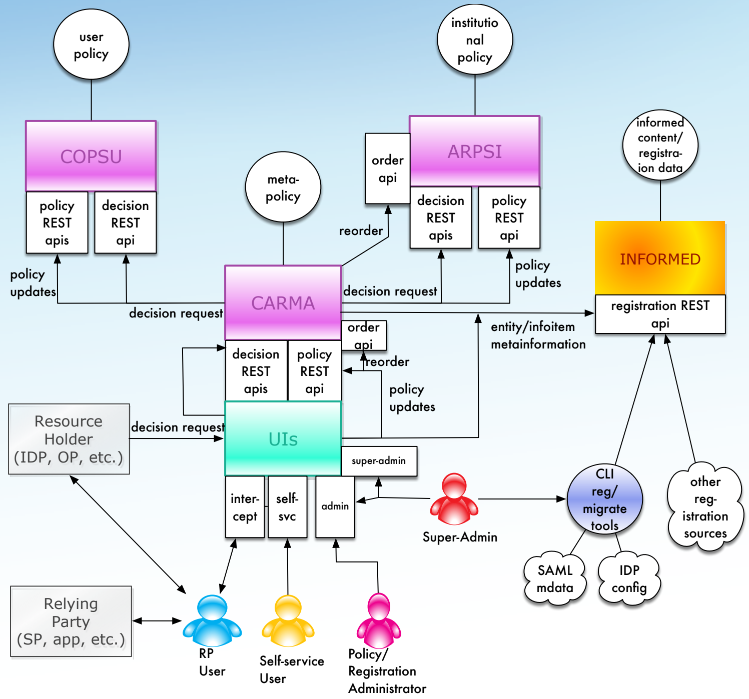
Name	URL/Service ID	Updated	manage
Amber CARMA	localhost	04/08/2020	manage
ContentRUs (The Content People)	content-r-us.com	04/18/2020	manage
Peanuts: The Amber Payroll System	payroll.amber.org	04/08/2020	manage
Research-r-Us (We Are Your People)	research-r-us.com	04/08/2020	manage
Scholarly Garage	scholars.amber.org	04/16/2020	manage

About these Sites

This page shows participating sites that have requested information about you, either because you have visited them or for administrative reasons. You can review and (where possible) manage what information about you will be shared with these sites.

Add A Site +

An API view


user policy
COPSU
policy REST apis
decision REST api
policy updates
decision request
meta-policy
CARMA
decision REST apis
policy REST api
order api
reorder
policy updates
institutional policy
ARPSI
order api
reorder
decision REST apis
policy REST api
decision request
policy updates
informed content/ registra-ion data
INFORMED
registration REST api
entity/infoitem metainformation
Resource Holder (IDP, OP, etc.)
decision request
UIs
super-admin
inter-cept
self-svc
admin
Super-Admin
CLI reg/ migrate tools
other reg-istration sources
SAML mdata
IDP config
Relying Party (SP, app, etc.)
RP User
Self-service User
Policy/ Registration Administrator

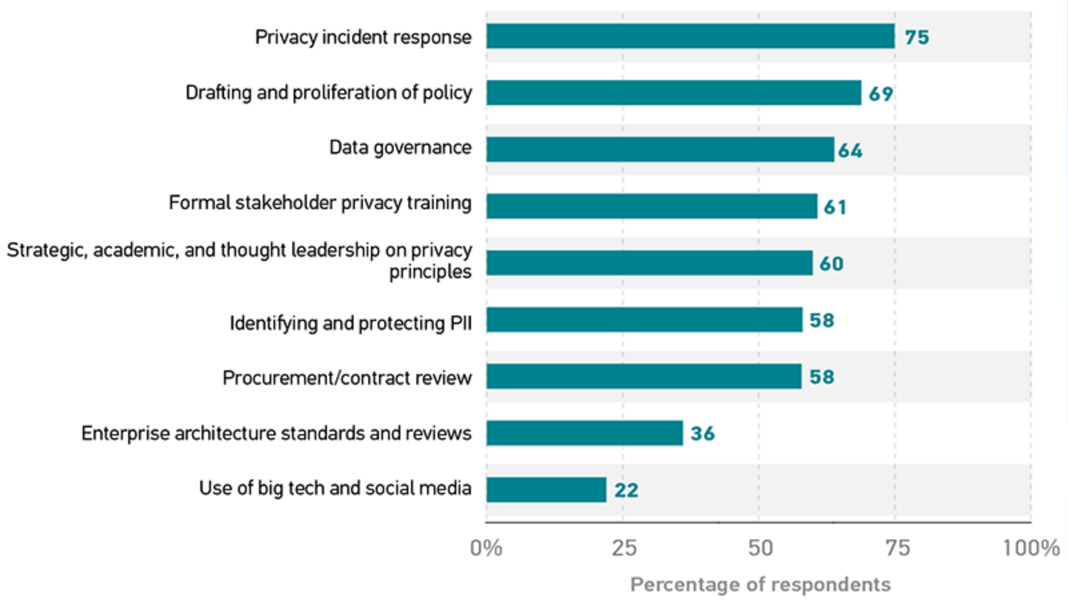
Privacy Stewardship

- Players
- Process
- Partnerships
- https://www.educause.edu/ecar/research-publications/the-evolving-landscape-of-data-privacy-in-higher-education/privacy-management

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, GDPA)
- **Conducts** regular privacy reviews to identify privacy-related vulnerabilities
- **Serves** as the centralized contact and authority for privacy issues
- **Supports** technology related to privacy

Process – library related attribute release

- 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