CAR

Under the Hood

VIGNETTE I: R&S

A Tale of Three Case Studies

BACKGROUND

- R&S: service mark for "Research and Scholarship" RPs, IDPs urged to release bundle of attributes to all of R&S
- Federation Participant Concerns
  - Vetting of service profile, not privacy/security profile
  - One size fits all across user population
  - Release liability rests exclusively with the IDP-OP

BACKGROUND (CONT'D)

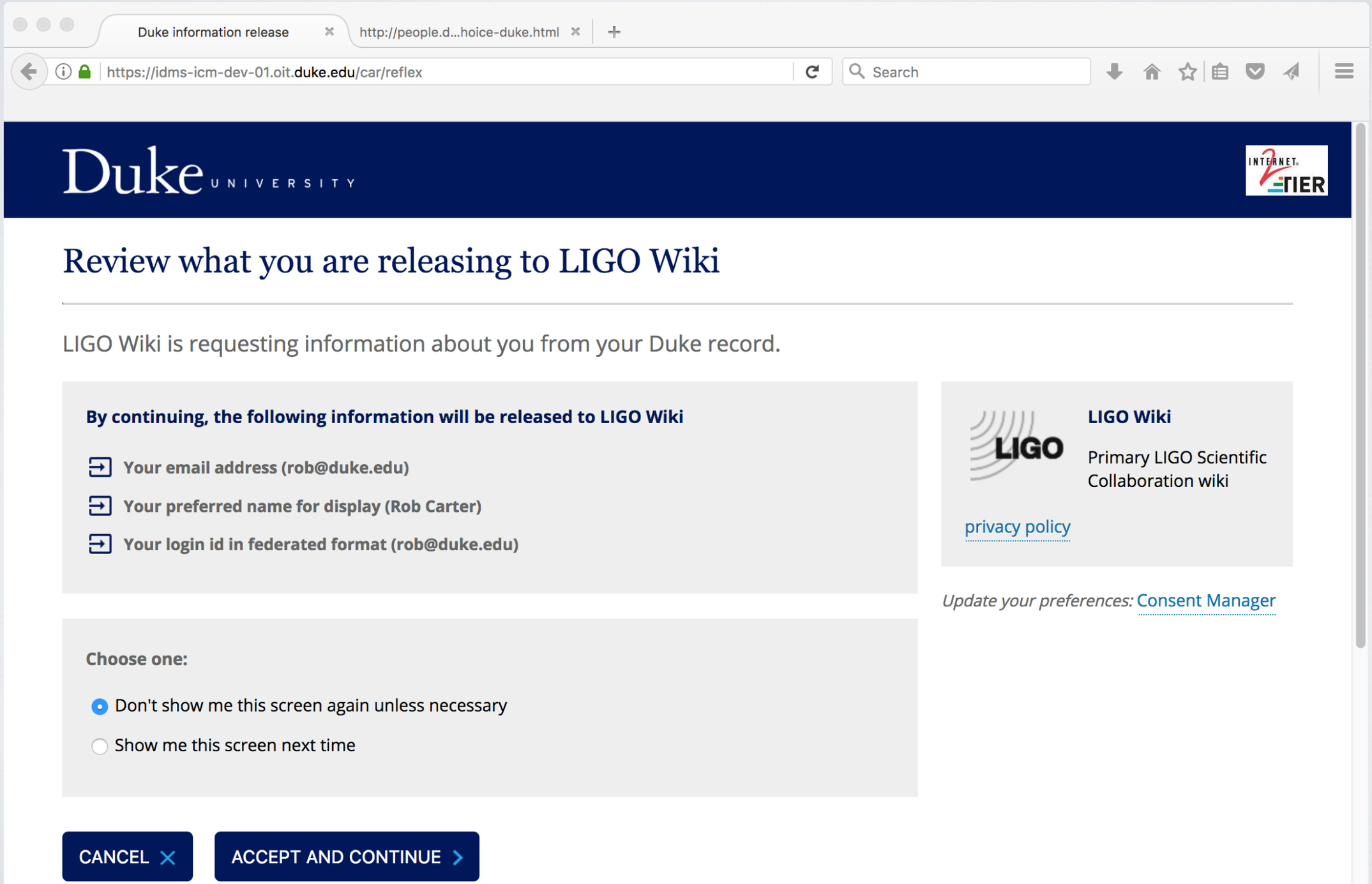
- Result: **Very** low adoption across InCommon

- **CAR** can provide flexible substrate for implementing R&S in multiple ways and:
  - relax liability concerns thru informed user consent
  - support flexible, user-centric release policies
  - increase transparency for more informed users, with or without employing consent

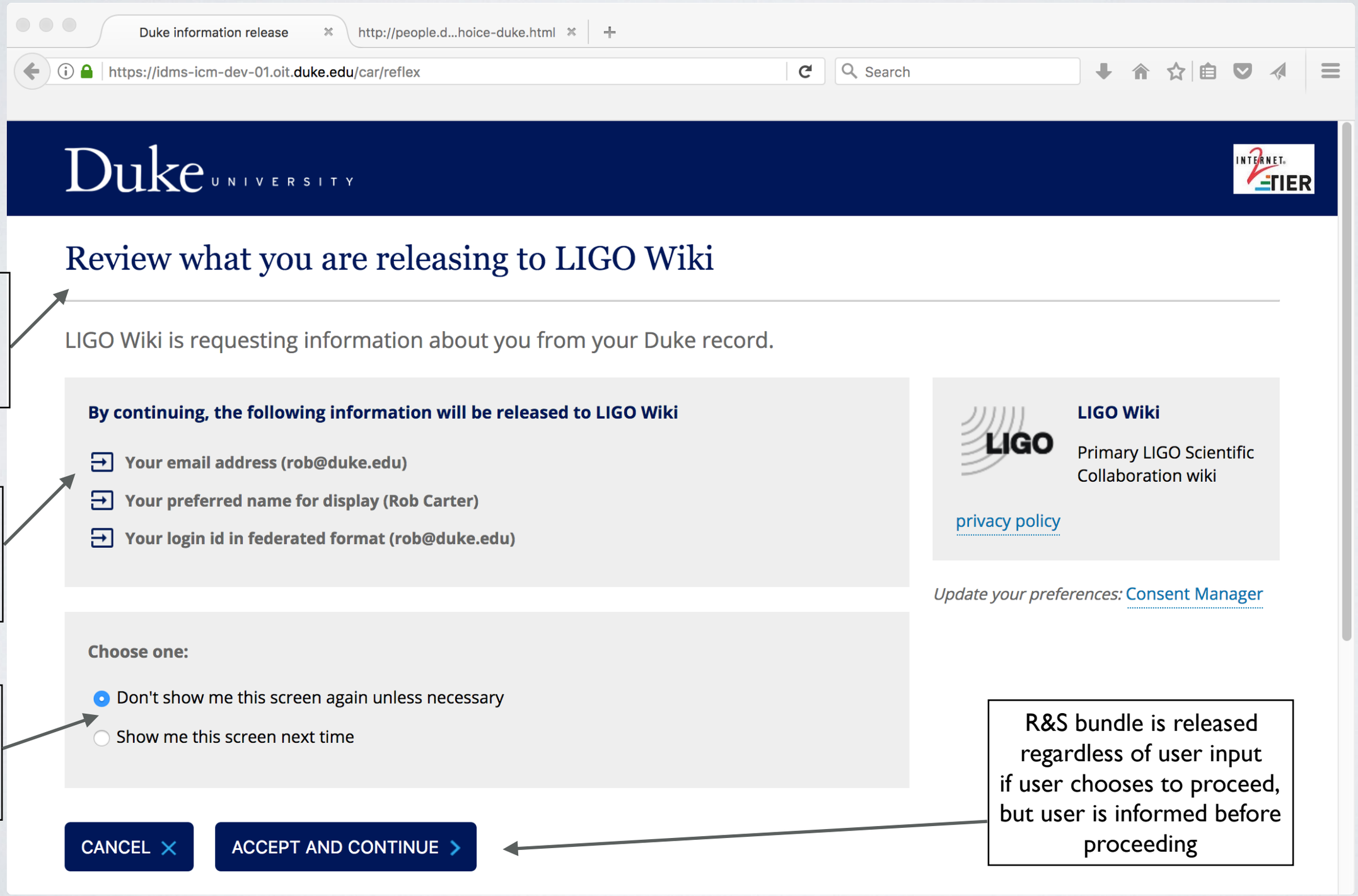
CASE I: INSTITUTIONAL CONTROL

- Institution asserts "ownership" of all release decisions
- No "national security" position — users may see into process
- Conclusion: releasing (ePPN + displayName + mail) to all R&S RPs is appropriate without explicit consent, but **with user transparency**

CASE I: USER EXPERIENCE



CASE I: USER EXPERIENCE



On first visit user can review releases

Review includes items and values

User may suppress future review

R&S bundle is released regardless of user input if user chooses to proceed, but user is informed before proceeding

CASE I: POLICY DESIGN

- Use two simple policies:
    - Institutional policy permits one subset of R&S bundle to all R&S RPs, denies remainder of bundle
    - Combining meta-policy gives **institutional policy** control of R&S attributes for R&S sites

CASE 1 : POLICY DETAILS

Combining Meta Policy (excerpts)

```
"relyingPartyPropertyArray":[
 {…"servicemark",…"RandS"…}
],
"userPropertyArray":[
 {…"eduPersonPrincipalName"…".*"…}
],
"arrayOfInfoReleaseStatement":[
{["eduPersonPrincipalName","displayName",
  "givenName","sn","mail",
  "eduPersonScopedAffiliation"]…"ARPSI"}
]
```

Apply policy to any RP with "RandS" service mark

Apply policy to users with any (".*") ePPN value set

For R&S bundle attributes, institutional policy ("ARPSI") takes precedence over user policy

Institutional Policy (excerpts)

Apply policy to any RP with "RandS" service mark

Apply policy to users with any (".*") ePPN value set

For ePPN, displayName, and mail, permit release; For remainder of R&S bundle, deny release

```
"relyingPartyPropertyArray":[
 {…"servicemark",…"RandS"…}
],
"userPropertyArray":[
 {…"eduPersonPrincipalName"…".*"…}
],
"arrayOfInfoReleaseStatement":[
 {["eduPersonPrincipalName","displayName",
   "mail"]…"PERMIT",
  ["eduPersonScopedAffiliation","givenName",
   "sn","eduPersonTargetedId"]…"DENY"
 }
```

CASE II: FULL CONSENT

- Institution determines that R&S attributes should be released, but only with explicit user consent

- Any values may be released, provided user consents

- Institution will **recommend** an R&S bundle subset for consent (ePPN + mail + displayName + ePSA)

CASE II : USER EXPERIENCE

Manage policies | Duke information release

https://idms-icm-dev-01.oit.duke.edu/car/reflex 80% Search

Duke UNIVERSITY

INTERNET2 TIER

Review and edit what you are releasing to LIGO Wiki

LIGO Wiki is requesting information about you from your Duke record.

You have to decide whether to release the following. Duke recommends:

- PERMIT **Your login id in federated format (rob@duke.edu)**
  To uniquely identify you
- PERMIT **Your email address (rob@duke.edu)**
  To contact you about LIGO business
- DENY **Your surname (Carter)**
  To allow other users to recognize you
- PERMIT **Your relationships with Duke (staff@duke.edu)**
  to tailor your profile to your institutional role
- PERMIT **Your relationships with Duke (member@duke.edu)**
  to tailor your profile to your institutional role
- DENY **Your legal first name (Robert)**
  To allow other users to recognize you
- PERMIT **Your preferred name for display (Rob Carter)**
  To allow other users to recognize you

EDIT THESE CHOICES | CONTINUE WITHOUT EDITING

LIGO Wiki (R&S)

Primary LIGO Scientific Collaboration wiki

privacy policy

Update your preferences: Consent Manager

The following information will also be released if you continue:

Hide -

CASE II : USER EXPERIENCE

Manage policies | Duke information release

https://idms-icm-dev-01.oit.duke.edu/car/reflex 80% Search

Duke UNIVERSITY

INTERNET2 TIER

Review and edit what you are releasing to LIGO Wiki

LIGO Wiki is requesting information about you from your Duke record.

You have to decide whether to release the following. Duke recommends:

- PERMIT **Your login id in federated format (rob@duke.edu)** — *To uniquely identify you*
- PERMIT **Your email address (rob@duke.edu)** — *To contact you about LIGO business*
- DENY **Your surname (Carter)** — *To allow other users to recognize you*
- PERMIT **Your relationships with Duke (staff@duke.edu)** — *to tailor your profile to your institutional role*
- PERMIT **Your relationships with Duke (member@duke.edu)** — *to tailor your profile to your institutional role*
- DENY **Your legal first name (Robert)** — *To allow other users to recognize you*
- PERMIT **Your preferred name for display (Rob Carter)** — *To allow other users to recognize you*

EDIT THESE CHOICES | CONTINUE WITHOUT EDITING

The following information will also be released if you continue:

Hide -

LIGO Wiki (R&S)

Primary LIGO Scientific Collaboration wiki

privacy policy

Update your preferences: Consent Manager

User **must** make decisions on first visit

R&S indicator displayed

Institutional recommendations

Initial decisions mirror institutional recommendations; Permit subset of R&S bundle

User may modify decisions or accept institutional recommendations

No automatic releases; all under user consent control

CASE II : USER EXPERIENCE (2)

Manage policies | Duke information release

https://idms-icm-dev-01.oit.duke.edu/car/reflex 67% Search

Duke UNIVERSITY

INTERNET2 TIER

Review and edit what you are releasing to LIGO Wiki

LIGO Wiki is requesting information about you from your Duke record.

What would you like to release to LIGO Wiki? ← "Edit These Choices" interface

PERMIT / DENY	**Your login id in federated format (rob@duke.edu)** *To uniquely identify you*
PERMIT / DENY	**Your email address (rob@duke.edu)** *To contact you about LIGO business*
PERMIT / DENY	**Your surname (Carter)** *To allow other users to recognize you*
PERMIT / DENY	**Your relationships with Duke (staff@duke.edu)** *to tailor your profile to your institutional role*
PERMIT / DENY	**Your relationships with Duke (member@duke.edu)** *to tailor your profile to your institutional role*
PERMIT / DENY	**Your legal first name (Robert)** *To allow other users to recognize you*
PERMIT / DENY	**Your preferred name for display (Rob Carter)** *To allow other users to recognize you*

Hide -

Permit/ Deny option button for each attribute/ value pair

LIGO **LIGO Wiki** (R&S)

Primary LIGO Scientific Collaboration wiki

privacy policy

Update your preferences: Consent Manager

Show other information that will be shared with LIGO Wiki +

Choose one:

- (•) Save my choices; don't show me this screen again unless necessary.
- ( ) Save my choices, but show me this screen next time.
- ( ) Don't save the choices I made just now. Show me this screen next time.

User may save decisions and suppress consent dialogs, save decisions without suppressing, or continue as indicated without saving

CANCEL × ACCEPT AND CONTINUE ›

User may always opt to cancel or accept settings and continue

CASE II: POLICY DESIGN

- Use two policies similar to Case I:
    - Institutional policy acts as **recommendation,** permitting subset of R&S bundle to R&S sites, denying remainder
    - Combining meta-policy gives **user-defined** policy control of all values of all attributes for R&S sites

CASE II : POLICY DETAILS

Combining Meta Policy (excerpts)

```
"relyingPartyPropertyArray":[
  {…"servicemark",…"RandS"…}
],
"userPropertyArray":[
  {…"eduPersonPrincipalName"…".*"…}
],
"allOtherOrgInfoReleaseStatement":
  {…"allOtherValues"…"COPSU"…}
```

Apply policy to RPs with "RandS" service mark

Apply policy to users with any value (".*") of eduPersonPrincipalName

Use user policy ("COPSU") for all values of all attributes

Institutional Policy (excerpts)

Apply policy to RPs with "RandS" service mark

Apply to users with any value of eduPersonPrincipalName

Permit/Deny values become user recommendations

```
"relyingPartyPropertyArray":[
 {…"servicemark",…"RandS"…}
],
"userPropertyArray":[
 {…"eduPersonPrincipalName"…".*"…}
],
"arrayOfInfoReleaseStatement":[
  {["eduPersonPrincipalName","displayName",
    "mail","eduPersonScopedAffiliation]…"PERMIT",
    ["givenName","sn"]…"DENY"
  }
]
```

CASE III: FLEXIBLE CONSENT

- Institution determines that **some** of R&S bundle should be released automatically; **majority** requires user consent

- Decision to require consent depends on the user and the values — student data, faculty names/email require consent

- Institution will **recommend against** release of some values, but allow user choice to prevail

CASE III : STUDENT EXPERIENCE

Manage policies | Duke information release

https://idms-icm-dev-01.oit.duke.edu/car/reflex 67% Search

Duke UNIVERSITY

Review and edit what you are releasing to LIGO Wiki

LIGO Wiki is requesting information about you from your Duke record.

You have to decide whether to release the following. Duke recommends:

- PERMIT **Your login id in federated format (hiro@duke.edu)**
  To uniquely identify you
- PERMIT **Your email address (hiro@duke.edu)**
  To contact you about LIGO business
- DENY **Your surname (Test Person)**
  To allow other users to recognize you
- PERMIT **Your relationships with Duke (member@duke.edu)**
  to tailor your profile to your institutional role
- PERMIT **Your relationships with Duke (affiliate@duke.edu)**
  to tailor your profile to your institutional role
- DENY **Your relationships with Duke (student@duke.edu)**
  to tailor your profile to your institutional role
- DENY **Your legal first name (SYSTEM92)**
  To allow other users to recognize you
- PERMIT **Your preferred name for display (SYSTEM92 Test Person Jr, Ph.D)**
  To allow other users to recognize you

EDIT THESE CHOICES | CONTINUE WITHOUT EDITING >

Show other information that will be shared with LIGO Wiki +

LIGO

LIGO Wiki

Primary LIGO Scientific Collaboration wiki

privacy policy

Update your preferences: Consent Manager

CASE III : STUDENT EXPERIENCE

Manage policies | Duke information release

https://idms-icm-dev-01.oit.duke.edu/car/reflex 67% Search

Duke UNIVERSITY

Review and edit what you are releasing to LIGO Wiki

LIGO Wiki is requesting information about you from your Duke record.

You have to decide whether to release the following. Duke recommends:

R&S policy for students requires consent (first visit)

PERMIT **Your login id in federated format (hiro@duke.edu)**
To uniquely identify you

PERMIT **Your email address (hiro@duke.edu)**
To contact you about LIGO business

DENY **Your surname (Test Person)**
To allow other users to recognize you

Institutional R&S policy sets recommended decisions

PERMIT **Your relationships with Duke (member@duke.edu)**
to tailor your profile to your institutional role

PERMIT **Your relationships with Duke (affiliate@duke.edu)**
to tailor your profile to your institutional role

Recommending release of two affiliations, denial of "student" affiliation

User has student affiliation

DENY **Your relationships with Duke (student@duke.edu)**
to tailor your profile to your institutional role

DENY **Your legal first name (SYSTEM92)**
To allow other users to recognize you

PERMIT **Your preferred name for display (SYSTEM92 Test Person Jr, Ph.D)**
To allow other users to recognize you

EDIT THESE CHOICES | CONTINUE WITHOUT EDITING

R&S indicator suppressed

LIGO **LIGO Wiki**
Primary LIGO Scientific Collaboration wiki
privacy policy

Update your preferences: Consent Manager

The following information will also be released if you continue:

Institutional policy requires user consent for all data for student user

Hide -

CASE III: FACULTY EXP.

Manage policies | Duke information release

https://idms-icm-dev-01.oit.duke.edu/car/reflex 67% Search

Duke UNIVERSITY

Review and edit what you are releasing to LIGO Wiki

LIGO Wiki is requesting information about you from your Duke record.

You have to decide whether to release the following. Duke recommends:

- PERMIT **Your login id in federated format (hiro@duke.edu)**
  To uniquely identify you
- PERMIT **Your email address (hiro@duke.edu)**
  To contact you about LIGO business
- PERMIT **Your surname (Test Person)**
  To allow other users to recognize you
- PERMIT **Your legal first name (SYSTEM92)**
  To allow other users to recognize you
- DENY **Your preferred name for display (SYSTEM92 Test Person Jr, Ph.D)**
  To allow other users to recognize you

EDIT THESE CHOICES | CONTINUE WITHOUT EDITING

LIGO Wiki

Primary LIGO Scientific Collaboration wiki

privacy policy

Update your preferences: Consent Manager

The following information will also be released if you continue:

- **Your relationships with Duke (faculty@duke.edu)**
- **Your relationships with Duke (member@duke.edu)**
- **Your relationships with Duke (affiliate@duke.edu)**

Hide -

CASE III: FACULTY EXP.

Manage policies | Duke information release

https://idms-icm-dev-01.oit.duke.edu/car/reflex 67% Search

Duke UNIVERSITY

INTERNET2 TIER

Review and edit what you are releasing to LIGO Wiki

LIGO Wiki is requesting information about you from your Duke record.

You have to decide whether to release the following. Duke recommends:

R&S policy for faculty requires consent (first visit)

PERMIT **Your login id in federated format (hiro@duke.edu)**
To uniquely identify you

PERMIT **Your email address (hiro@duke.edu)**
To contact you about LIGO business

For faculty, institution recommends releasing ePPN, mail, sn, givenName to R&S sites

PERMIT **Your surname (Test Person)**
To allow other users to recognize you

PERMIT **Your legal first name (SYSTEM92)**
To allow other users to recognize you

DENY **Your preferred name for display (SYSTEM92 Test Person Jr, Ph.D)**
To allow other users to recognize you

For faculty, institutional policy recommendation is to deny displayName

EDIT THESE CHOICES CONTINUE WITHOUT EDITING

LIGO **LIGO Wiki**
Primary LIGO Scientific Collaboration wiki

privacy policy

Update your preferences: Consent Manager

Faculty, not student

The following information will also be released if you continue:

Your relationships with Duke (faculty@duke.edu)
Your relationships with Duke (member@duke.edu)
Your relationships with Duke (affiliate@duke.edu)

For faculty, release of non-student affiliations is mandatory to all R&S RPs

Hide -

CASE III: POLICY DESIGN

- Two institutional policies, two combining metapolicies:
  - Institutional policy #1 applied to students + R&S RPs permits ePPN, mail, displayName, and non-student **values** of eduPersonScopedAffiliation
  - Institutional policy #2 applied to faculty + R&S RPs permits ePPN, mail, givenName, sn, and non-student values of eduPersonScopedAffiliation
  - Combining metapolicy #1 applied to students + R&S RPs delegates control of all release to user-defined policy
  - Combining metapolicy #2 applied to faculty + R&S RPs delegates control of ePSA to institutional policy, remainder to user-defined policy

CASE III: POLICY DETAILS

Combining MetaPolicies (excerpts)

```
Policy1:

"relyingPartyPropertyArray": [
  {…"servicemark",…"RandS"…}
],
"userPropertyArray": [
  {…"eduPersonScopedAffiliation"…"student@duke.edu"…}
],
"allOtherOrgInfoReleaseStatement":
  {…"allOtherValues"…"COPSU"…}

Policy 2:

"relyingPartyPropertyArray": [
  {…"servicemark",…"RandS"…}
],
"userPropertyArray": [
  {…"eduPersonScopedAffiliation"…"faculty@duke.edu"…}
],
"arrayOfInfoReleaseStatement": [
  {["mail","displayName","givenName","sn","eduPersonPrincipalName"]…"COPSU"}
]
"allOtherOrgInfoReleaseStatement":
  {…"allOtherValues"…"ARPSI"…}
```

Policies applied in rank order (1, then 2)

Combining policy for students + R&S RPs

User policy (COPSU) controls everything

Faculty have user control over all but affiliation; institution (ARPSI) controls affiliation

Institutional Policies (excerpts)

Institutional policy for students + R&S RPs

Permit mail, displayName, ePPN, and non-student-related affiliations

Institutional policy for faculty + R&S RPs

Permit all the R&S bundle except displayName

```
Policy 1:

"relyingPartyPropertyArray": [
  {…"servicemark",…"RandS"…}
],
"userPropertyArray": [
  {…"eduPersonScopedAffiliation"…"student@duke.edu"…}
],
"arrayOfInfoReleaseStatement": [
  {["mail","displayName","eduPersonPrincipalName",
      {"eduPersonScopedAffiliation",["member@duke.edu",…"affiliate@duke.edu"]}]…"PERMIT"},
  {["givenName","sn",{"eduPersonScopedAffiliation",["student@duke.edu","alumni@duke.edu"]}]
…"DENY"},
]

Policy 2:

"relyingPartyPropertyArray": [
  {…"servicemark",…"RandS"…}
],
"userPropertyArray": [
  {…"eduPersonScopedAffiliation"…"faculty@duke.edu"…}
],
"arrayOfInfoReleaseStatement": [
  {["mail","givenName","sn","eduPersonPrincipalName","eduPersonScopedAffiliation"]…"PERMIT"},
  {["displayName"]…"DENY"}
]
```

CAR+R&S SUMMARY

- CAR's flexible policies can make R&S attribute release safer and more adaptive

- Institutions can choose what user consent controls down to the user and/or attribute-value level

- Users can be informed even if they cannot control release decisions, and can control their experience

- Institutions have flexibility in presentation (eg., to show or suppress service mark identifiers in the UI)