The implications of

Simon Willison

Google Tech Talk, 25th June 2007

Who here has used OpenID?

Who uses it regularly?

What **is** OpenID?

OpenID is a
decentralised mechanism
for Single Sign On

What problems
does it solve?

“Too many passwords!”

“Someone else already grabbed my username”

“My online profile is scattered across dozens of sites”

What is **an OpenID**?

An OpenID is a URL

http://swillison.livejournal.com/

http://simonw.myopenid.com/

http://simonwillison.net/

http://openid.aol.com/simonwillison/

What can you do with an OpenID?

You can claim
that you own it

You can prove
that claim

Why is **that** useful?

You can use it for authentication

“Who the heck are you?!”

“I’m simonwillison.net”

“prove it!”

XTECH CONFERENCE
XTech 2007: “The Ubiquitous Web” — 15-18 May 2007, Paris, France
News
About
Register
Schedule
Speakers
Sponsorship
Media
Hotel & venue
Speaker info
XTech 2006
News feeds
Atom 1.0
RSS 1.0
Registration has now opened for XTech 2007
Join us on 15-18 May 2007, in Paris, France for Europe’s premier web technology conference.
Register • Schedule • Tutorials • Sponsor • Keynotes • BOFs
Online registration closed, but you can still register on-site
Community coverage of XTech 2007
To read aggregated coverage of XTech 2007, head over to Planet XTech. Featuring blog posts, bookmarks and photos from the conference, Planet XTech is a good way to get a snapshot of what people are seeing and saying.
If you’re attending XTech, there’s an easy way to get your coverage on to Planet XTech: just tag your blog posts, Flickr pictures or del.icio.us bookmarks as ‘xtech’, and the planet will pick them up.
Link | 14-May-2007 18:12 CEST
Web Browser, Standards and Interop Summit, XTech Paris
In Paris this May 15th, XTech 2007, Molly.Com, Inc. and Useful Information Company have combined resources to join industry influentials and peers for the first annual Browser, Standards and Interop Summit in parallel with the XTech conference.
The Summit will consist of an open meeting of as many browser vendors, standards advocates, W3C and related standards supporters as we can gather. We will also have workgroups and an open mike session so everyone can be heard.
The day will be open to observation for interested journalists (particularly bloggers, podcasters and videocasters) based on available space. Participants will include representatives from Opera Software, Mozilla, Microsoft Corporation and others. It’s an opportunity to make voices heard
Your account
Email address
Password
New user?
Log in
Log in with an OpenID (?)
XTech 2007 news
Subscribe to receive news about XTech
Partners
AOL
DataDirect TECHNOLOGIES
IBM
JUST. SYSTEMS

(magic happens)

“OK, you’re in!”

XTECH CONFERENCE
XTech 2007: “The Ubiquitous Web” — 15-18 May 2007, Paris, France
News
About
Register
Schedule
Speakers
Sponsorship
Media
Hotel & venue
Speaker info
XTech 2006
News feeds
Atom 1.0
RSS 1.0
Registration has now opened for XTech 2007
Join us on 15-18 May 2007, in Paris, France for Europe’s premier web technology conference.
Register • Schedule • Tutorials • Sponsor • Keynotes • BOFs
Online registration closed, but you can still register on-site
Community coverage of XTech 2007
To read aggregated coverage of XTech 2007, head over to Planet XTech. Featuring blog posts, bookmarks and photos from the conference, Planet XTech is a good way to get a snapshot of what people are seeing and saying.
If you’re attending XTech, there’s an easy way to get your coverage on to Planet XTech: just tag your blog posts, Flickr pictures or del.icio.us bookmarks as ‘xtech’, and the planet will pick them up.
Link | 14-May-2007 18:12 CEST
Web Browser, Standards and Interop Summit, XTech Paris
In Paris this May 15th, XTech 2007, Molly.Com, Inc. and Useful Information Company have combined resources to join industry influentials and peers for the first annual Browser, Standards and Interop Summit in parallel with the XTech conference.
The Summit will consist of an open meeting of as many browser vendors, standards advocates, W3C and related standards supporters as we can gather. We will also have workgroups and an open mike session so everyone can be heard.
The day will be open to observation for interested journalists (particularly bloggers, podcasters and videocasters) based on available space. Participants will include representatives from Opera Software, Mozilla, Microsoft Corporation and others. It’s an opportunity to make voices heard
Your account
Email address
Password
New user?
Log in
Log in with an OpenID (?)
XTech 2007 news
Subscribe to receive news about XTech
Partners
AOL
DataDirect TECHNOLOGIES
IBM
JUST. SYSTEMS

So it's a bit like Microsoft Passport, then?

Yes, but you don’t need to ask their permission to implement it

And Microsoft
don’t get to own your
credentials

Who **does** get to own them?

You, the user, decide.

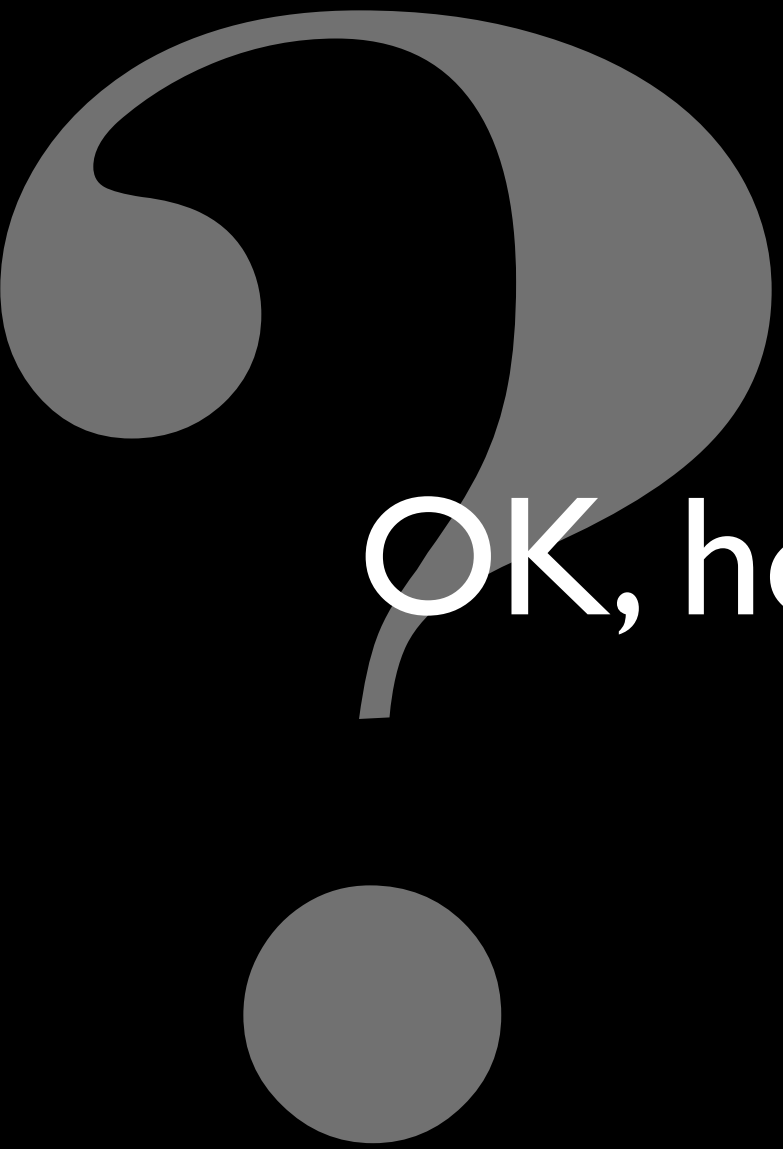
You pick your own provider

(just like e-mail)

So I'm still giving someone the keys to my kingdom?

Yes, but it can be someone you trust

If you have the ability to run your own server software, you can do it for yourself.



OK, how do I use it?

Zooomr :: Experience the World Through Photos

http://beta.zooomr.com/home

Google

Sign-In | Sign-Up

Zooomr™

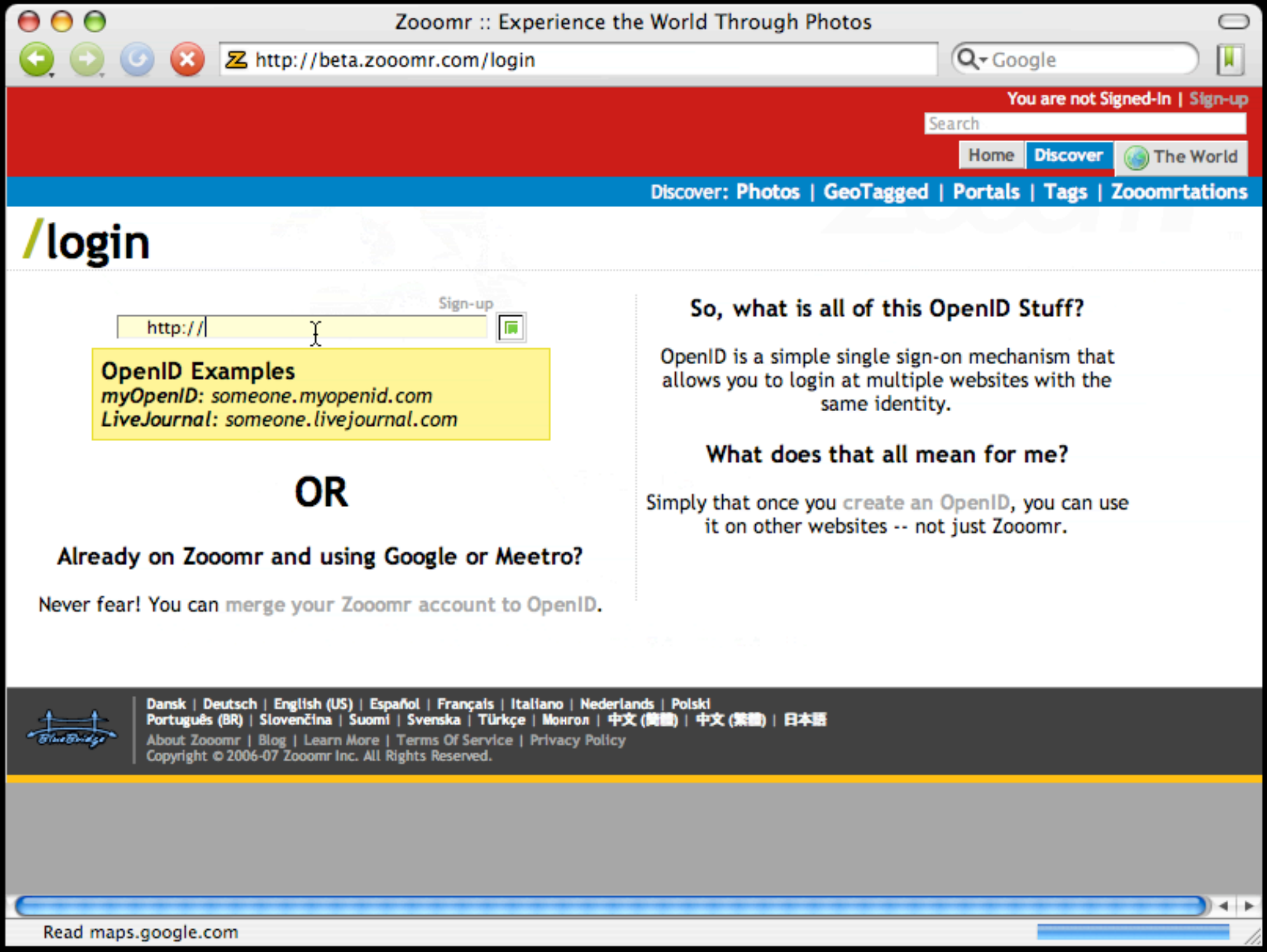
Universally the best way to share, search, store and sort your photos online.

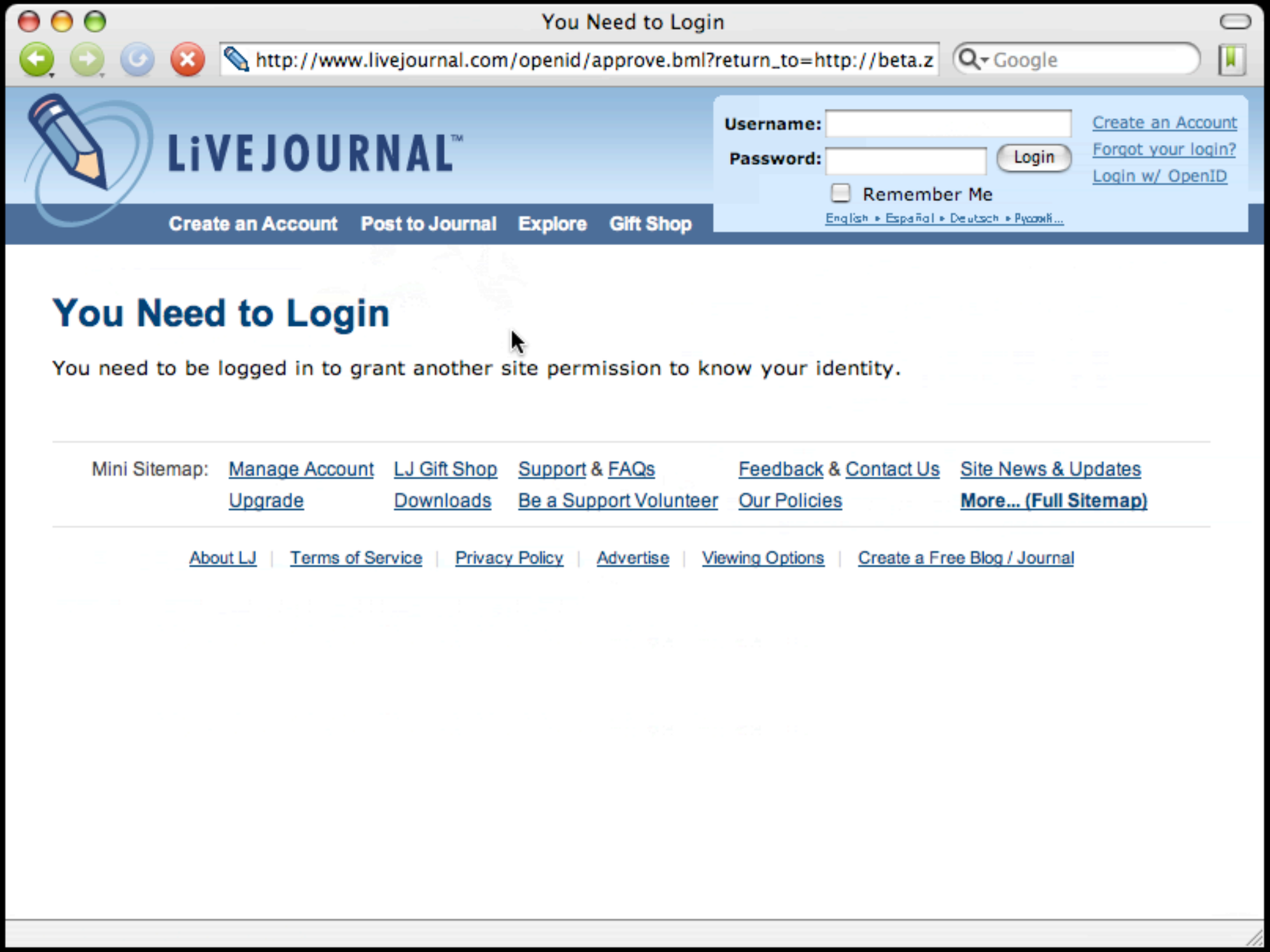
Learn More

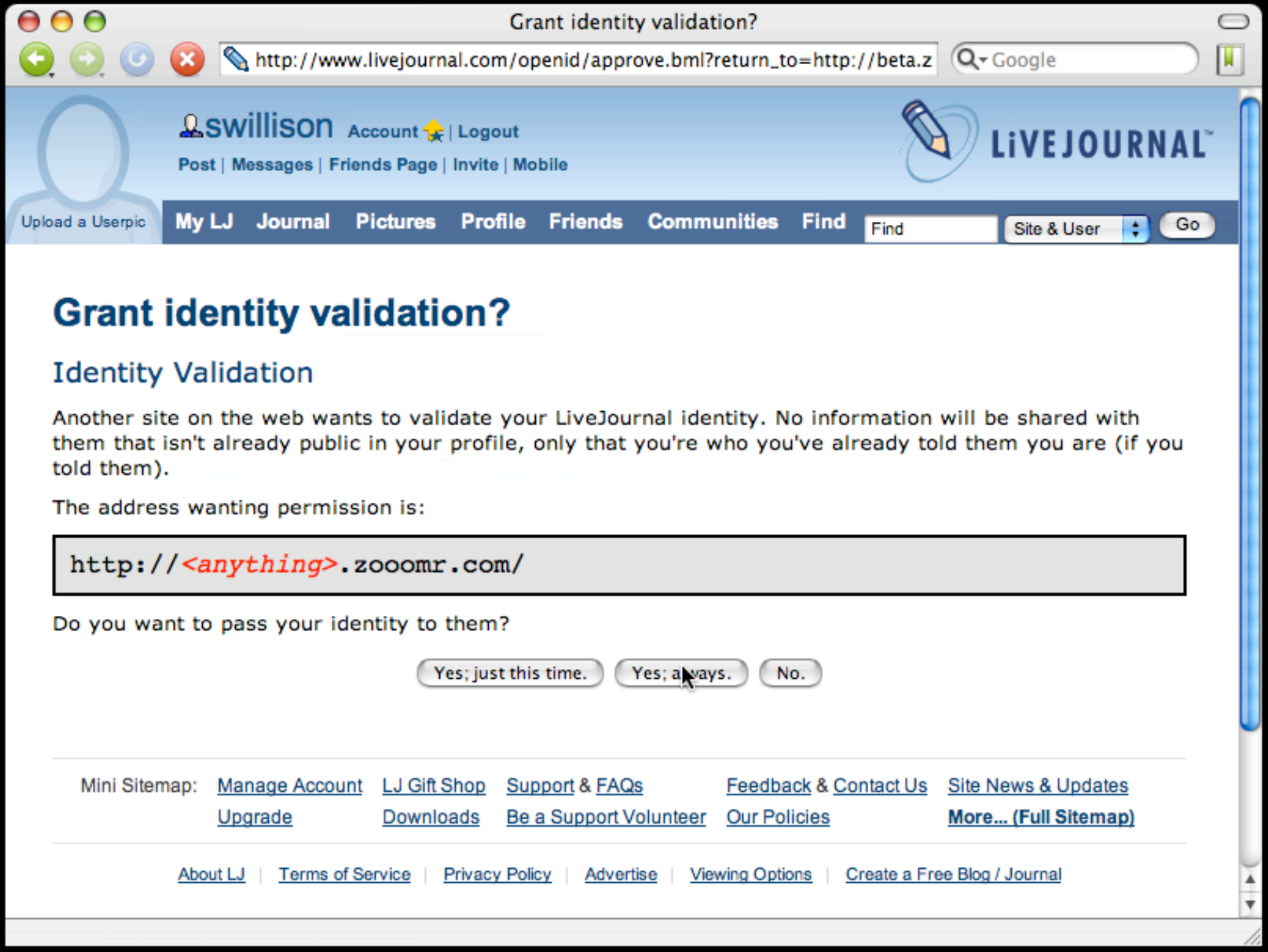
Dansk | Deutsch | English (US) | Español | Français | Italiano | Nederlands | Polski
Português (BR) | Slovenčina | Suomi | Svenska | Türkçe | Монгол | 中文 (簡體) | 中文 (繁體) | 日本語

About Zooomr | Blog | Learn More | Terms Of Service | Privacy Policy

Copyright © 2006-07 Zooomr Inc. All Rights Reserved.


Zooomr :: Experience the World Through Photos
http://beta.zooomr.com/login
Google
You are not Signed-In | Sign-up
Search
Home
Discover
The World
Discover: Photos | GeoTagged | Portals | Tags | Zooomrtations
/login
Sign-up
http://
OpenID Examples
myOpenID: someone.myopenid.com
LiveJournal: someone.livejournal.com
OR
Already on Zooomr and using Google or Meetro?
Never fear! You can merge your Zooomr account to OpenID.
So, what is all of this OpenID Stuff?
OpenID is a simple single sign-on mechanism that allows you to login at multiple websites with the same identity.
What does that all mean for me?
Simply that once you create an OpenID, you can use it on other websites -- not just Zooomr.
Dansk | Deutsch | English (US) | Español | Français | Italiano | Nederlands | Polski
Português (BR) | Slovenčina | Suomi | Svenska | Türkçe | Монгол | 中文 (簡體) | 中文 (繁體) | 日本語
About Zooomr | Blog | Learn More | Terms Of Service | Privacy Policy
Copyright © 2006-07 Zooomr Inc. All Rights Reserved.
Read maps.google.com


You Need to Login
http://www.livejournal.com/openid/approve.bml?return_to=http://beta.z
Google
LiVEJOURNAL™
Username:
Password:
Login
Remember Me
Create an Account
Forgot your login?
Login w/ OpenID
English • Español • Deutsch • Русский...
Create an Account
Post to Journal
Explore
Gift Shop
You Need to Login
You need to be logged in to grant another site permission to know your identity.
Mini Sitemap:
Manage Account
LJ Gift Shop
Support & FAQs
Feedback & Contact Us
Site News & Updates
Upgrade
Downloads
Be a Support Volunteer
Our Policies
More... (Full Sitemap)
About LJ
Terms of Service
Privacy Policy
Advertise
Viewing Options
Create a Free Blog / Journal


Grant identity validation?
http://www.livejournal.com/openid/approve.bml?return_to=http://beta.z
Google
swillison Account | Logout
Post | Messages | Friends Page | Invite | Mobile
LiVEJOURNAL
Upload a Userpic
My LJ Journal Pictures Profile Friends Communities Find
Find
Site & User
Go
Grant identity validation?
Identity Validation
Another site on the web wants to validate your LiveJournal identity. No information will be shared with them that isn't already public in your profile, only that you're who you've already told them you are (if you told them).
The address wanting permission is:
http://<anything>.zooomr.com/
Do you want to pass your identity to them?
Yes; just this time.
Yes; always.
No.
Mini Sitemap: Manage Account LJ Gift Shop Support & FAQs Feedback & Contact Us Site News & Updates
Upgrade Downloads Be a Support Volunteer Our Policies More... (Full Sitemap)
About LJ | Terms of Service | Privacy Policy | Advertise | Viewing Options | Create a Free Blog / Journal

Zooomr :: Experience the World Through Photos

http://beta.zooomr.com/welcomemat

Google

Hello, swillison! | | Sign-Out

Search

WelcomeMat | Upload | Discover | You | Social Circle | The World

You: Your Photos | Your Profile | Your Faves | Recent Activity | Your Account

/WelcomeMat

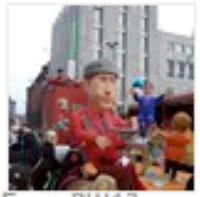
Hey, swillison!

You last logged in on Sun 12 Feb 2006 16:19:53 PST

What would you like to do?

» Upload photos
» View your photos page
» View your profile page

Everyone's Photos


From DIM13

From DIM13

From LordTureis

From DIM13

From DIM13

Dansk | Deutsch | English (US) | Español | Français | Italiano | Nederlands | Polski
Português (BR) | Slovenčina | Suomi | Svenska | Türkçe | Монгол | 中文 (简體) | 中文 (繁體) | 日本語

About Zooomr | Blog | Learn More | Terms Of Service | Privacy Policy

Copyright © 2006-07 Zooomr Inc. All Rights Reserved.

So my users don't have to sign up for an account?

Not necessarily

An OpenID tells you
very little about a user

You don’t know
their name

You don’t know
their e-mail address

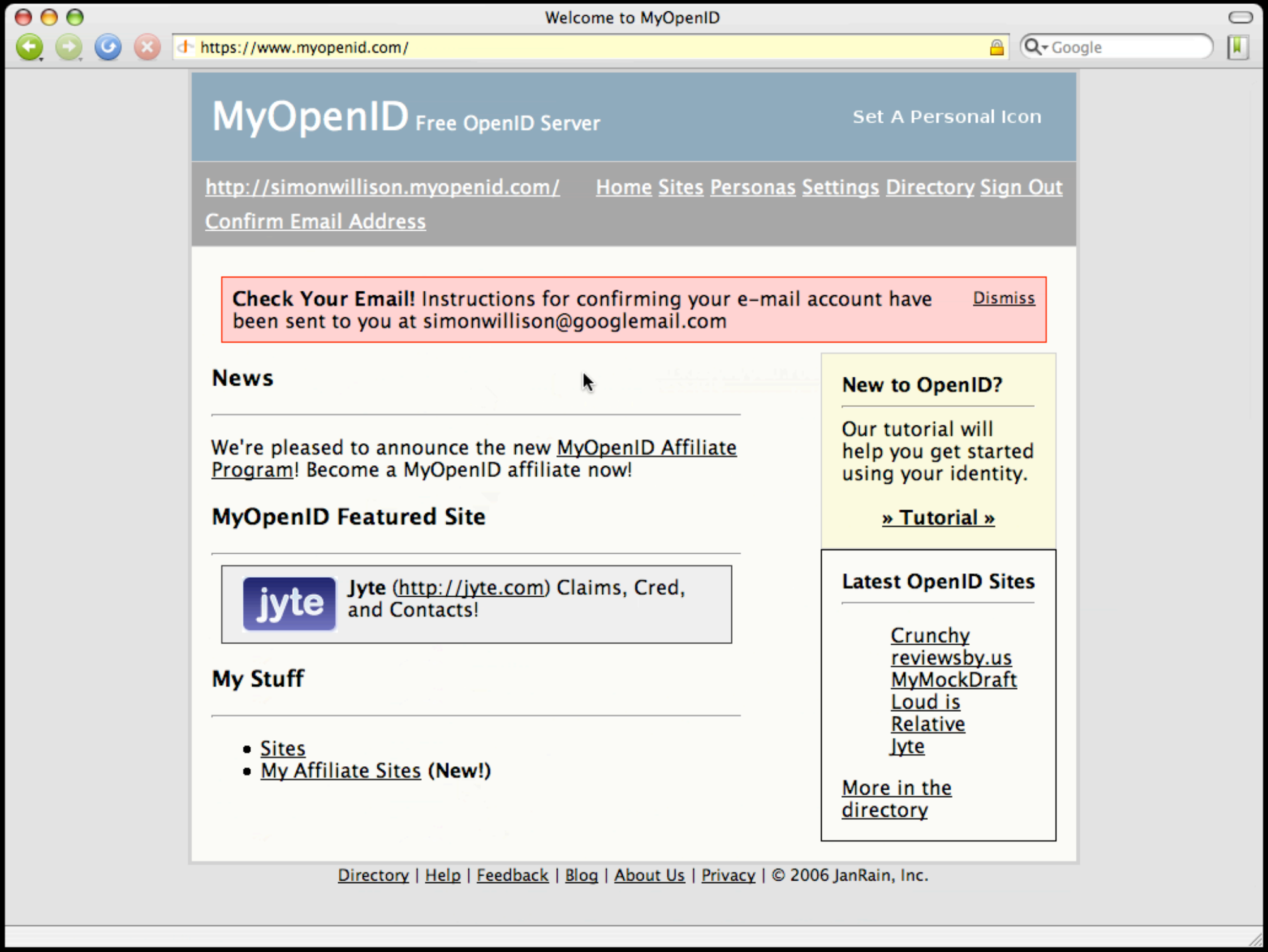
You don’t know
if they’re a person
or an evil robot

(or a dog)

Where do I get that information from?

You ask them!

OpenID can even help them answer


Welcome to MyOpenID
https://www.myopenid.com/
Google
MyOpenID Free OpenID Server
Set A Personal Icon
http://simonwillison.myopenid.com/ Home Sites Personas Settings Directory Sign Out
Confirm Email Address
Check Your Email! Instructions for confirming your e-mail account have been sent to you at simonwillison@googlemail.com
Dismiss
News
We're pleased to announce the new MyOpenID Affiliate Program! Become a MyOpenID affiliate now!
MyOpenID Featured Site
jyte
Jyte (http://jyte.com) Claims, Cred, and Contacts!
My Stuff
Sites
My Affiliate Sites (New!)
New to OpenID?
Our tutorial will help you get started using your identity.
» Tutorial »
Latest OpenID Sites
Crunchy
reviewsby.us
MyMockDraft
Loud is Relative
Jyte
More in the directory
Directory | Help | Feedback | Blog | About Us | Privacy | © 2006 JanRain, Inc.

Ma.gnolia.com – Find Web Sites & Build Community Online

http://ma.gnolia.com/

Google

Sign In | Learn More

ma.gnolia

Discover, share and discuss the best of the web. Join Us or Learn More.

xmlDate

Marked in Ma.gnolia by davosian

Find more about javascript, timezones or work

Download "Ma.gnolia Blossom," Damien Tanner's Dashboard Widget

Discover sites about tshirts, cool GO

Featured Linker

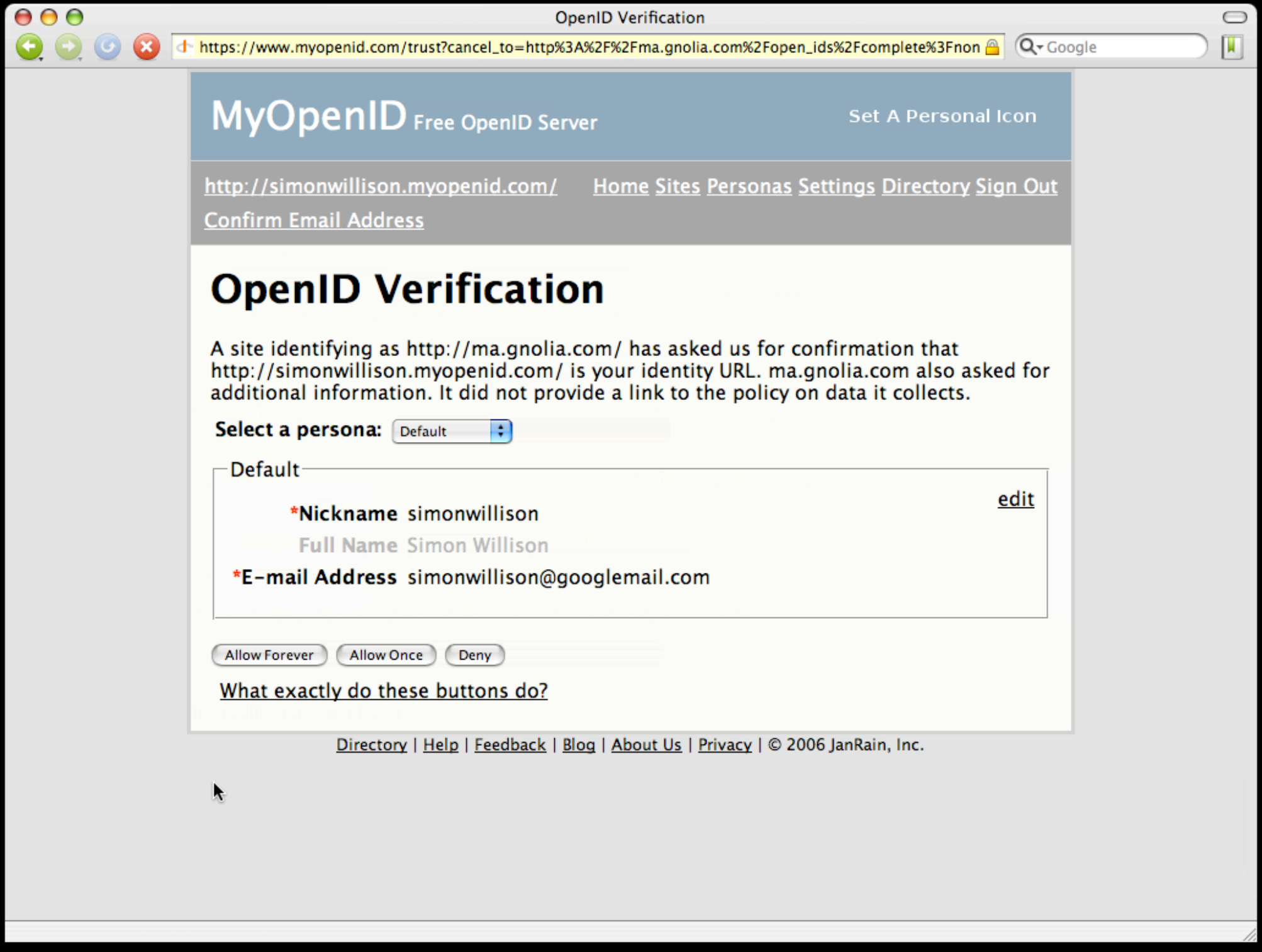
Don Cram

Fr Don is Canon Pastor of the Episcopal Cathedral Church in Albuquerque, an avid reader, cook, motorcyclist, live-steam garden railroader, and since 1986 a Mac user.

Hot Group

Graphic Design & More

Graphic design is influenced by innovations and ideas from countless other industries—these links showcase items that spark the mind of the professional creative.

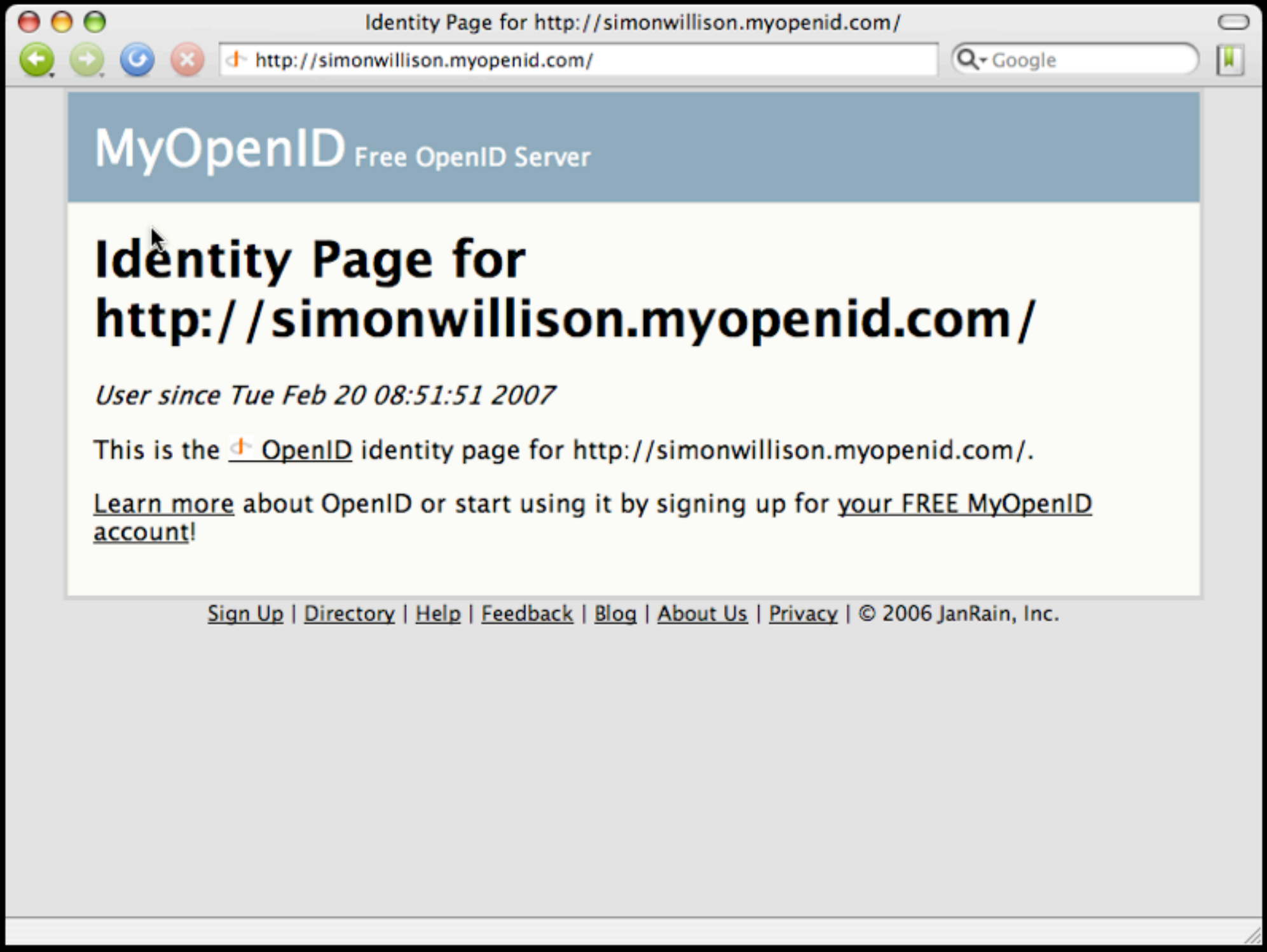

OpenID Verification
https://www.myopenid.com/trust?cancel_to=http%3A%2F%2Fma.gnolia.com%2Fopen_ids%2Fcomplete%3Fnon
Google
MyOpenID Free OpenID Server
Set A Personal Icon
http://simonwillison.myopenid.com/
Home Sites Personas Settings Directory Sign Out
Confirm Email Address
OpenID Verification
A site identifying as http://ma.gnolia.com/ has asked us for confirmation that http://simonwillison.myopenid.com/ is your identity URL. ma.gnolia.com also asked for additional information. It did not provide a link to the policy on data it collects.
Select a persona:
Default
Default
edit
*Nickname simonwillison
Full Name Simon Willison
*E-mail Address simonwillison@googlemail.com
Allow Forever
Allow Once
Deny
What exactly do these buttons do?
Directory | Help | Feedback | Blog | About Us | Privacy | © 2006 JanRain, Inc.

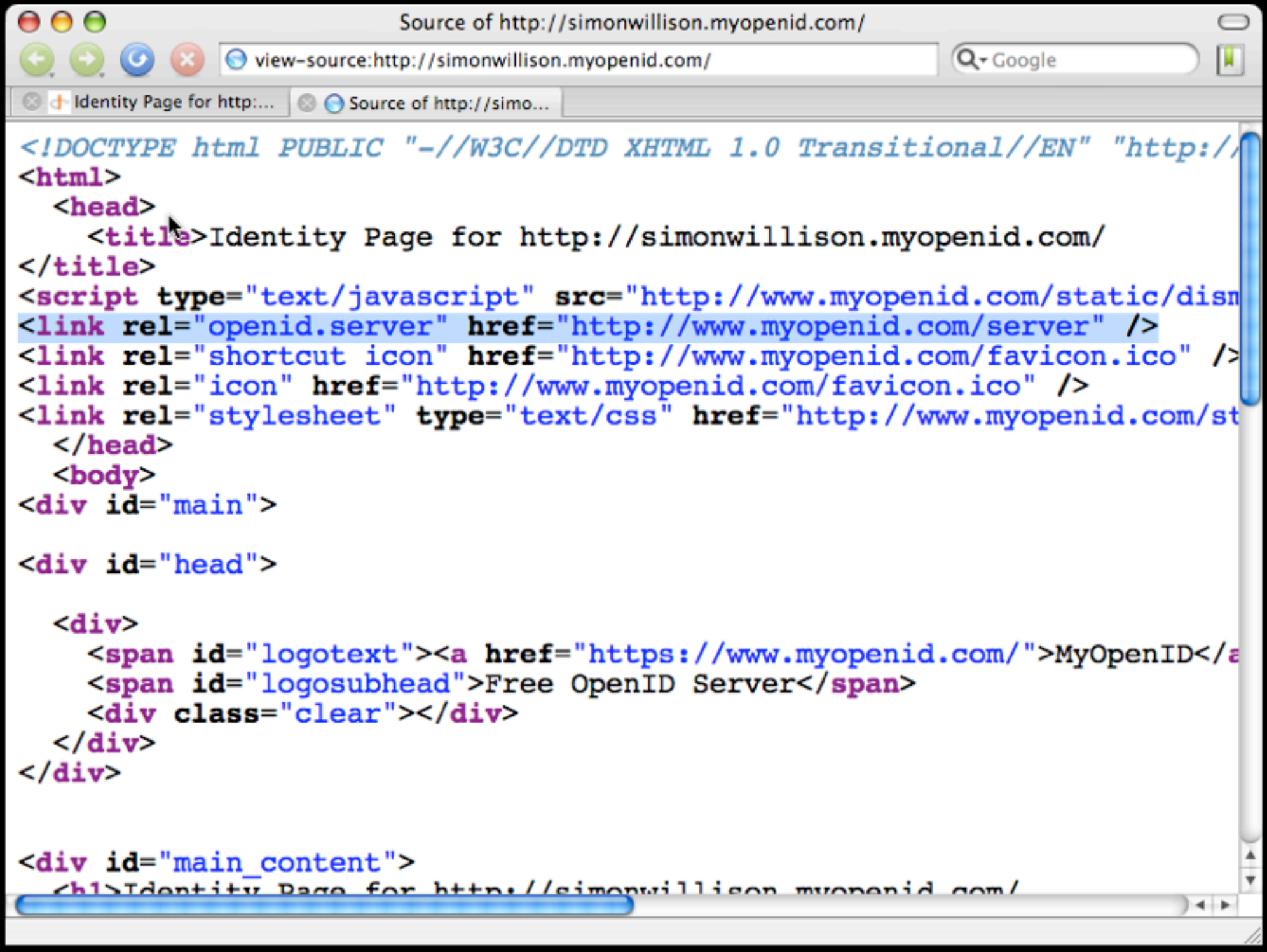
Ma.gnolia.com – Find Web Sites & Build Community Online
http://ma.gnolia.com/open_ids/complete?nonce=B8rDrw55&openid.assoc_handle=%7BHMAC-SHA1%7D%7B45c
Google
Sign In | Learn More
ma.gnolia
BOOKMARKS | TAGS | PEOPLE | GROUPS | DISCUSSIONS | SUPPORT & TOOLS | SIGN IN | JOIN
Your OpenID is Verified!
Your OpenID can now be associated with a new or existing Ma.gnolia membership. You can change the association later in your Ma.gnolia profile.
Associate your OpenID
If you're joining Ma.gnolia, associate your OpenID with a new account. If you're already a member, associate with your existing account.
A New Account
Screen Name
simonwillison
This screen name is available.
Email
simonwillison@gmail.com
This email is not in use.
Notify me about my Ma.gnolia messages and news.
CREATE MY ACCOUNT
By creating an account, you accept our terms of service and privacy policy.
An Existing Account
Screen Name
simonwillison
Password
VERIFY
© 2007 Gnolia Systems. All Rights Reserved.
About Us | Blog | Wiki | Advertise | Terms | Privacy | Contact Us

How can I tell if they're an evil spambot?

Same as usual: challenge them with a CAPTCHA

So how does OpenID actually work?


Identity Page for http://simonwillison.myopenid.com/
http://simonwillison.myopenid.com/
Google
MyOpenID Free OpenID Server
Identity Page for http://simonwillison.myopenid.com/
User since Tue Feb 20 08:51:51 2007
This is the OpenID identity page for http://simonwillison.myopenid.com/.
Learn more about OpenID or start using it by signing up for your FREE MyOpenID account!
Sign Up | Directory | Help | Feedback | Blog | About Us | Privacy | © 2006 JanRain, Inc.


Source of http://simonwillison.myopenid.com/
view-source:http://simonwillison.myopenid.com/
Google
Identity Page for http:...
Source of http://simo...
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://
<html>
<head>
<title>Identity Page for http://simonwillison.myopenid.com/
</title>
<script type="text/javascript" src="http://www.myopenid.com/static/dism
<link rel="openid.server" href="http://www.myopenid.com/server" />
<link rel="shortcut icon" href="http://www.myopenid.com/favicon.ico" />
<link rel="icon" href="http://www.myopenid.com/favicon.ico" />
<link rel="stylesheet" type="text/css" href="http://www.myopenid.com/st
</head>
<body>

<a href="https://www.myopenid.com/">MyOpenID</a
Free OpenID Server

<h1>Identity Page for http://simonwillison.myopenid.com/

```
<link rel="openid.server"
  href="http://www.myopenid.com/server" />
```

“I’m simonwillison.myopenid.com”

Site fetches HTML,
discovers identity provider

Establishes shared secret with identity provider

(Using Diffie-Hellman key exchange)

Redirects you to the identity provider

If you’re logged in there,
you get redirected back

How does my identity provider know who I am?

OpenID deliberately doesn't specify

username/password
is common

But providers can use other methods if they want to

Client SSL certificates

Out of band
authentication via SMS,
e-mail or Jabber

IP based login restrictions

(one guy set that up
using DynDNS)

SecurID keyfobs

No authentication at all
(just say “Yes”)

Just say “yes”?

Yup. That's the OpenID version of bugmenot.com

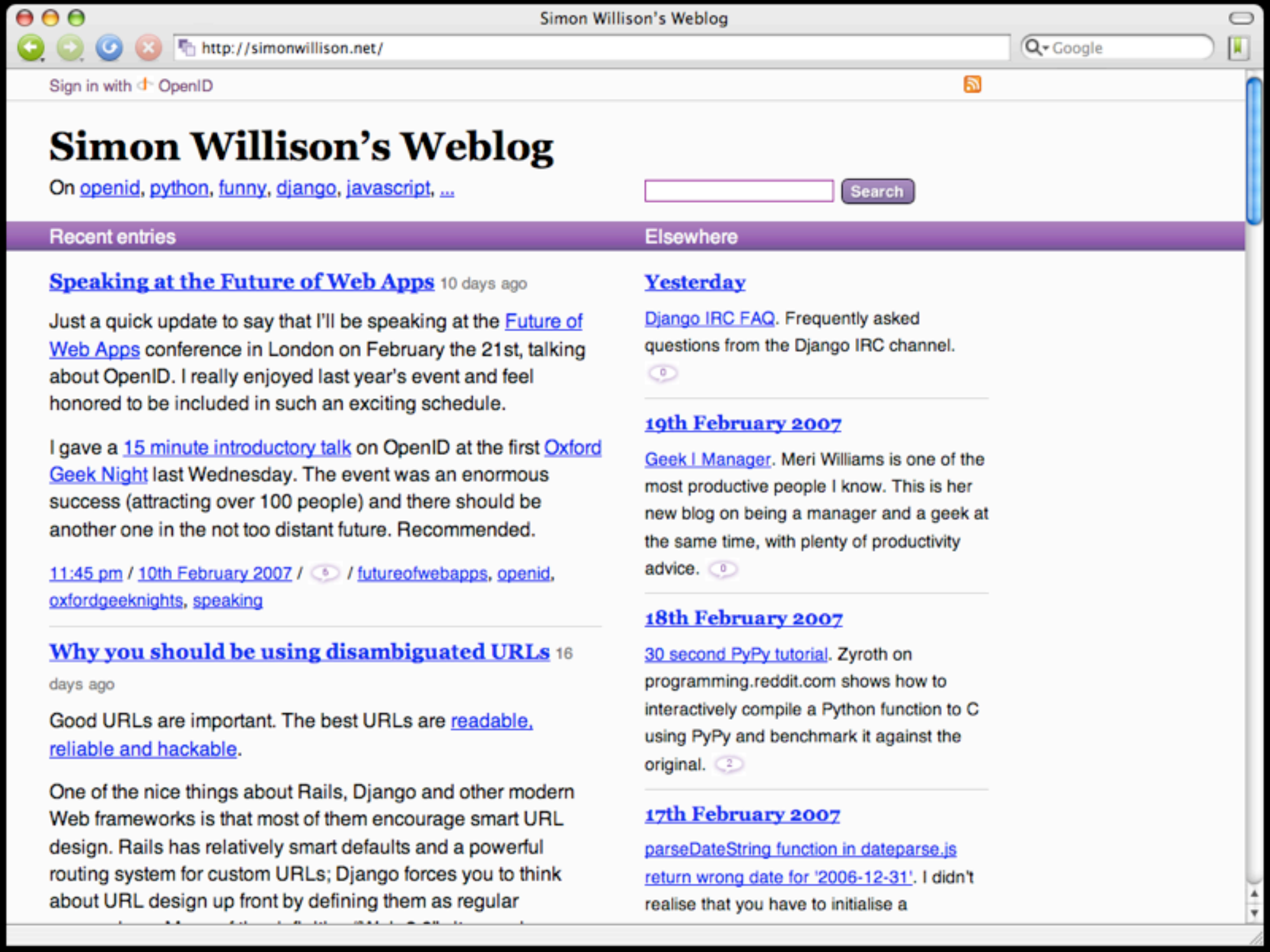
http://www.jkg.in/openid/

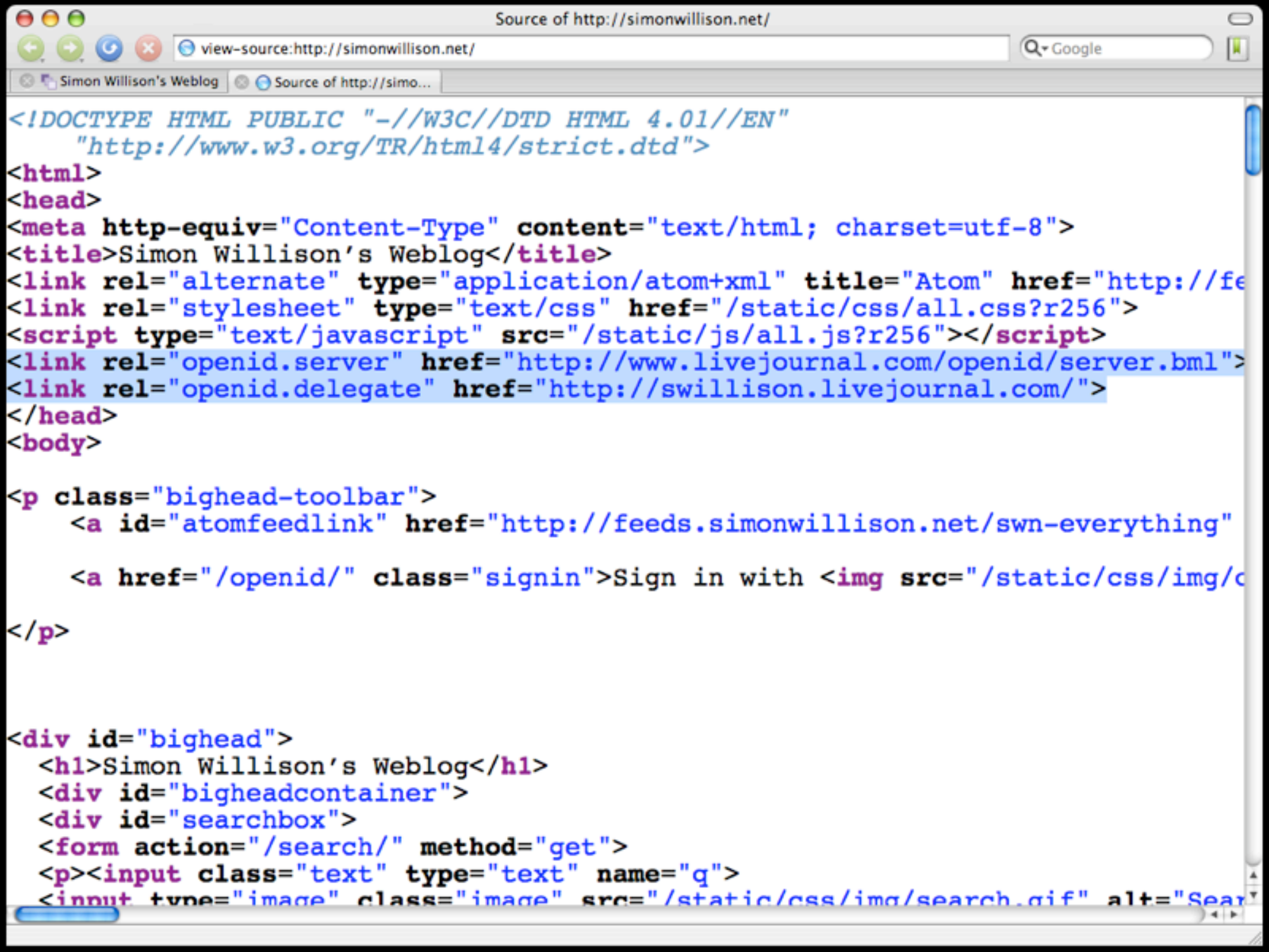
Users can give away their passwords today - this is just the OpenID equivalent

What if I decide I hate my provider?

Use your own domain name

Delegate to a
provider you trust


Simon Willison's Weblog
http://simonwillison.net/
Google
Sign in with OpenID
Simon Willison's Weblog
On openid, python, funny, django, javascript, ...
Search
Recent entries
Elsewhere
Speaking at the Future of Web Apps 10 days ago
Just a quick update to say that I'll be speaking at the Future of Web Apps conference in London on February the 21st, talking about OpenID. I really enjoyed last year's event and feel honored to be included in such an exciting schedule.
I gave a 15 minute introductory talk on OpenID at the first Oxford Geek Night last Wednesday. The event was an enormous success (attracting over 100 people) and there should be another one in the not too distant future. Recommended.
11:45 pm / 10th February 2007 / 5 / futureofwebapps, openid, oxfordgeeknights, speaking
Why you should be using disambiguated URLs 16 days ago
Good URLs are important. The best URLs are readable, reliable and hackable.
One of the nice things about Rails, Django and other modern Web frameworks is that most of them encourage smart URL design. Rails has relatively smart defaults and a powerful routing system for custom URLs; Django forces you to think about URL design up front by defining them as regular
Yesterday
Django IRC FAQ. Frequently asked questions from the Django IRC channel.
0
19th February 2007
Geek | Manager. Meri Williams is one of the most productive people I know. This is her new blog on being a manager and a geek at the same time, with plenty of productivity advice. 0
18th February 2007
30 second PyPy tutorial. Zyroth on programming.reddit.com shows how to interactively compile a Python function to C using PyPy and benchmark it against the original. 2
17th February 2007
parseDateString function in dateparse.js return wrong date for '2006-12-31'. I didn't realise that you have to initialise a


Source of http://simonwillison.net/
view-source:http://simonwillison.net/
Google
Simon Willison's Weblog
Source of http://simo...
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Simon Willison's Weblog</title>
<link rel="alternate" type="application/atom+xml" title="Atom" href="http://fe
<link rel="stylesheet" type="text/css" href="/static/css/all.css?r256">
<script type="text/javascript" src="/static/js/all.js?r256"></script>
<link rel="openid.server" href="http://www.livejournal.com/openid/server.bml">
<link rel="openid.delegate" href="http://swillison.livejournal.com/">
</head>
<body>

<a id="atomfeedlink" href="http://feeds.simonwillison.net/swn-everything"
<a href="/openid/" class="signin">Sign in with <img src="/static/css/img/c

<h1>Simon Willison's Weblog</h1>

<form action="/search/" method="get">
<input class="text" type="text" name="q">
<input type="image" class="image" src="/static/css/img/search.gif" alt="Sear

```
<link rel="openid.server"
  href="http://www.livejournal.com/openid/server.bml">
<link rel="openid.delegate"
  href="http://swillison.livejournal.com/">
```

Support for delegation
is **compulsory**

This minimises lock in

So everyone will end up with one OpenID that they use for everything?

Probably not

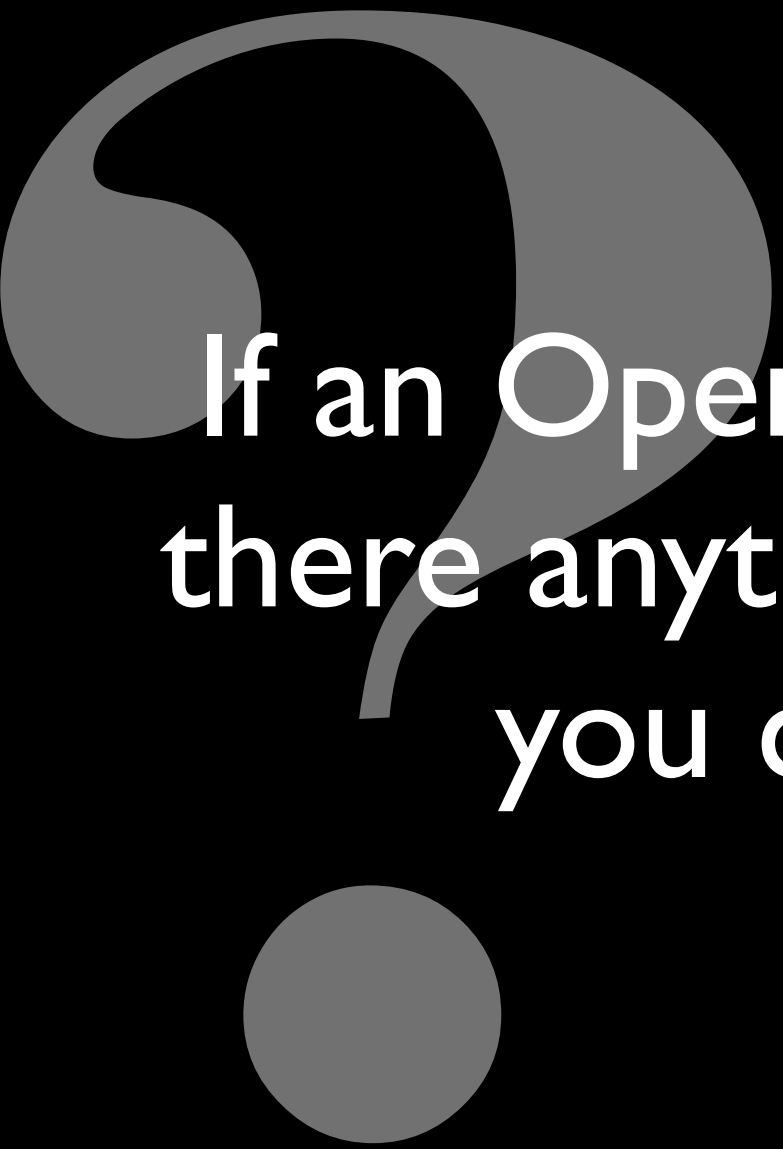
(I have half a dozen
OpenIDs already)

People like maintaining multiple online personas

professional
social
secret
...

OpenID makes it easier to manage multiple online personas

Three accounts is still
better than three dozen



If an OpenID is just a URL, is there anything else interesting you can do with it?

Yes. Different OpenIDs can express different things

My AOL OpenID proves my AIM screen name

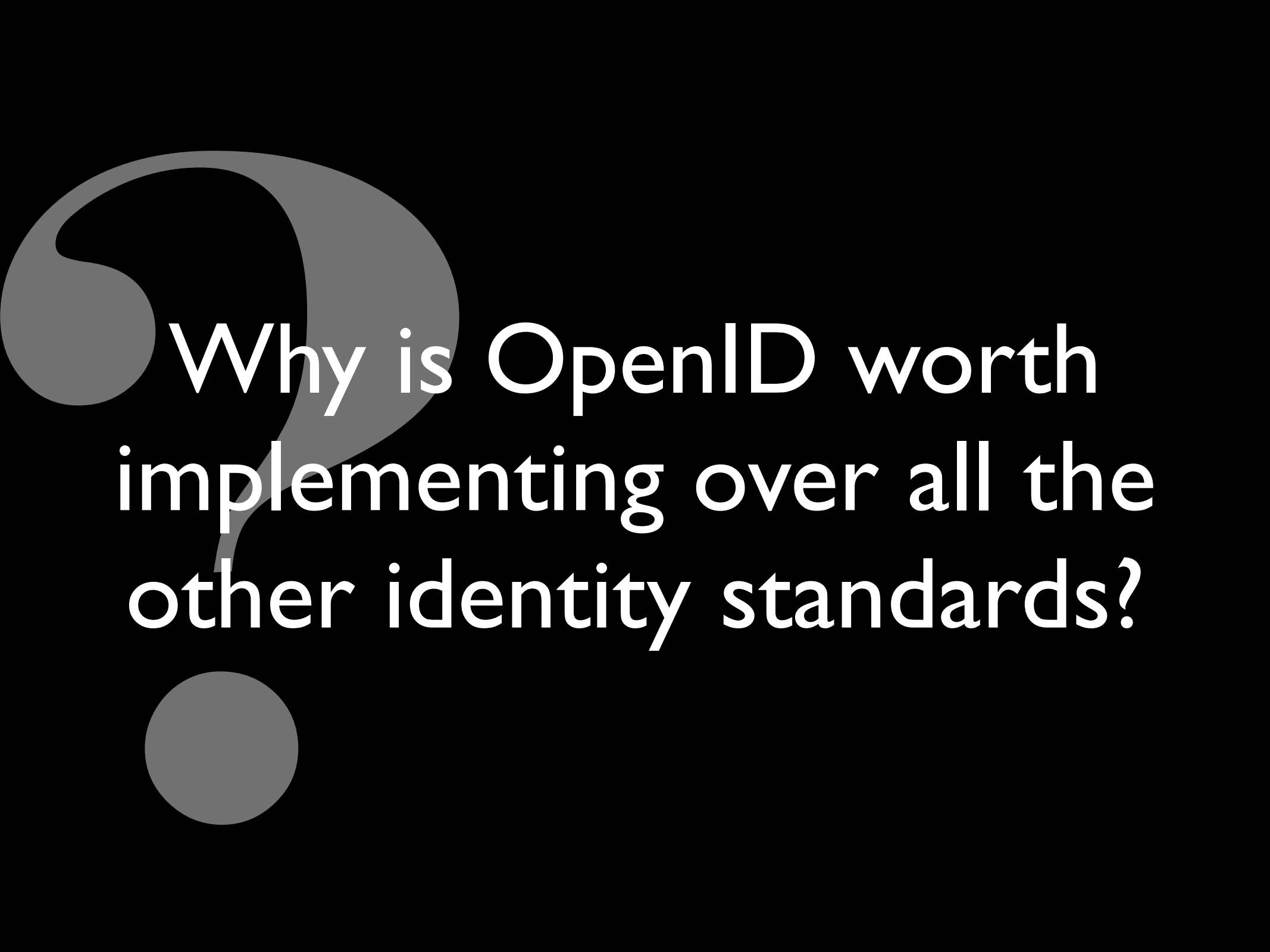
An OpenID from sun.com proves that someone is a current Sun employee

A last.fm OpenID
could incorporate
my taste in music

My LiveJournal OpenID tells you where to find my blog

... and a FOAF file
listing my friends

doxory.com uses this
for contact imports


Why is OpenID worth implementing over all the other identity standards?

It’s simple

Unix philosophy:
It solves one,
tiny problem

It’s a dumb network

Many of the competing standards are now on board

Isn't putting all my eggs in one basket a really bad idea?

Bad news: chances are you already do

“I forgot my password” means your e-mail account is already an SSO mechanism

OpenID just makes this
a bit more obvious

What about phishing?

Phishing is a problem

I can has lolcats!? BETA

Make your own lolcats! lol

Sign in with your OpenID:

OpenID: Sign in

http://icanhascheezburger.com/2007/05/16/i-has-a-backpack/

Your identity provider

Fake edition

Username and password, please!

Username:

Password:

Log in

Identity theft :(

An untrusted site redirects you to your trusted provider

Sound familiar?

PayPal
Yahoo! BBAuth
Google Auth
Google Checkout

You guys already need
to solve that problem!

One solution: don't let the user log in on the identity provider "landing page"

You need to sign in

You need to log in to idproxy.net to complete this process.

You should **use a bookmark** or **type in the address** to do this. This page does not contain any links, to protect you from phishing.

Better solutions

CardSpace

Native browser support for OpenID (e.g. SeatBelt)

Competition between providers

Permanent cookie set using out-of-band token

Best practices for OpenID consumers?

“I forgot my password” becomes “I can’t sign in with my OpenID”

Allow multiple OpenIDs to be associated with a single account

People can still sign in if one of their providers is down

People can un-associate an OpenID without locking themselves out

You can take advantage of site-specific services around each of their OpenIDs

Any other neat tricks?

Portable contact lists

Facebook (and others) currently ask for the user's Google username and password

I don’t need to tell you
why that’s a horrible idea

Lightweight accounts

Pre-approved accounts

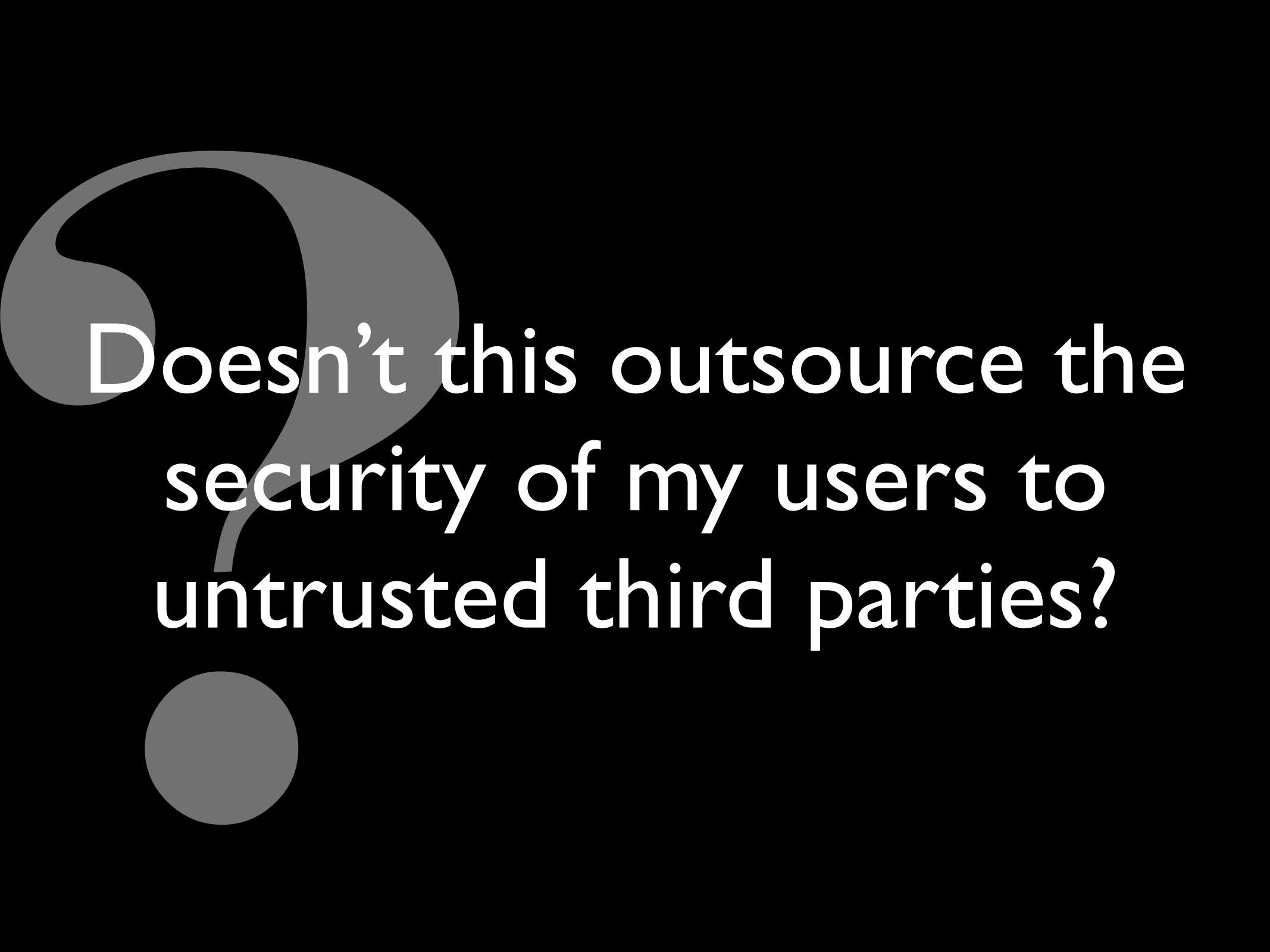
Social whitelists

OpenID and microformats

Decentralised social networks?

"People keep asking me to join the LinkedIn network, but I'm already part of a network, it's called the Internet."

Gary McGraw, via Jon Udell, via Gavin Bell


Doesn’t this outsource the security of my users to untrusted third parties?

Yes it does. But...

... so do “forgotten password” e-mails!

If e-mail is secure enough for your user's authentication, so is OpenID

Password e-mails are essentially SSO with a deliberately bad user experience

What are the privacy implications?

Cross correlation of accounts

Don’t publish a user’s OpenID without making it clear that you’re going to do that

Allow users to opt-out of sharing their OpenID

The online equivalent of a credit reporting agency?

This could be built today by sites conspiring to share e-mail addresses

IANAL, but legal protections against this already exist

“Directed identity” in OpenID 2.0 makes it easy to use a different OpenID for every site

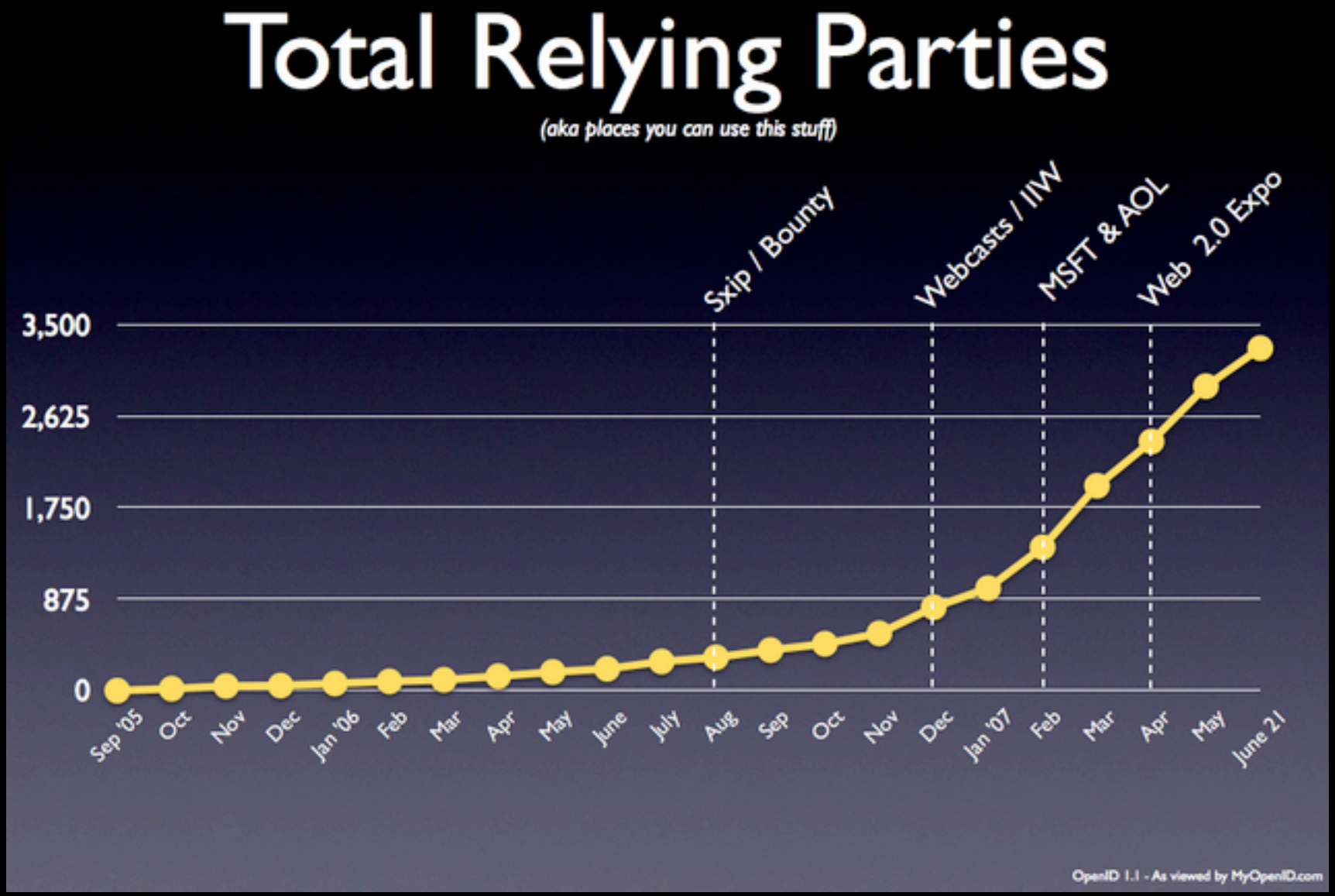
Patents?

Sun and VeriSign have both announced "patent covenants"

They won't smack you down with their patents for using OpenID 1.1

They *will* smack down anyone else who asserts their own patents against OpenID

Who else is involved?



(Slide borrowed from David Recordon)

AOL - provider, full consumer by end of July

Microsoft: Bill Gates expressed their interest at the RSA conference

(mainly as good PR
for CardSpace?)

Sun: Patent Covenant,
33,000 employees

Six Apart

VeriSign

JanRain

Yahoo! - indirectly

idproxy.net – use your Yahoo! account as an OpenID

http://idproxy.net/

Google

idproxy.net

idproxy.net lets you use your Yahoo! account to sign in to sites that support the OpenID standard (read more, blog announcement).

Click below to get started:

YAHOO! Sign In

Home · About this site

Google?

http://openid.net/

http://www.openidenabled.com/

http://simonwillison.net/tags/openid/

Thank you