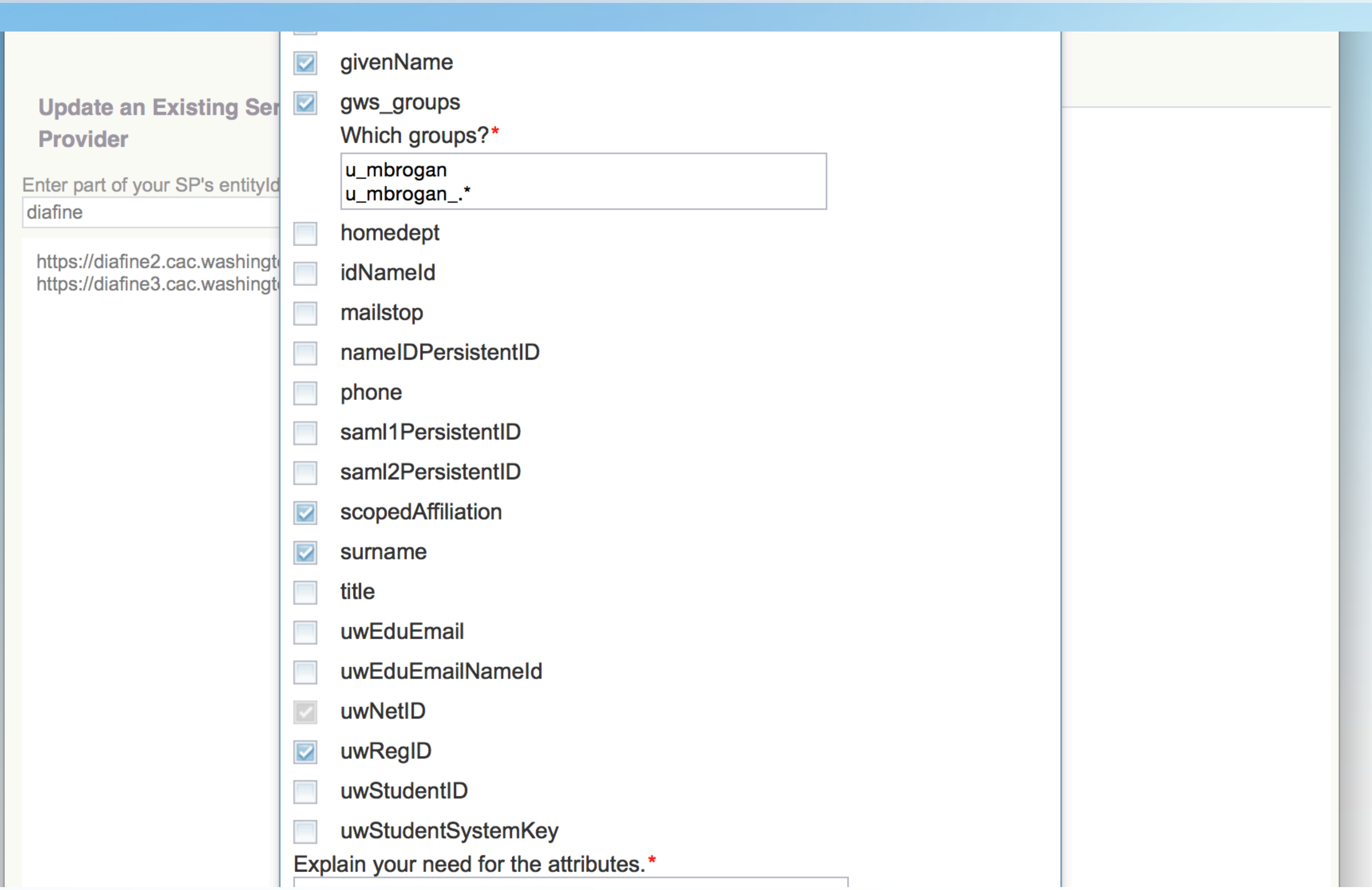
Reaching the Age of Consent

Ken Klingenstein, Internet2

Topics

- Internal and federated use cases for consent
  - Alternatives to consent
- Good practices in consent
- Privacy Lens as a pardigm
- Consent Management infrastructure
- Takeaways

Univ of Washington attribute “menu”



Update an Existing Ser
Provider

Enter part of your SP's entityId

diafine

https://diafine2.cac.washingt
https://diafine3.cac.washingt

☑ givenName

☑ gws_groups

Which groups?*

u_mbrogan
u_mbrogan_.*

□ homedept

□ idNameId

□ mailstop

□ nameIDPersistentID

□ phone

□ saml1PersistentID

□ saml2PersistentID

☑ scopedAffiliation

☑ surname

□ title

□ uwEduEmail

□ uwEduEmailNameId

☑ uwNetID

☑ uwRegID

□ uwStudentID

□ uwStudentSystemKey

Explain your need for the attributes.*

The internal and federated use cases

- Federated use cases classic:
  - And difficult because of their often international aspects
  - In the US, a significant number of "deciders" are outside of central IT
- Internal use cases: the student app marketplace at Duke and

the departmental app marketplace at U Washington and . . .

- student consent for release of enterprise data needed because of independence of app

  - https://wiki.cac.washington.edu/display/infra/Guide+to+Attributes+Available+from+the+UW+IdP
  - https://wiki.cac.washington.edu/display/infra/Request+Attributes+from+the+UW+IdP

Some federations provide services to support end-user consent

- https://www.switch.ch/aai/support/tools/resource-registry/
- http://jagger.heanet.ie/
- https://manager.aaf.edu.au/federationregistry/
- Hub-and-spoke federations do consent management at the hub, though that can be pushed out to the end-user.

Characteristics of Good Practices in Consent:

- Fine-grain attribute release capabilities, with reasonable use of “bundles” and “meta-attributes” where appropriate.
- Informed consent that addresses the following concerns:
  - Hierarchical, flexible, accessible, etc.
  - Clear, concise human-readable explanations of attributes to be sent
- Additional detail provided when needed, including
  - which attributes are required
  - values of attributes
  - how SP will use each attribute
  - how long SP will keep each attribute (attribute privacy policy)
- Revocation of an attribute release policy (out of band is fine)
- Ability to convey trust marks and other guides to user
- Providing a variety of options for attribute release during future visits to the same site, including using the current settings, periodic resets or reconfirmations, out-of-band notifications, etc.
- Provide an audit interface and history to support both privacy and security
- The ability to combine a set of individual attributes into a common single meta attribute (e.g. combining cn and sn into a single name field for consent)

More good practices

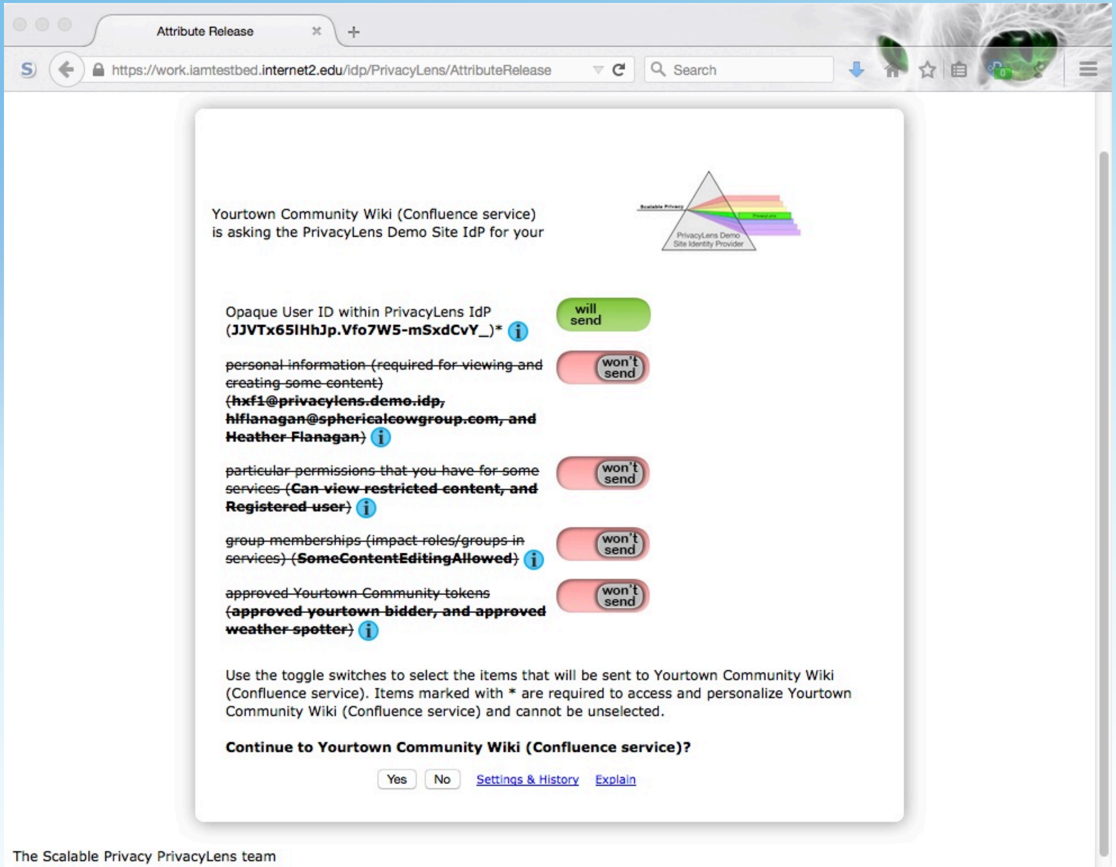
- Affirmative actions and actionable choices -- it's clear what the user needs to decide and how to convey the decision (e.g. use of “yes” versus “continue”)
- Ability to display the values being released
- The ability to present attributes together as “bundles” requiring a single consent
- The external interactions include:
- Ability to access metadata to populate attributes, bundles, informed consent dialogues, etc.
- Ability to participate in orchestrated activities that may include MFA, provisioning, etc.
- Ability to import and export user preferences and histories in a standard format

Some other Noble Principles

- Identity portability
  - Being able to move one's consent preferences from one IdP to another
  - Not necessarily portability of identifiers, attributes or authorizations
- Unobservability not part of this model, but non-correlating opaque identifiers are
- Auditability for legal or regulatory requirements
- Adding Privacy to Accessibility

PrivacyLens as a paradigm

- Enabling effective and informed end-user consent
- Embraces a set of capabilities
  - Hierarchical information, fine grain control, bundling, revocation of consent, flexible notifications, etc.
- Embraces a style of presentation
  - Clear screens and slides
  - Optional display of values being sent
  - Affirmative user actions
- Embraces a variety of platforms and management approaches
  - Protocol-agnostic
  - Enterprise management consoles and management
  - Audit and security logs
- Built on an open consent management infrastructure


Attribute Release
https://work.iamtestbed.internet2.edu/idp/PrivacyLens/AttributeRelease
Search
Scalable Privacy
PrivacyLens
PrivacyLens Demo Site Identity Provider

Yourtown Community Wiki (Confluence service) is asking the PrivacyLens Demo Site IdP for your

Opaque User ID within PrivacyLens IdP (**JJVTx65IHhJp.Vfo7W5-mSxdCvY_**)* — will send

~~personal information (required for viewing and creating some content)~~ ~~(**hxf1@privacylens.demo.idp, hlflanagan@sphericalcowgroup.com, and Heather Flanagan**)~~ — won't send

~~particular permissions that you have for some services (**Can view restricted content, and Registered user**)~~ — won't send

~~group memberships (impact roles/groups in services) (**SomeContentEditingAllowed**)~~ — won't send

~~approved Yourtown Community tokens (**approved yourtown bidder, and approved weather spotter**)~~ — won't send

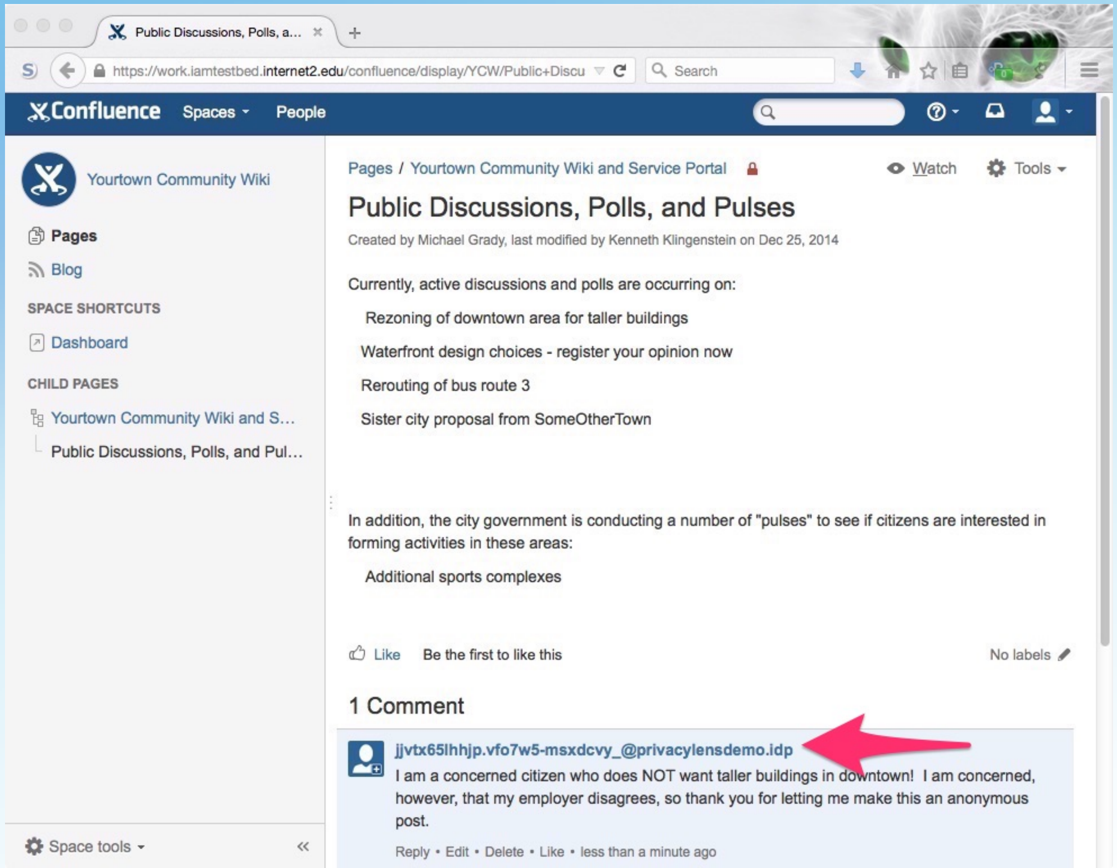
Use the toggle switches to select the items that will be sent to Yourtown Community Wiki (Confluence service). Items marked with * are required to access and personalize Yourtown Community Wiki (Confluence service) and cannot be unselected.

Continue to Yourtown Community Wiki (Confluence service)?

Yes No Settings & History Explain

The Scalable Privacy PrivacyLens team

Releasing an opaque identifier only


Public Discussions, Polls, a...
https://work.iamtestbed.internet2.edu/confluence/display/YCW/Public+Discu
Search
Confluence
Spaces
People
Yourtown Community Wiki
Pages
Blog
SPACE SHORTCUTS
Dashboard
CHILD PAGES
Yourtown Community Wiki and S...
Public Discussions, Polls, and Pul...
Space tools
Watch
Tools

Pages / Yourtown Community Wiki and Service Portal

Public Discussions, Polls, and Pulses

Created by Michael Grady, last modified by Kenneth Klingenstein on Dec 25, 2014

Currently, active discussions and polls are occurring on:

Rezoning of downtown area for taller buildings

Waterfront design choices - register your opinion now

Rerouting of bus route 3

Sister city proposal from SomeOtherTown

In addition, the city government is conducting a number of "pulses" to see if citizens are interested in forming activities in these areas:

Additional sports complexes

Like Be the first to like this No labels

1 Comment

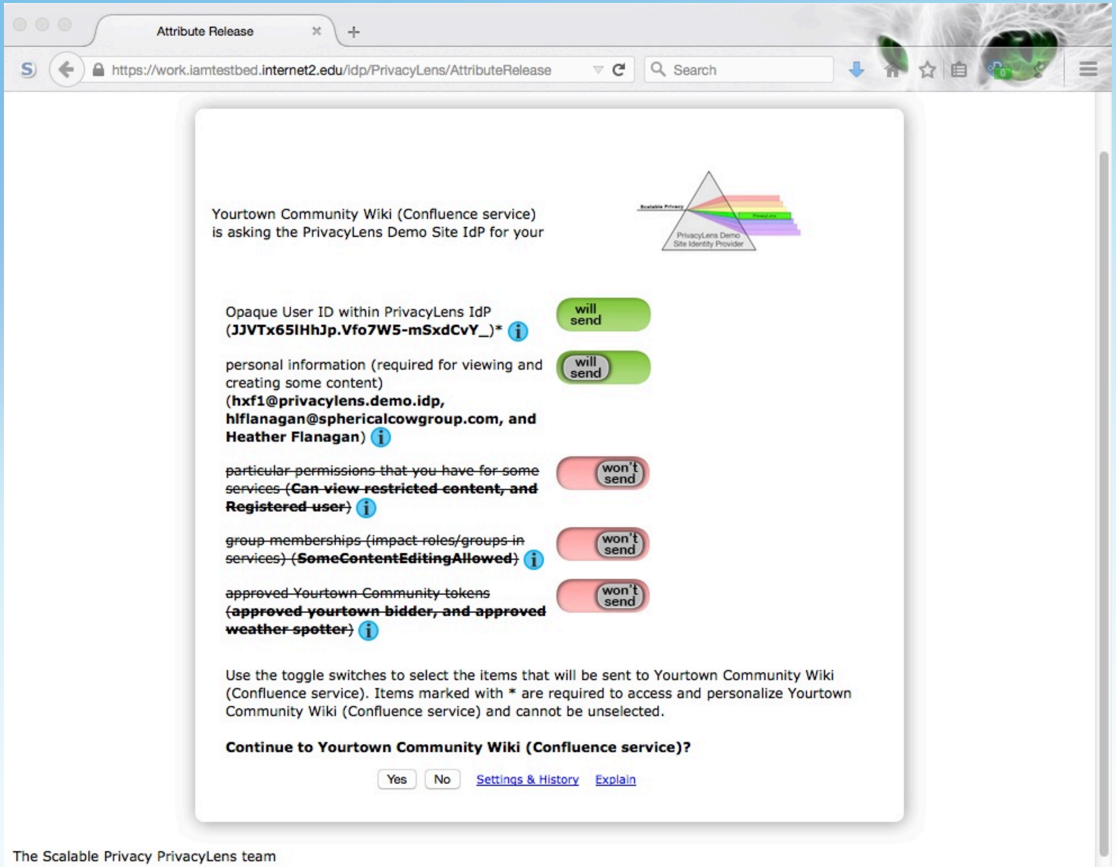
jjvtx65lhhjp.vfo7w5-msxdcvy_@privacylensdemo.idp

I am a concerned citizen who does NOT want taller buildings in downtown! I am concerned, however, that my employer disagrees, so thank you for letting me make this an anonymous post.

Reply • Edit • Delete • Like • less than a minute ago

Anonymous comments

With only the opaque identifier released, individuals may post comments while preserving their anonymity within the community.


Attribute Release
https://work.iamtestbed.internet2.edu/idp/PrivacyLens/AttributeRelease
Search
Scalable Privacy
PrivacyLens
PrivacyLens Demo Site Identity Provider

Yourtown Community Wiki (Confluence service) is asking the PrivacyLens Demo Site IdP for your

Opaque User ID within PrivacyLens IdP (**JJVTx65IHhJp.Vfo7W5-mSxdCvY_**)* ⓘ

personal information (required for viewing and creating some content) (**hxf1@privacylens.demo.idp, hlflanagan@sphericalcowgroup.com, and Heather Flanagan**) ⓘ

~~particular permissions that you have for some services (**Can view restricted content, and Registered user**)~~ ⓘ

~~group memberships (impact roles/groups in services) (**SomeContentEditingAllowed**)~~ ⓘ

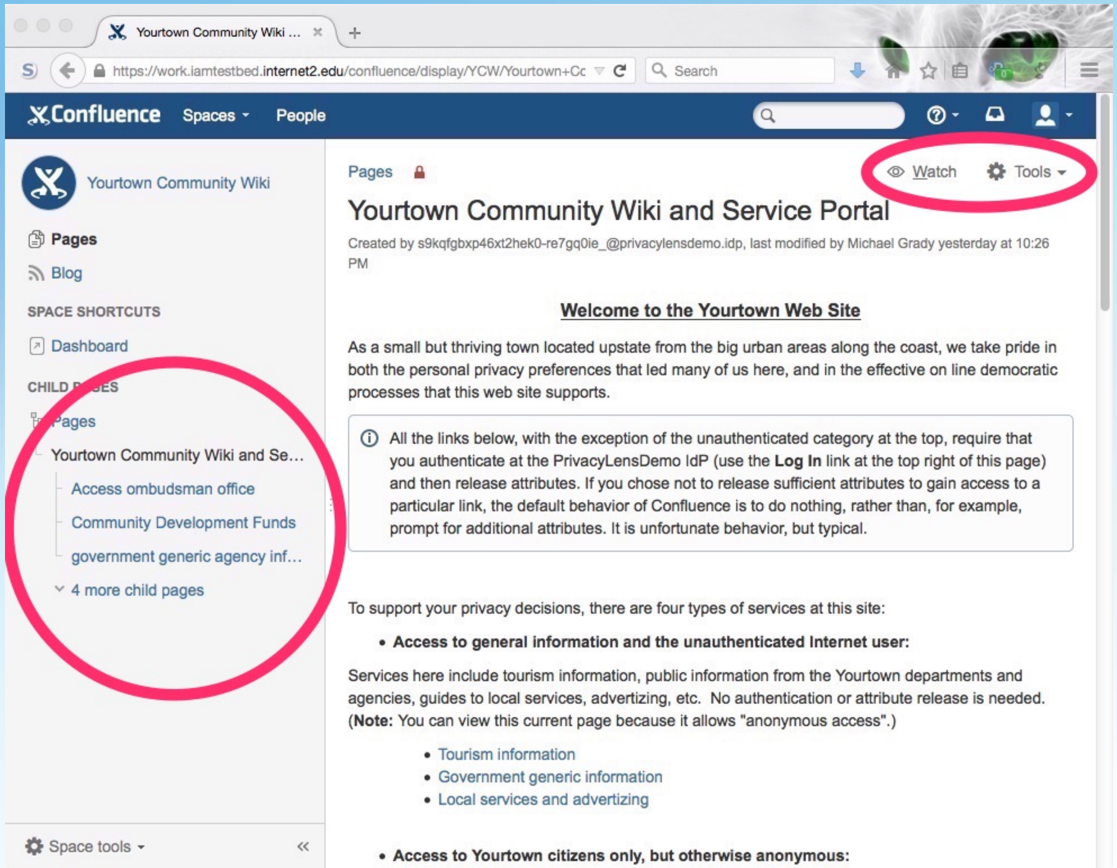
~~approved Yourtown Community tokens (**approved yourtown bidder, and approved weather spotter**)~~ ⓘ

Use the toggle switches to select the items that will be sent to Yourtown Community Wiki (Confluence service). Items marked with * are required to access and personalize Yourtown Community Wiki (Confluence service) and cannot be unselected.

Continue to Yourtown Community Wiki (Confluence service)?

The Scalable Privacy PrivacyLens team

Releasing an opaque identifier and some personal information


Yourtown Community Wiki ...
https://work.iamtestbed.internet2.edu/confluence/display/YCW/Yourtown+Cc
Search
Confluence
Spaces
People
Yourtown Community Wiki
Pages
Blog
SPACE SHORTCUTS
Dashboard
CHILD PAGES
Pages
Yourtown Community Wiki and Se...
Access ombudsman office
Community Development Funds
government generic agency inf...
4 more child pages
Space tools
Pages
Watch
Tools

Yourtown Community Wiki and Service Portal

Created by s9kqfgbxp46xt2hek0-re7gq0ie_@privacylensdemo.idp, last modified by Michael Grady yesterday at 10:26 PM

Welcome to the Yourtown Web Site

As a small but thriving town located upstate from the big urban areas along the coast, we take pride in both the personal privacy preferences that led many of us here, and in the effective on line democratic processes that this web site supports.

ⓘ All the links below, with the exception of the unauthenticated category at the top, require that you authenticate at the PrivacyLensDemo IdP (use the **Log In** link at the top right of this page) and then release attributes. If you chose not to release sufficient attributes to gain access to a particular link, the default behavior of Confluence is to do nothing, rather than, for example, prompt for additional attributes. It is unfortunate behavior, but typical.

To support your privacy decisions, there are four types of services at this site:

- **Access to general information and the unauthenticated Internet user:**

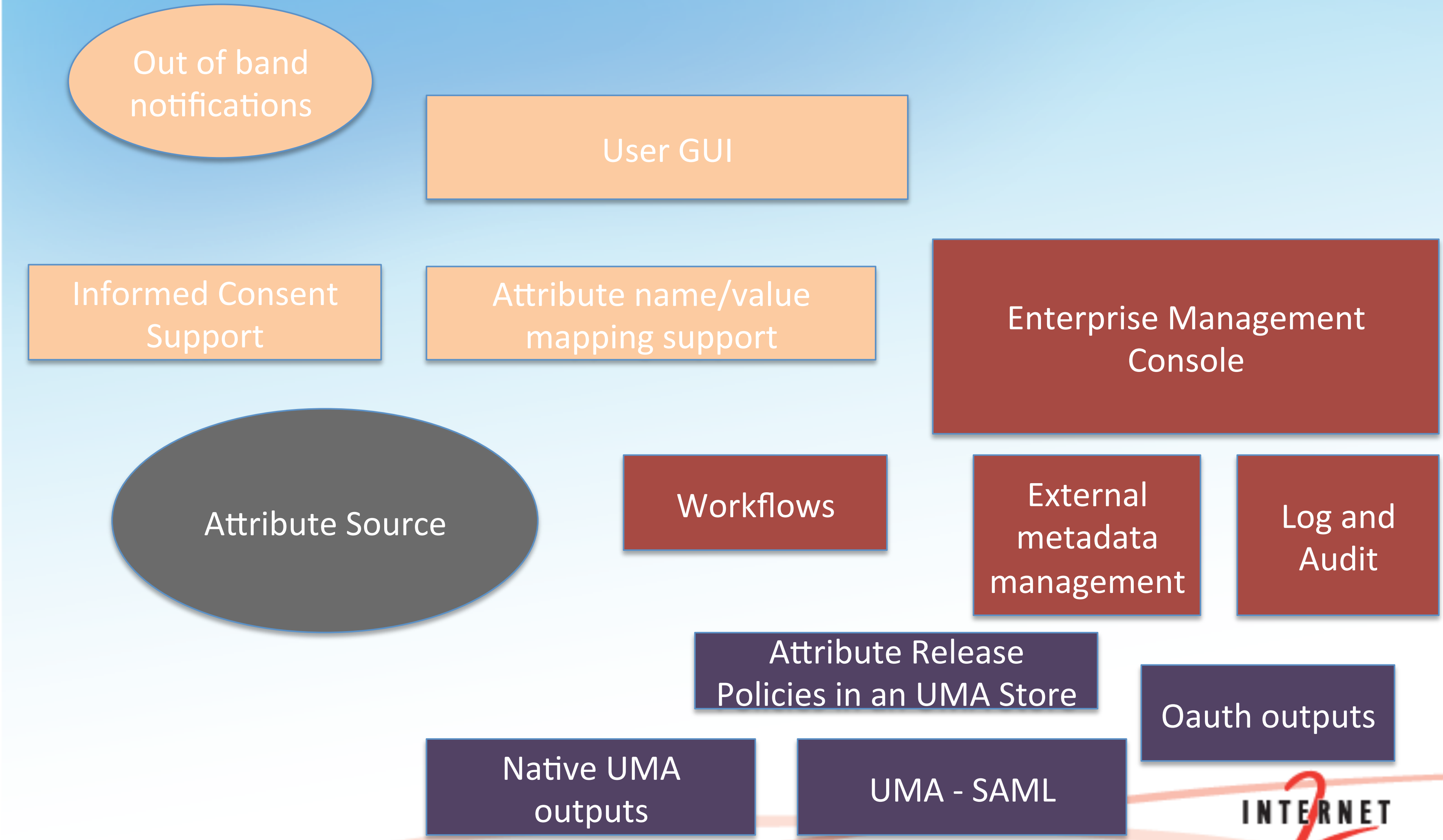
Services here include tourism information, public information from the Yourtown departments and agencies, guides to local services, advertizing, etc. No authentication or attribute release is needed. (**Note:** You can view this current page because it allows "anonymous access".)

- Tourism information
- Government generic information
- Local services and advertizing

- **Access to Yourtown citizens only, but otherwise anonymous:**

Releasing an opaque identifier and personal information

Components of a consent infrastructure



Out of band notifications

User GUI

Informed Consent Support

Attribute name/value mapping support

Enterprise Management Console

Attribute Source

Workflows

External metadata management

Log and Audit

Attribute Release Policies in an UMA Store

Oauth outputs

Native UMA outputs

UMA - SAML

Key functions - IdP Management Console

- Enterprise IdP Management Console Desirable features:
- Ability to control the UI design and user choices on a per SP basis
- Display of values being sent
- Display of SP Logo, etc
- Options for notification, consent suppression, frequency (e.g. one-time releases vs recurring releases), etc.
- Ability to plug in a variety of notification options
- Integration with revocation mechanism
- Ability to manage the informed consent info via API's, local stores, etc
- Ability to skin the UI
- Ability to change the UI
- Shib integration issues
- Managing audit logs
- Security for console
- Mapping attribute names, etc
- Interfacing with metadata
- Linking to informed consent mechanisms

Lessons Learned

- The most important metrics for MFA are:
  - Integrations – the number of apps that can use it
  - Federated leverage – the number of external third parties that use local MFA installations
- Schema are important
  - Critical to effective application use
  - Identifiers need to be specifically characterized
    - persistence, linkability, opacity, statefulness
- Trustmarks are critical for both user and entity; getting the granularity right for each will be key.
- Selective release of values from a multi-valued attributes is very hard, both in UI and infrastructure aspects
  - Confine the selection in use cases (develop alternatives)
  - Build an audit infrastructure for minimum/appropriate release

Lessons Learned – Consent Management

- Consent management at scale seems viable, but needs infrastructure
- Applications don't know how to do data minimization
  - Very few are privacy-preserving; most lead with a request for identity when, at that point, only statefulness is needed
  - "You are what you release" functionality not leveraged
- Need to guard against habituation, oppressiveness; need to permit rubber squeeze toys
- There are multiple approaches to informing consent

For more information:

- https://spaces.internet2.edu/display/scalepriv/Scalable+Privacy
  - Scalable Privacy Overview
- https://work.iamtestbed.internet2.edu/drupal/
  - PrivacyLens and Consent Management infrastructure
- https://work.iamtestbed.internet2.edu/confluence/display/YCW/Yourtown+Community+Wiki+and+Service+Portal
  - Privacy-responsive and attribute aware applications