Managing privacy constraints in directories

Universidad de Málaga RedIRIS/red.es

Madrid, December 12th 2006

Outline

Outline

Outline

Defintions

¿Contradictions?. . .

According to D.R.A.E.

Defintions

¿Contradictions?. . .

According to D.R.A.E.

Directory

5. m. Roster of people belonging to a group, with indication of diverse information about them, such as role, location data, phone numbers, etc.

Defintions

¿Contradictions?. . .

According to D.R.A.E.

Directory

5. m. Roster of people belonging to a group, with indication of diverse information about them, such as role, location data, phone numbers, etc.

Privacy

1. f. Part of private life that a person has the right to protect form any kind of intrussion.

Defintions

¿Contradictions?. . .

According to D.R.A.E.

Directory

5. m. Roster of people belonging to a group, with indication of diverse information about them, such as role, location data, phone numbers, etc.

Privacy

1. f. Part of private life that a person has the right to protect form any kind of intrussion.

Private

2. adj. Particular y personal of each individual.

3. adj. Something that is not a public or state property, but belongs to individuals.

Institutional mandate
that starts the problem

Institutional mandate
that starts the problem

Public institutions must serve the public so they need to. . .

Institutional mandate
that starts the problem

Public institutions must serve the public so they need to...

- Offer information about themselves

Institutional mandate
that starts the problem

Public institutions must serve the public so they need to...

- Offer information about themselves
- Offer information about their members

Institutional mandate
that starts the problem

Public institutions must serve the public so they need to...

- Offer information about themselves
- Offer information about their members
- Collaborate amongst them

Users' needs

Users' needs

Users want

Users' needs

Users want

- To find others for communicating

Users' needs

Users want

- To find others for communicating
- To be found by possible partners for projects

Users' needs

Users want

- To find others for communicating
- To be found by possible partners for projects

but they do not want

Users' needs

Users want

- To find others for communicating
- To be found by possible partners for projects

but they do not want

- their data exposed

Legal matters
in the problem

Legal matters
in the problem

- People's right to privacy

Legal matters
in the problem

- People's right to privacy
  Persons have the right to conceal their data

Legal matters
in the problem

- People's right to privacy
  Persons have the right to conceal their data
- Internet searchable directories may be international transfers of personal data

Technical requirements
that are part of the problem

Technical requirements
that are part of the problem

- The directory should be accessed directly

Technical requirements
that are part of the problem

- The directory should be accessed directly
- Enforce the policy regardless the access method.

Technical requirements
that are part of the problem

- The directory should be accessed directly
- Enforce the policy regardless the access method.
- Different treatment for

Technical requirements
that are part of the problem

- The directory should be accessed directly
- Enforce the policy regardless the access method.
- Different treatment for
  - Inside searches

Technical requirements
that are part of the problem

- The directory should be accessed directly
- Enforce the policy regardless the access method.
- Different treatment for
  - Inside searches
  - Outside searches

Technical requirements
that are part of the problem

- The directory should be accessed directly
- Enforce the policy regardless the access method.
- Different treatment for
  - Inside searches
  - Outside searches
- Reduce the administrative burden

Different approaches
for solving the problem

Different approaches
for solving the problem

- Lawyers approach

Different approaches
for solving the problem

- Lawyers approach

Ditch the directory

Different approaches
for solving the problem

- Lawyers approach

Ditch the directory

- Users approach

Different approaches
for solving the problem

- Lawyers approach

  Ditch the directory

- Users approach

  None

Different approaches
for solving the problem

- Lawyers approach

  Ditch the directory

- Users approach

  None, they just want *it* to work

Different approaches
for solving the problem

- Lawyers approach

  Ditch the directory

- Users approach

  None, they just want *it* to work

- Technicians approach

Different approaches
for solving the problem

- Lawyers approach

  Ditch the directory

- Users approach

  None, they just want *it* to work

- Technicians approach

  Ditch the lawyers

Points to find a solution
without having to ditch anyone

Points to find a solution
without having to ditch anyone

- Put control on the hands of the user

Points to find a solution
without having to ditch anyone

- Put control on the hands of the user
- Policy is defined by the organization

Points to find a solution
without having to ditch anyone

- Put control on the hands of the user
- Policy is defined by the organization
- Abide by the law

Two sides of a coin

user side / server side

Two sides of a coin
user side / server side

- User side

Two sides of a coin
user side / server side

- User side
  The user must have control of her data

Two sides of a coin
user side / server side

- User side
  The user must have control of her data
- Server side

Two sides of a coin
user side / server side

- User side
  The user must have control of her data
- Server side
  The solution must work whichever the interface

The user decides about his data

The user decides about his data

We need:

The user decides about his data

We need:

- An interface for setting user preferences

The user decides about his data

We need:

- An interface for setting user preferences
  We know what to do

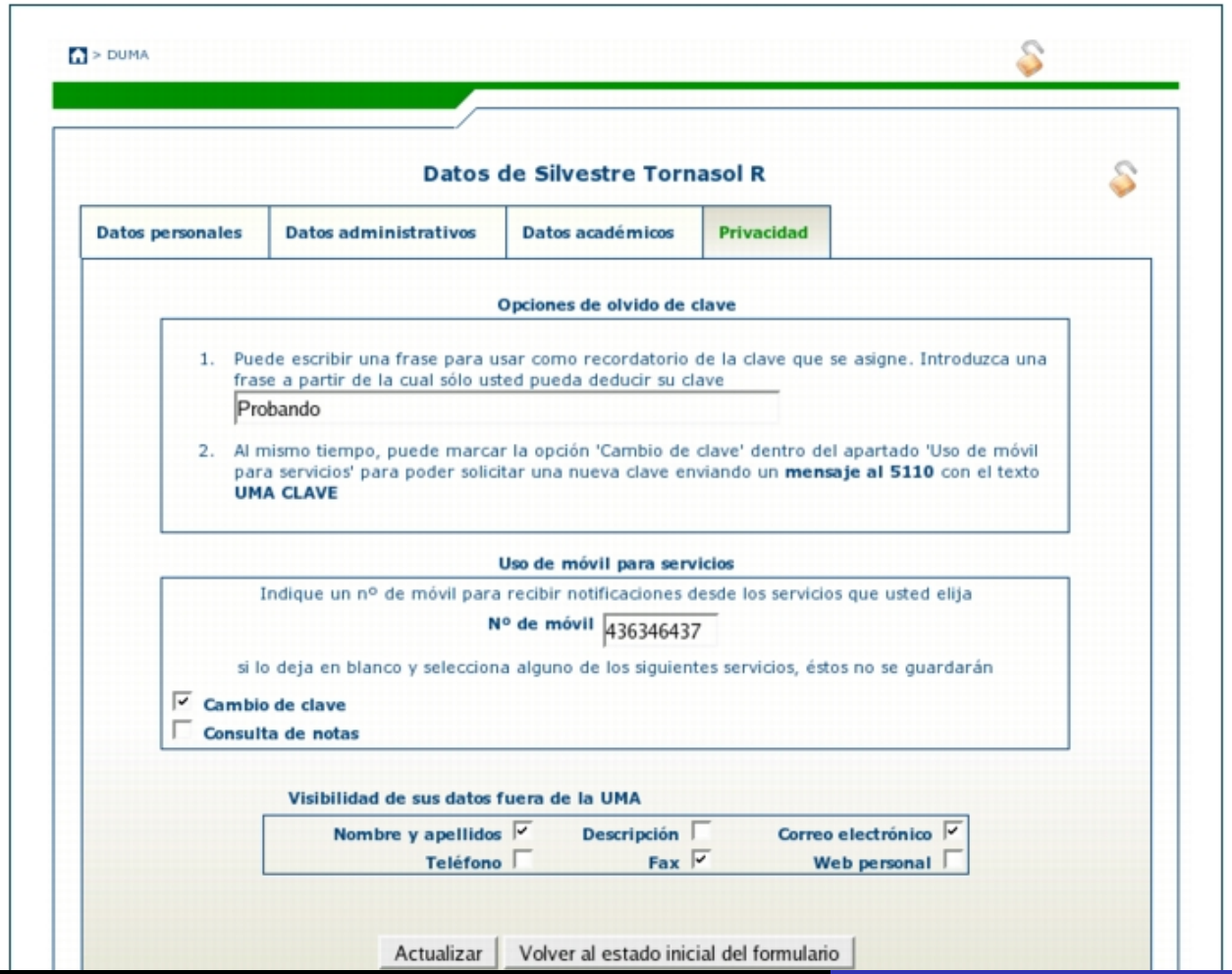
The user decides about his data

We need:

- An interface for setting user preferences
  We know what to do: design a nice web form

The user decides about his data

via a nice web form



The user decides about his data

We need:

- An interface for setting user preferences
  We know what to do: design a nice web form
- Directory attribute for holding the preferences

The user decides about his data

We need:

- An interface for setting user preferences
  We know what to do: design a nice web form
- Directory attribute for holding the preferences

irisUserPrivateAttribute

The user decides about his data

We need:

- An interface for setting user preferences
  We know what to do: design a nice web form
- Directory attribute for holding the preferences

schacUserPrivateAttribute

The user decides about his data

We need:

- An interface for setting user preferences
  We know what to do: design a nice web form
- Directory attribute for holding the preferences

schacUserPrivateAttribute

because Europe likes the idea

The institution sets the policy

The institution sets the policy

- Policy enforcement whichever the interface

The institution sets the policy

- Policy enforcement whichever the interface
  Application level control is discarded

The institution sets the policy

- Policy enforcement whichever the interface
  Application level control is discarded
- Policy enforcement at server level

The institution sets the policy

- Policy enforcement whichever the interface
  Application level control is discarded
- Policy enforcement at server level
  using OpenLDAP ACLs

Summary

Summary

- The user has control of her personal data

Summary

- The user has control of her personal data
- The policy is enforced at the server

Summary

- The user has control of her personal data
- The policy is enforced at the server
- Lawyers seem happy

Summary

- The user has control of her personal data
- The policy is enforced at the server
- Lawyers seem happy
- The solution is simple

Summary

- The user has control of her personal data
- The policy is enforced at the server
- Lawyers seem happy
- The solution is simple
- And it even

Summary

- The user has control of her personal data
- The policy is enforced at the server
- Lawyers seem happy
- The solution is simple
- And it even

WORKS

Summary

- The user has control of her personal data
- The policy is enforced at the server
- Lawyers seem happy
- The solution is simple
- And it even

WORKS

and we will be pleased to show it to anyone willing to

Revealing our attributes

though in a partial a virtual way

Revealing our attributes

though in a partial a virtual way

Definitions

LDAP, *Lightweigth Directory Access Protocol*

Source: Wikipedia.org

Definitions

LDAP, *Lightweigth Directory Access Protocol*

+ Network protocol used for querying and updating directory services over TCP/IP.

Source: Wikipedia.org

Definitions

LDAP, *Lightweigth Directory Access Protocol*

- Network protocol used for querying and updating directory services over TCP/IP.
- Usually, an LDAP directory follows the X.500 model: a tree of entries, each of which is composed of a set of attributes with name and value.

Source: Wikipedia.org

Definitions

LDAP, *Lightweigth Directory Access Protocol*

- Network protocol used for querying and updating directory services over TCP/IP.
- Usually, an LDAP directory follows the X.500 model: a tree of entries, each of which is composed of a set of attributes with name and value.
- Often an LDAP directory maps political, geographical and organizational divisions.

Source: Wikipedia.org

Definitions

LDAP, *Lightweigth Directory Access Protocol*

- Network protocol used for querying and updating directory services over TCP/IP.
- Usually, an LDAP directory follows the X.500 model: a tree of entries, each of which is composed of a set of attributes with name and value.
- Often an LDAP directory maps political, geographical and organizational divisions.
- The present version is LDAPv3, defined in RFC 3377

Source: Wikipedia.org

Definitions

OpenLDAP

Source: Wikipedia.org

Definitions

OpenLDAP

+ Free Open Source implementation of LDAP protocol.

Source: Wikipedia.org

Definitions

OpenLDAP

- Free Open Source implementation of LDAP protocol.
- The software is developed by the OpenLDAP Project and is distributed under its own license: *OpenLDAP Public License*.

Source: Wikipedia.org

Definitions

ACL, Access Control List

Source: Wikipedia.org

Definitions

ACL, Access Control List

+ Computer security concept used to enforce privilege separation.

Source: Wikipedia.org

Definitions

ACL, Access Control List

- Computer security concept used to enforce privilege separation.
- It's a means of determining access rights to a certain object depending on certain characteristics of the process that makes the request, mainly the identity of the process user.

Source: Wikipedia.org

OpenLDAP ACLs I

Privacy policy for students

irisUserPrivateAttribute may have a value of *all* or may be empty, denying or allowing access to ALL optional attributes, defined in *attrs*. Actually, our present policy for student personal data, denies access to the whole entry.

Deny access to all attributes

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(&(eduPersonAffiliation=student)
                  (irisUserPrivateAttribute=all))"
        attrs=entry
        by * none
```

OpenLDAP ACLs II

Privacy policy for students

If a student clears her irisUserPrivateAttribute, then the system allows access to the entry and, then, to the policy permitted attributes, so they may be shown.

Allow access to permited attributes

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(eduPersonAffiliation=student)"
        attrs=entry,displayName,mail,telephoneNumber
        by * read
```

OpenLDAP ACLs III

Privacy policy for non students

The organization may decide that an entry should not appear in searches. Then irisUserPrivateAttribute receives the value *entry*.

Blocking all access

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(irisUserPrivateAttribute=entry)"
        by * none
```

OpenLDAP ACLs IV

Privacy policy for non students

The user may decide which attributes should be hidden to anonymous searches, from a set defined by the organization's policy. irisUserPrivateAttribute holds the names of such attributes. In case the search is done by a bound user, the attribute is shown.

Blocking access to the phone number

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(irisUserPrivateAttribute=telephoneNumber)"
        attrs=telephoneNumber
        by users read
        by * none
```

OpenLDAP ACLs V

Privacy policy for non students

The user may decide to hide all attributes in the set defined by the organization's policy. In such case, irisUserPrivateAttribute holds a value of *all*. If the search is done by a bound user, the attributes are shown.

Blocking access to all attributes

```
access to dn.subtree="idnc=usr,dc=uma,dc=es"
        filter="(irisUserPrivateAttribute=all)"
        attrs=mail,telephoneNumber,facsimileTelephoneNumber
        by users read
        by * none
```