Web Security:
1) UI-based attacks
2) Tracking on the web

CS 161: Computer Security

Prof. Raluca Ada Popa

November 15, 2016

Contains new slides, slides from past CS 161 offerings and slides from Dan Boneh

Announcements

- Last core lecture, misc topics next
- High level ideas of misc topics on final
- Proj 3 due, Thur 17th Nov

Clickjacking attacks

- Exploitation where a user’s mouse click is used in a way that was not intended by the user

Talk to your partner

- How can a user’s click be used in a way different than intended?

Simple example

```
<a
 onMouseDown=window.open(http://www.evil.com)
 href=http://www.google.com/>
Go to Google</a>
```

What does it do?

- Opens a window to the attacker site

Why include `href` to Google?

- Browser status bar shows URL when hovering over as a means of protection

Recall: Frames

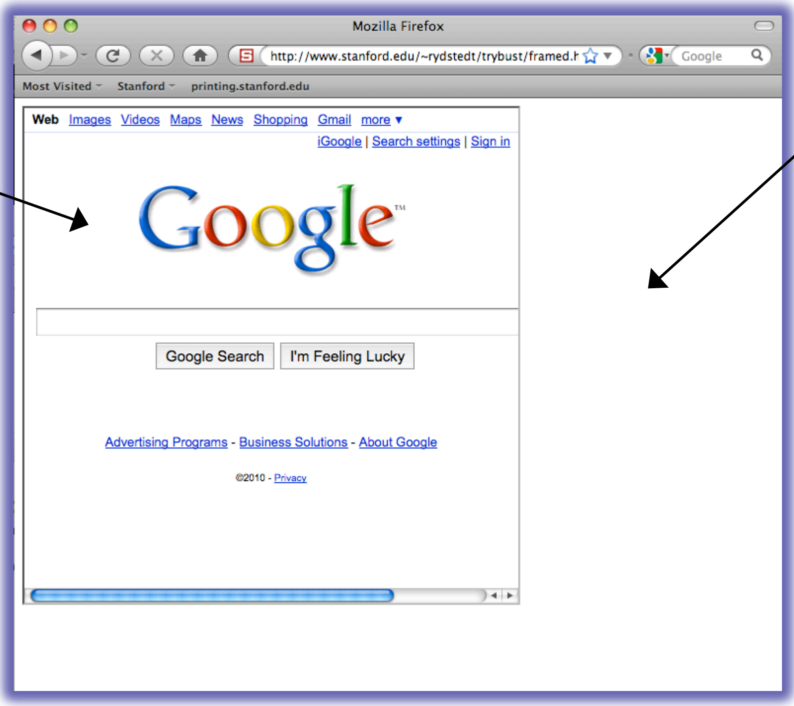
- A frame is used to embed another document within the current HTML document
- Any site can frame another site
- The <iframe> tag specifies an inline frame

Example

HTML page

```
<iframe  src=“http://www.google.com/”>
</iframe>
```

UI rendering


Mozilla Firefox
http://www.stanford.edu/~rydstedt/trybust/framed.h
Google
Most Visited
Stanford
printing.stanford.edu
Web Images Videos Maps News Shopping Gmail more ▾
iGoogle | Search settings | Sign in
Google
Google Search
I'm Feeling Lucky
Advertising Programs - Business Solutions - About Google
©2010 - Privacy

framed page/ inner page

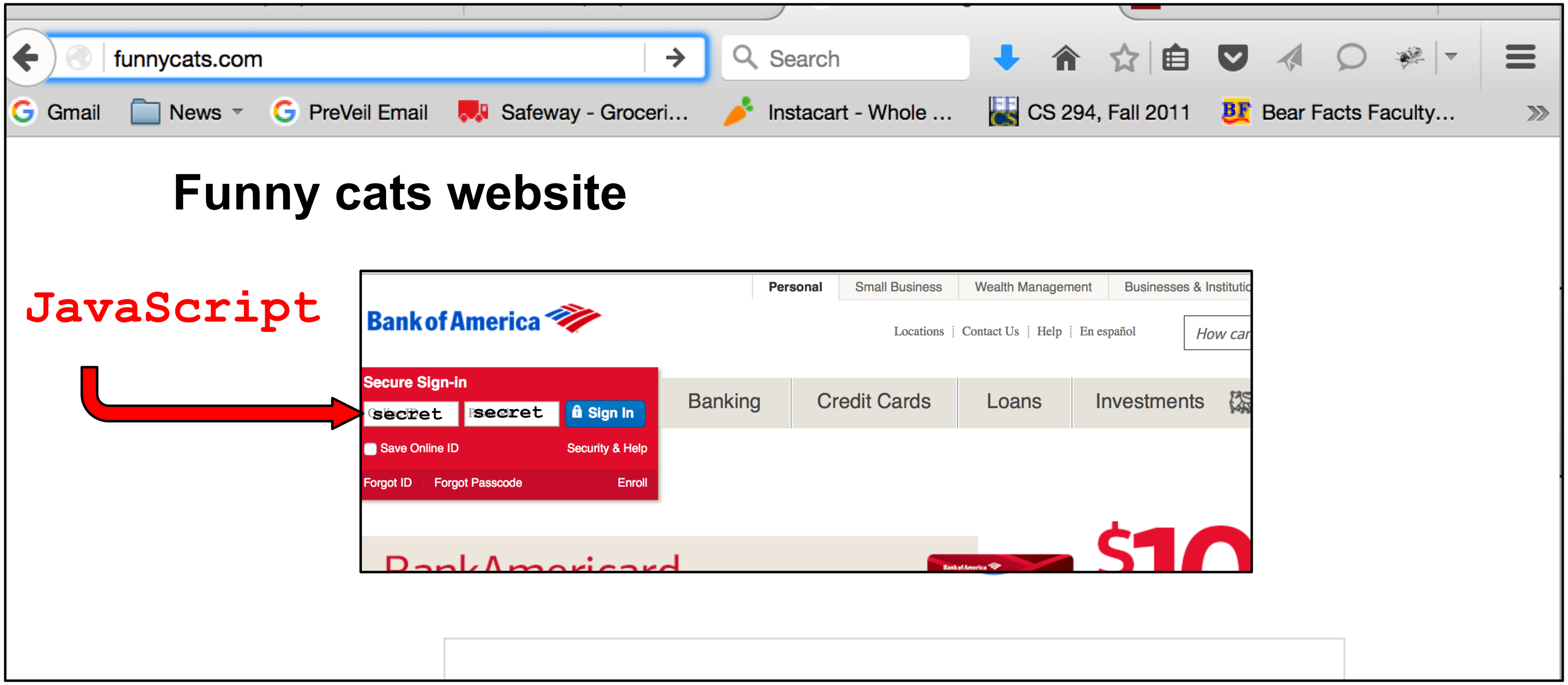
framing page/ outer page

Frames

- Outer page can set frame width, height
- But then, only framed site can draw in its own rectangle

- Modularity
  - Brings together code from different sources

What happens in this case?



funnycats.com

Funny cats website

JavaScript

Secure Sign-in

secret

secret

Frames: same-origin policy

- Frame inherits origin of its URL
- Same-origin policy: if frame and outer page have different origins, they cannot access each other
  - In particular, malicious JS on outer page cannot access resources of inner page

How to bypass same-origin policy for frames?

Clickjacking

Clickjacking using frames

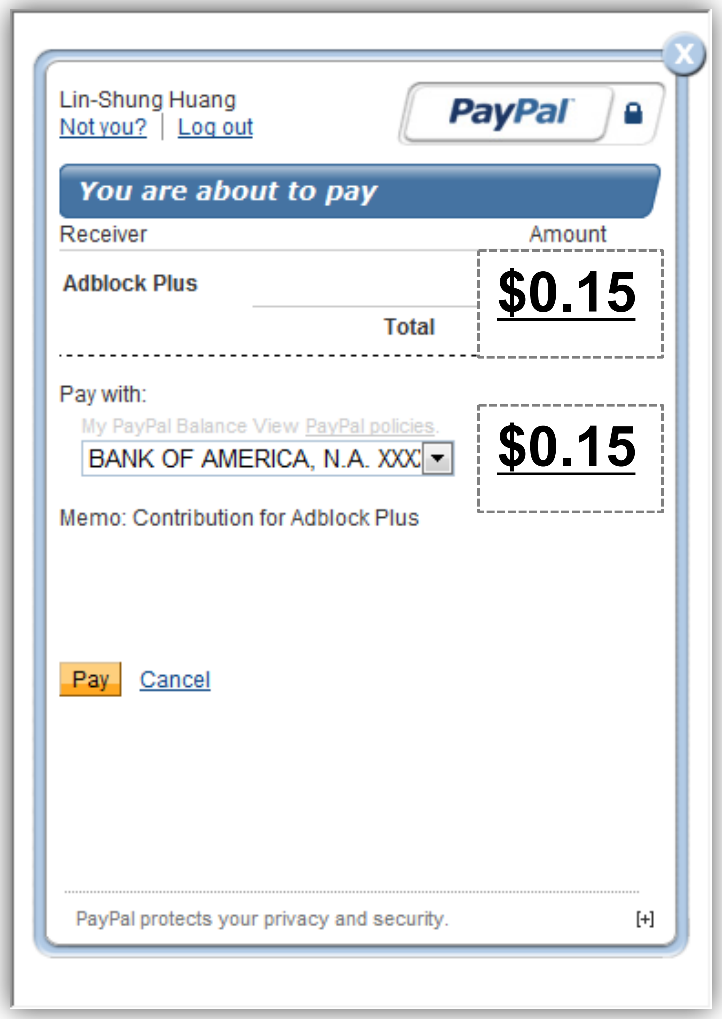
Evil site frames good site

Evil site covers good site by putting dialogue boxes or other elements on top of parts of framed site to create a different effect

Inner site now looks different to user

Compromise visual integrity – target

- Hiding the target
- Partial overlays



Lin-Shung Huang

Not you? | Log out

PayPal

You are about to pay

Receiver Amount

Adblock Plus $0.15

Total

Pay with:

My PayPal Balance View PayPal policies.

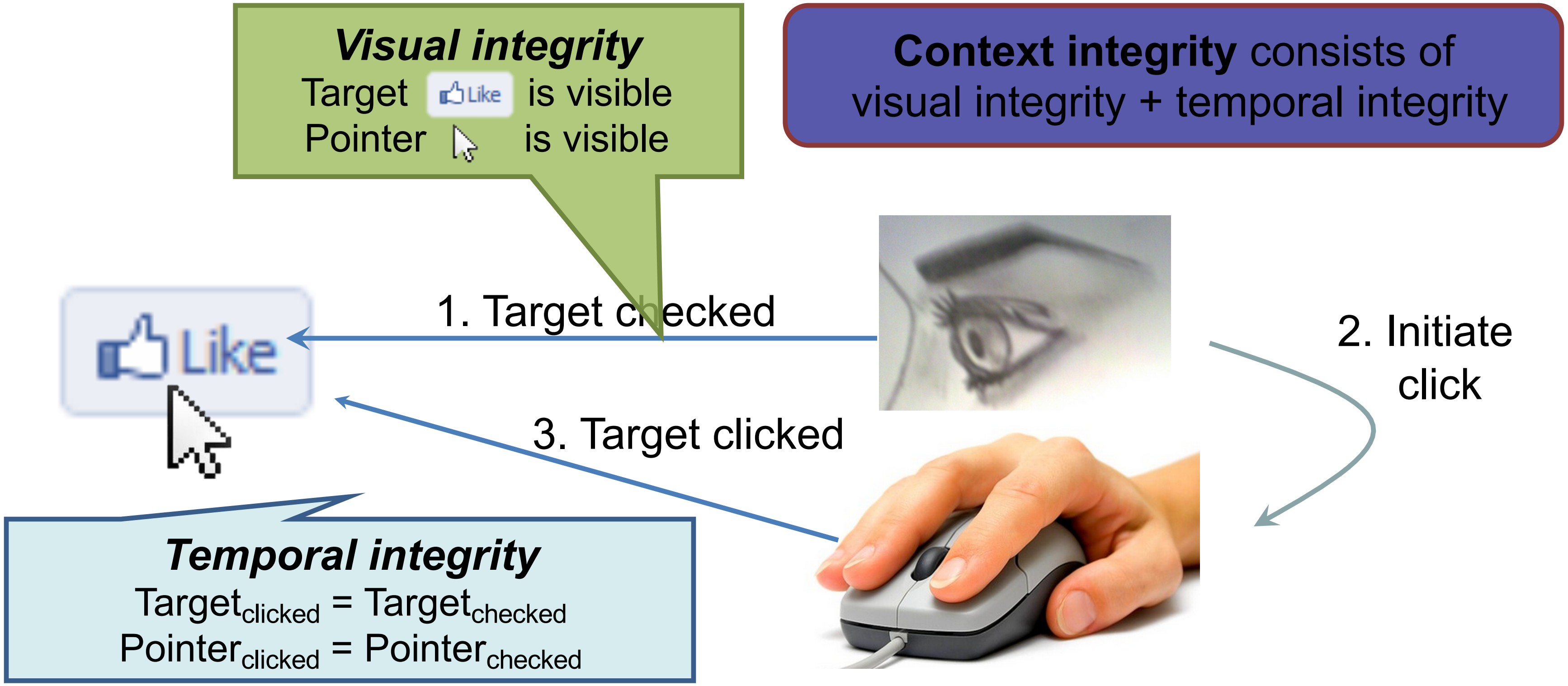
BANK OF AMERICA, N.A. XXX $0.15

Memo: Contribution for Adblock Plus

PayPal protects your privacy and security. [+]

UI Subversion: *Clickjacking*

- An attack application (script) compromises the *context integrity* of another application's User Interface when the user acts on the UI



Visual integrity

Target Like is visible

Pointer is visible

Context integrity consists of visual integrity + temporal integrity

1. Target checked

2. Initiate click

3. Target clicked

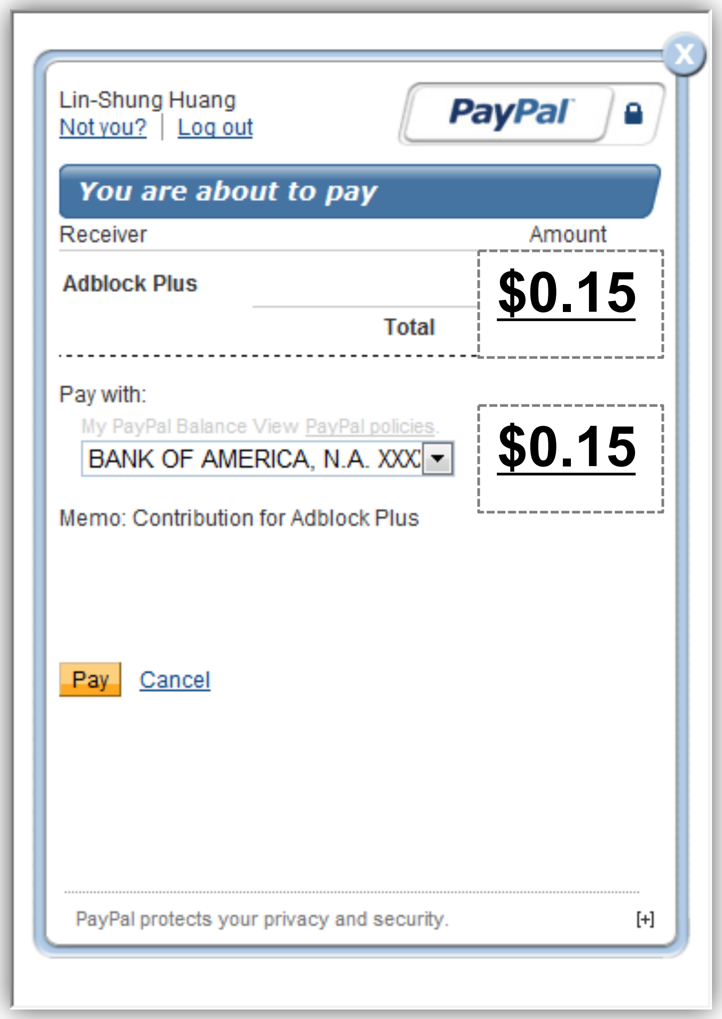
Temporal integrity

$\text{Target}_{\text{clicked}} = \text{Target}_{\text{checked}}$

$\text{Pointer}_{\text{clicked}} = \text{Pointer}_{\text{checked}}$

Compromise visual integrity – target

- Hiding the target
- Partial overlays



Lin-Shung Huang

Not you? | Log out

You are about to pay

Receiver	Amount
Adblock Plus	$0.15
Total	

Pay with:

My PayPal Balance View PayPal policies.

BANK OF AMERICA, N.A. XXX

$0.15

Memo: Contribution for Adblock Plus

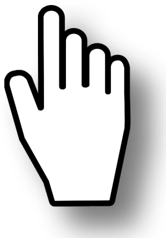
PayPal protects your privacy and security.

Compromise visual integrity – pointer: cursorjacking

- Can customize cursor!

```
CSS example:
#mycursor {
cursor: none;
width: 97px;
height: 137px;
background: url("images/custom-cursor.jpg")
  }
```

- Javascript can keep updating cursor, can display shifted cursor

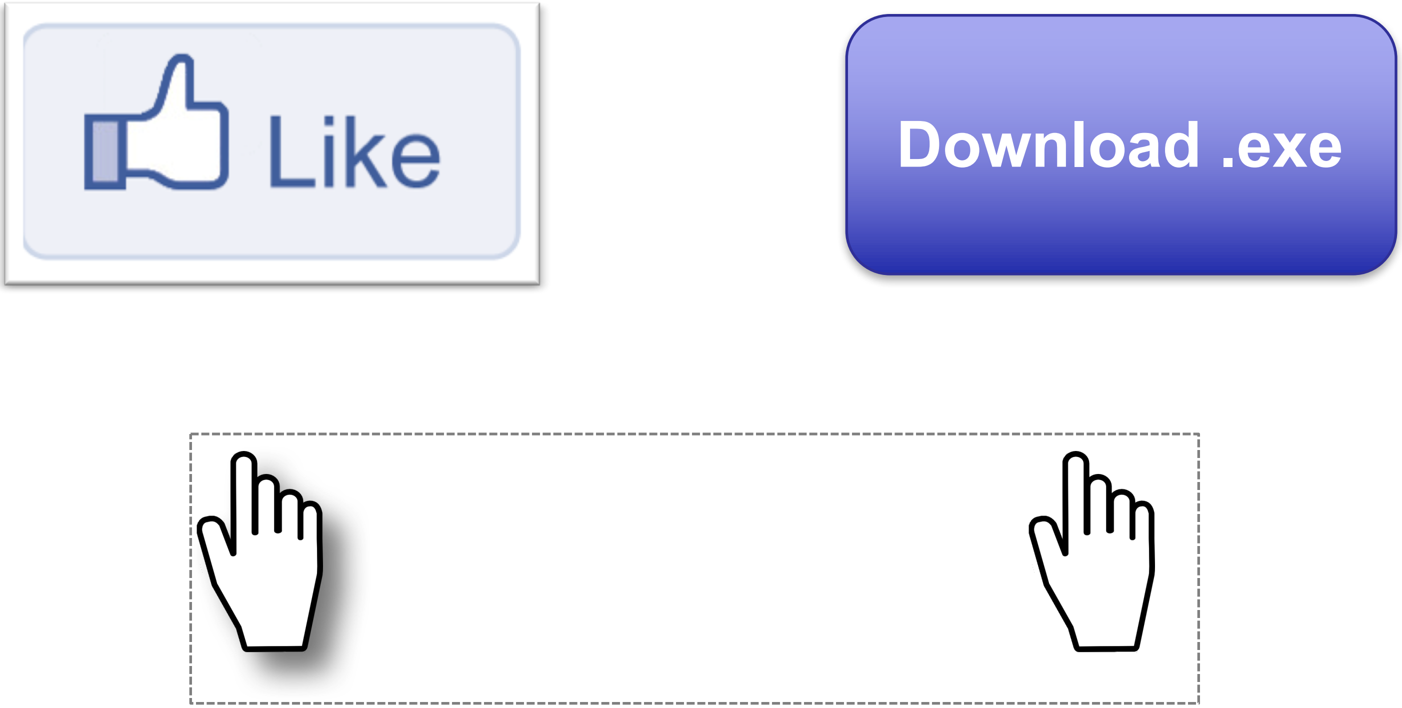


Fake cursor, but more visible

Real cursor

Compromise visual integrity – pointer: cursorjacking

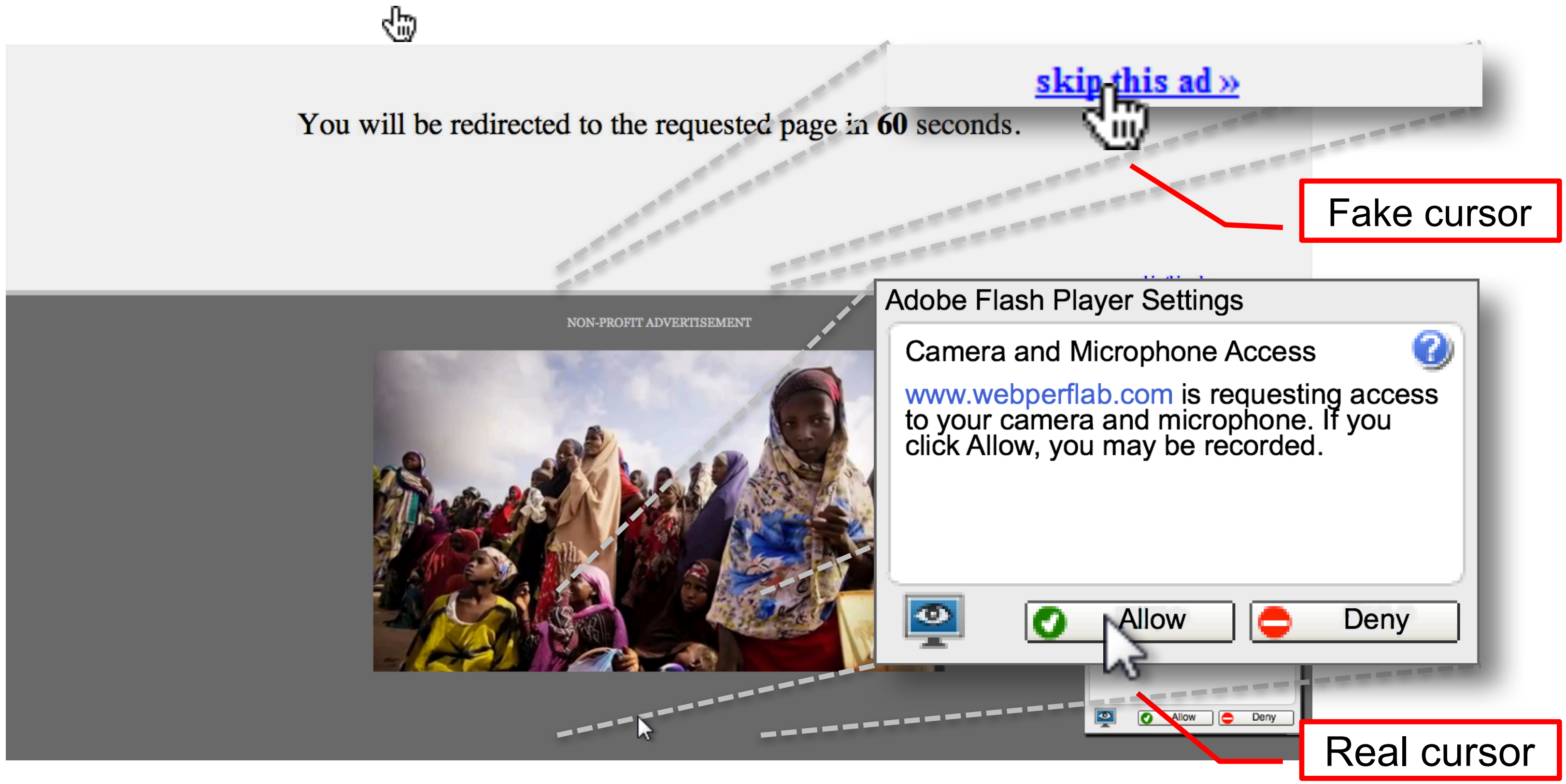
Cursorjacking deceives a user by using a custom cursor image, where the pointer was displayed with an offset



Fake, but more visible

real

Clickjacking to Access the User’s Webcam



skip this ad »

You will be redirected to the requested page in **60** seconds.

NON-PROFIT ADVERTISEMENT

Adobe Flash Player Settings

Camera and Microphone Access

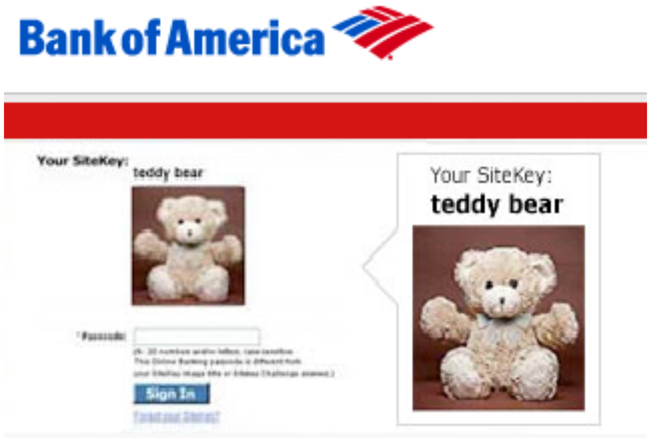
www.webperflab.com is requesting access to your camera and microphone. If you click Allow, you may be recorded.

Fake cursor

Real cursor

Defeating sitekeys

- Some sites use/used a secret image to identify site to user (e.g., Bank of America)
  - only good site should know the secret image
  - user should check that they receive the correct image



Invented by Berkeley grad student!

- What is it aimed to protect against?
  - phishing attacks

Not really used much now, not considered effective mostly because users ignore these images and don't remember what the image was for each site

How can clickjacking subvert sitekeys?

- Phishing sites frame login page to get correct image to appear
- Overlay input box from outer frame at the same location as the password box for the inner frame
- User types password accessible to attacker now

How can we defend against clickjacking?

Discuss with a partner

Defenses

- User confirmation

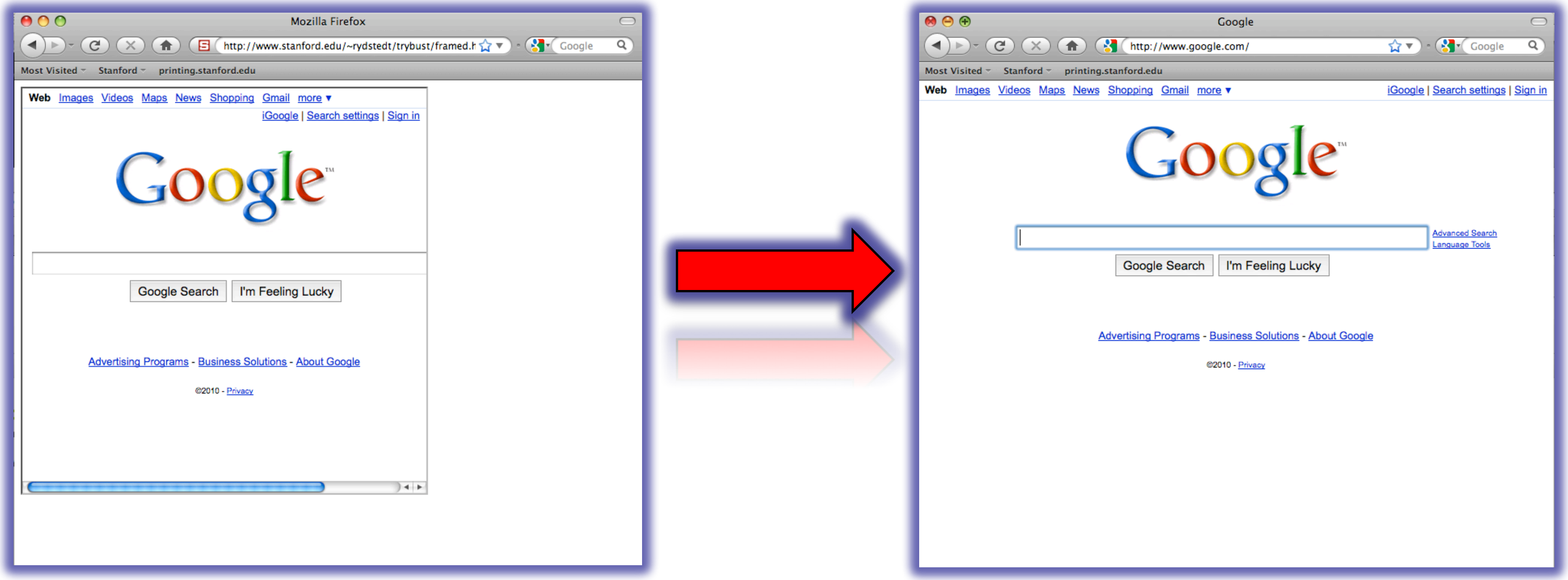
- Good site pops dialogue box with information on the action it is about to make and asks for user confirmation
- Degrades user experience

- UI randomization

- good site embeds dialogues at random locations so it is hard to overlay
- Difficult & unreliable (e.g. multi-click attacks)

Defense 3: Framebusting

Web site includes code on a page that prevents other pages from framing it


Mozilla Firefox
http://www.stanford.edu/~rydstedt/trybust/framed.h
Most Visited
Stanford
printing.stanford.edu
Web Images Videos Maps News Shopping Gmail more ▾
iGoogle | Search settings | Sign in
Google
Google Search
I'm Feeling Lucky
Advertising Programs - Business Solutions - About Google
©2010 - Privacy
Google
http://www.google.com/
Most Visited
Stanford
printing.stanford.edu
Web Images Videos Maps News Shopping Gmail more ▾
iGoogle | Search settings | Sign in
Google
Advanced Search
Language Tools
Google Search
I'm Feeling Lucky
Advertising Programs - Business Solutions - About Google
©2010 - Privacy

What is framebusting?

Framebusting code is often made up of

- a conditional statement and
- a counter action

Common method:

```
        if (top != self) {
                top.location = self.location;
        }
```

A Survey

Framebusting is very common at the Alexa Top 500 sites

[global traffic rank of a website]

Sites	Framebusting
Top 10	60%
Top 100	37%
Top 500	14%

credit: Gustav Rydstedt

Many framebusting methods

Conditional Statements
if (top != self)
if (top.location != self.location)
if (top.location != location)
if (parent.frames.length > 0)
if (window != top)
if (window.top !== window.self)
if (window.self != window.top)
if (parent && parent != window)
if (parent && parent.frames && parent.frames.length>0)
if((self.parent && !(self.parent===self)) && (self.parent.frames.length!=0))

Many framebusting methods

Counter-Action Statements
top.location = self.location
top.location.href = document.location.href
top.location.href = self.location.href
top.location.replace(self.location)
top.location.href = window.location.href
top.location.replace(document.location)
top.location.href = window.location.href
top.location.href = "URL"
document.write(’’)
top.location = location
top.location.replace(document.location)
top.location.replace(’URL’)
top.location.href = document.location

Most current framebusting can be defeated

Easy bugs

Goal: bank.com wants only bank.com’s sites to frame it

Bank runs this code to protect itself:

```
if (top.location != location) {
    if (document.referrer &&
        document.referrer.indexOf(”bank.com") == -1)
        {
                top.location.replace(document.location.href);
        }
  }
```

Problem: http://badguy.com?q=bank.com

Abusing the XSS filter

IE8 reflective XSS filters:

On a browser request containing script:

http://www.victim.com?var=<script> alert('xss') … </script>

Server responds

Brower checks

If <script> alert('xss'); appears in rendered page, the IE8 filter will replace it with <sc#pt> alert('xss') … </sc#pt>

How can attacker abuse this?

Abusing the XSS filter

Attacker figures out the framebusting code of victim site

(easy to do, just go to victim site in attacker’s browser and view the source code)

```
<script> if(top.location != self.location) //framebust </script>
```

Framing page does:

```
<iframe src=“http://www.victim.com?var=<script> if (top … “  >
```

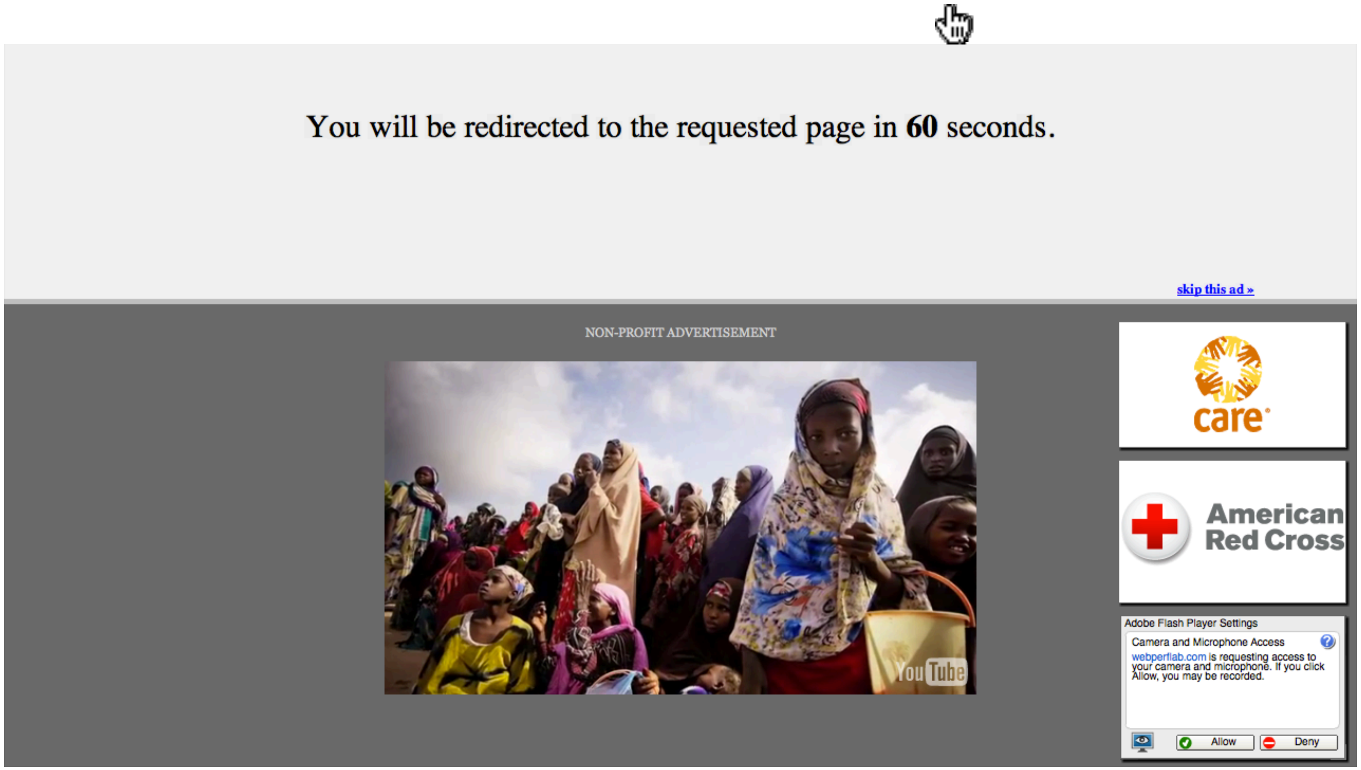
XSS filter modifies framebusting script to:

```
<sc#pt> if(top.location != self.location)
```

XSS filter disables legitimate framebusting code!!

Defense: Ensuring visual integrity of pointer

- Remove cursor customization
  - Attack success: 43% -> 16%



You will be redirected to the requested page in **60** seconds.

skip this ad »

NON-PROFIT ADVERTISEMENT

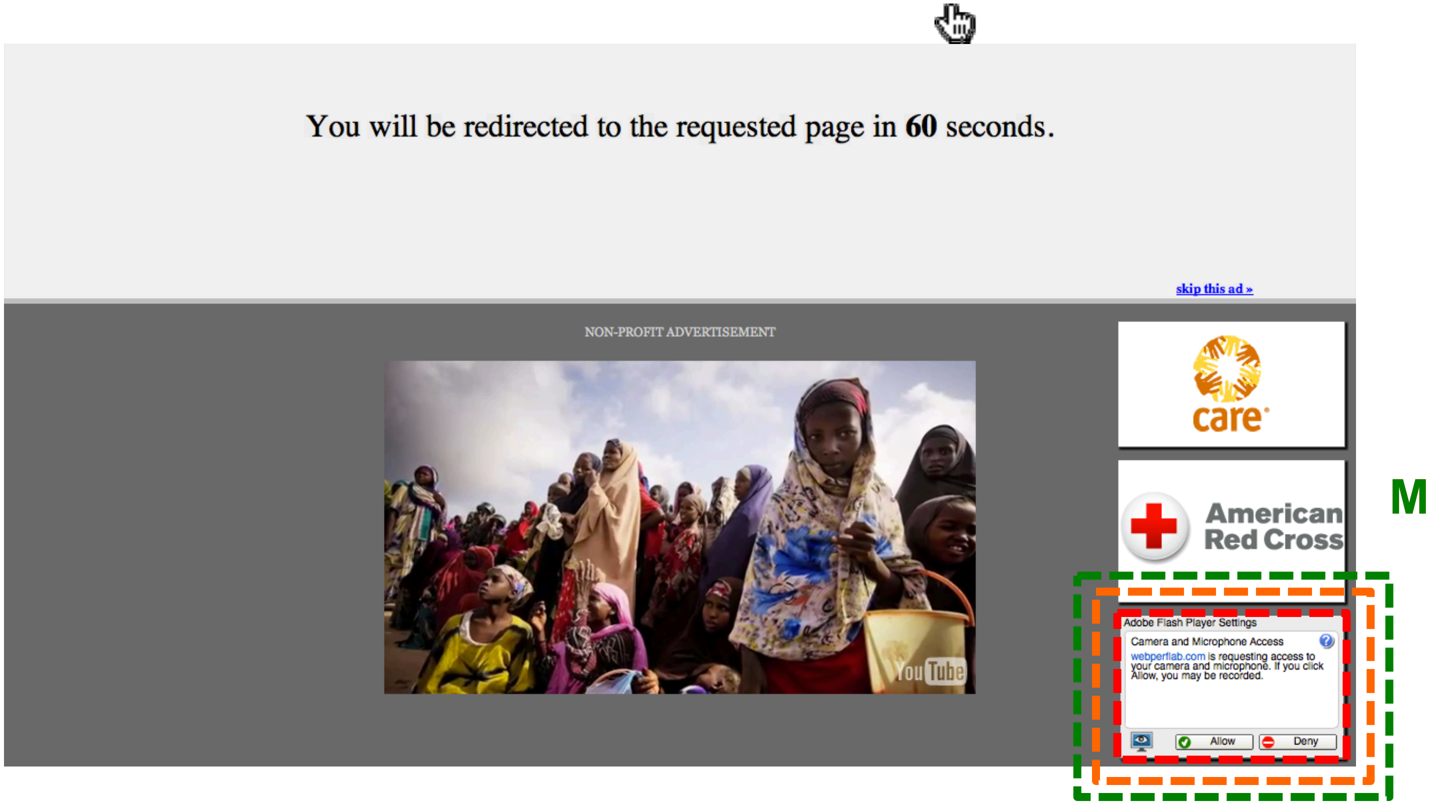
Adobe Flash Player Settings

Camera and Microphone Access

webperflab.com is requesting access to your camera and microphone. If you click Allow, you may be recorded.

Ensuring visual integrity of pointer

- Freeze screen outside of the target display area when the real pointer enters the target
  - Attack success: 43% -> 15%
  - Attack success (margin=10px): 12%
  - Attack success (margin=20px): 4% (baseline:5%)



You will be redirected to the requested page in **60** seconds.

Adobe Flash Player Settings

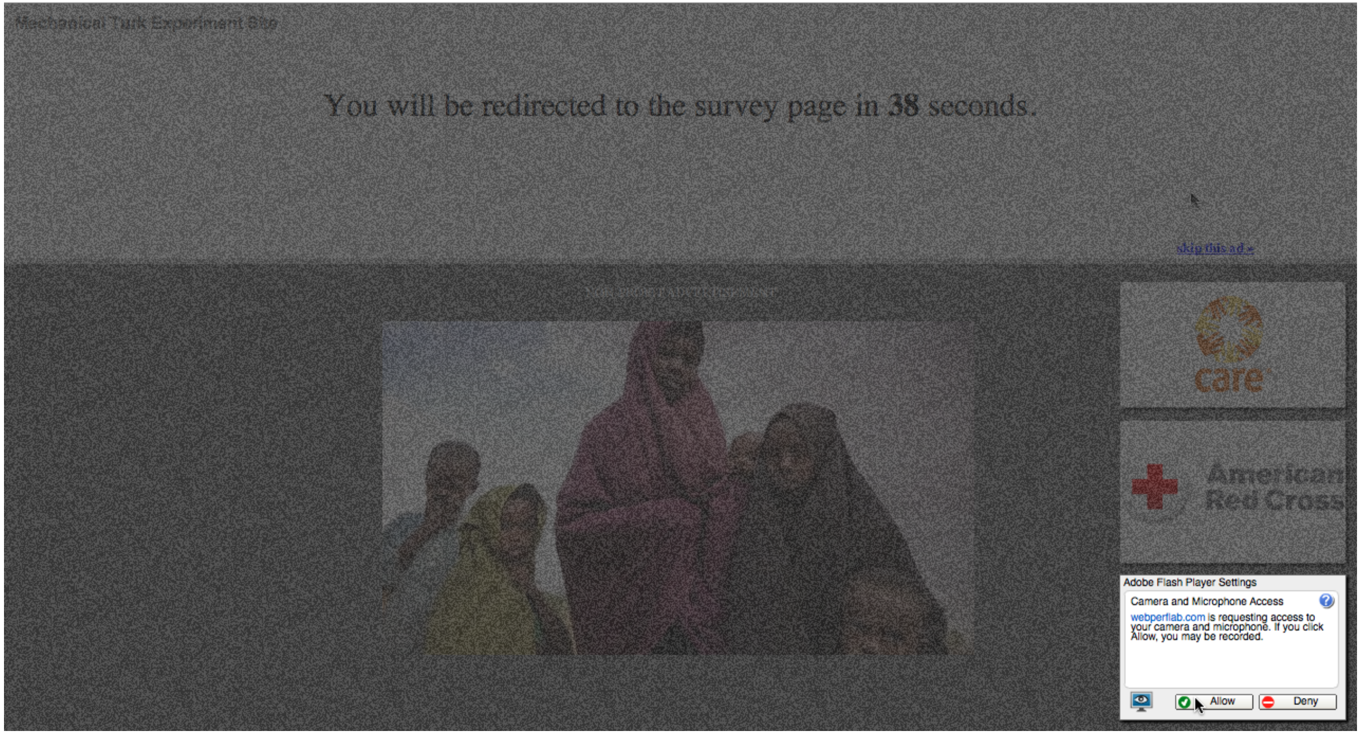
Camera and Microphone Access

webperflab.com is requesting access to your camera and microphone. If you click Allow, you may be recorded.

Margin=20px

Ensuring visual integrity of pointer

- Lightbox effect around target on pointer entry
  - Attack success (Freezing + lightbox): 2%



Mechanical Turk Experiment Site

You will be redirected to the survey page in **38** seconds.

skip this ad »

Adobe Flash Player Settings

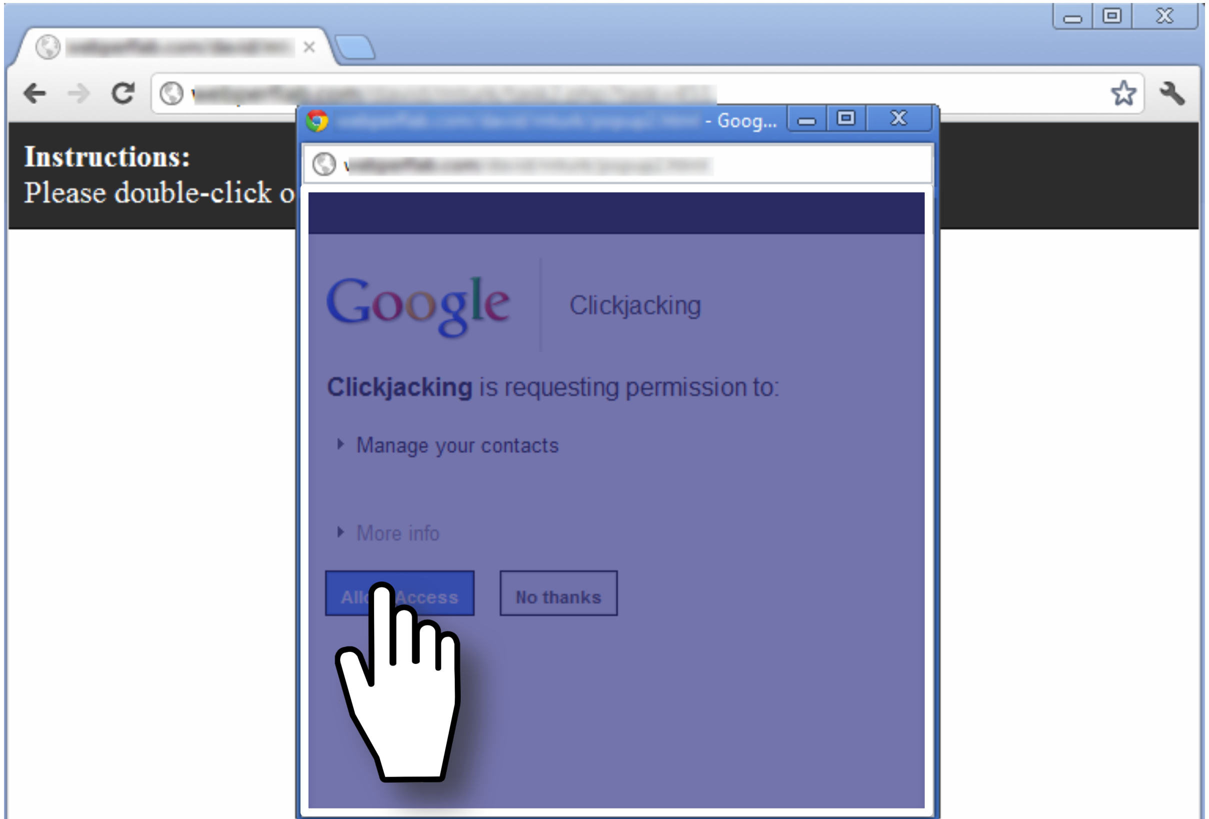
Camera and Microphone Access

webperflab.com is requesting access to your camera and microphone. If you click Allow, you may be recorded.

How about a temporal integrity attack example?

Enforcing temporal integrity

- UI delay: after visual changes on target or pointer, invalidate clicks for X ms
  - Attack success (delay=250ms): 47% -> 2% (2/91)
  - Attack success (delay=500ms): 1% (1/89)

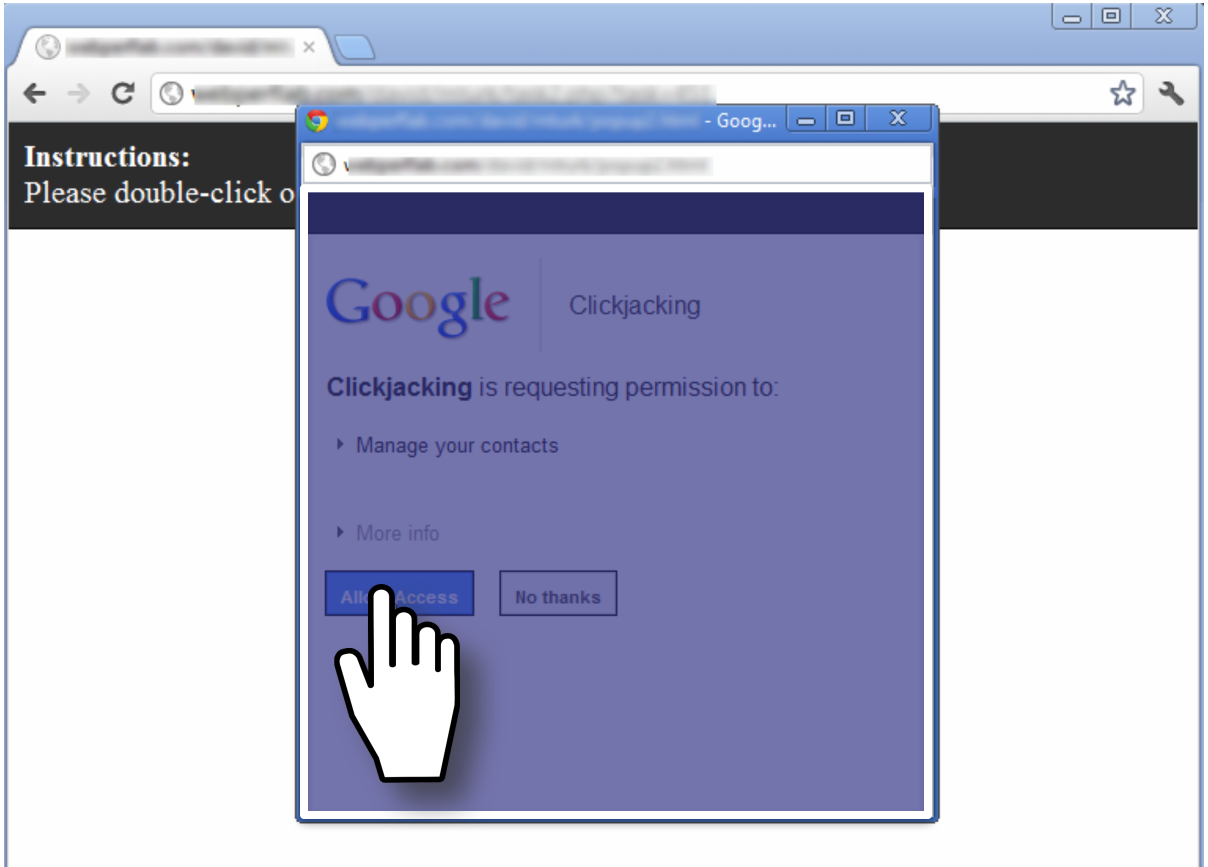


Instructions:
Please double-click o

Clickjacking is requesting permission to:

Enforcing temporal integrity

- Pointer re-entry: after visual changes on target, invalidate clicks until pointer re-enters target
  - Attack success: 0% (0/88)



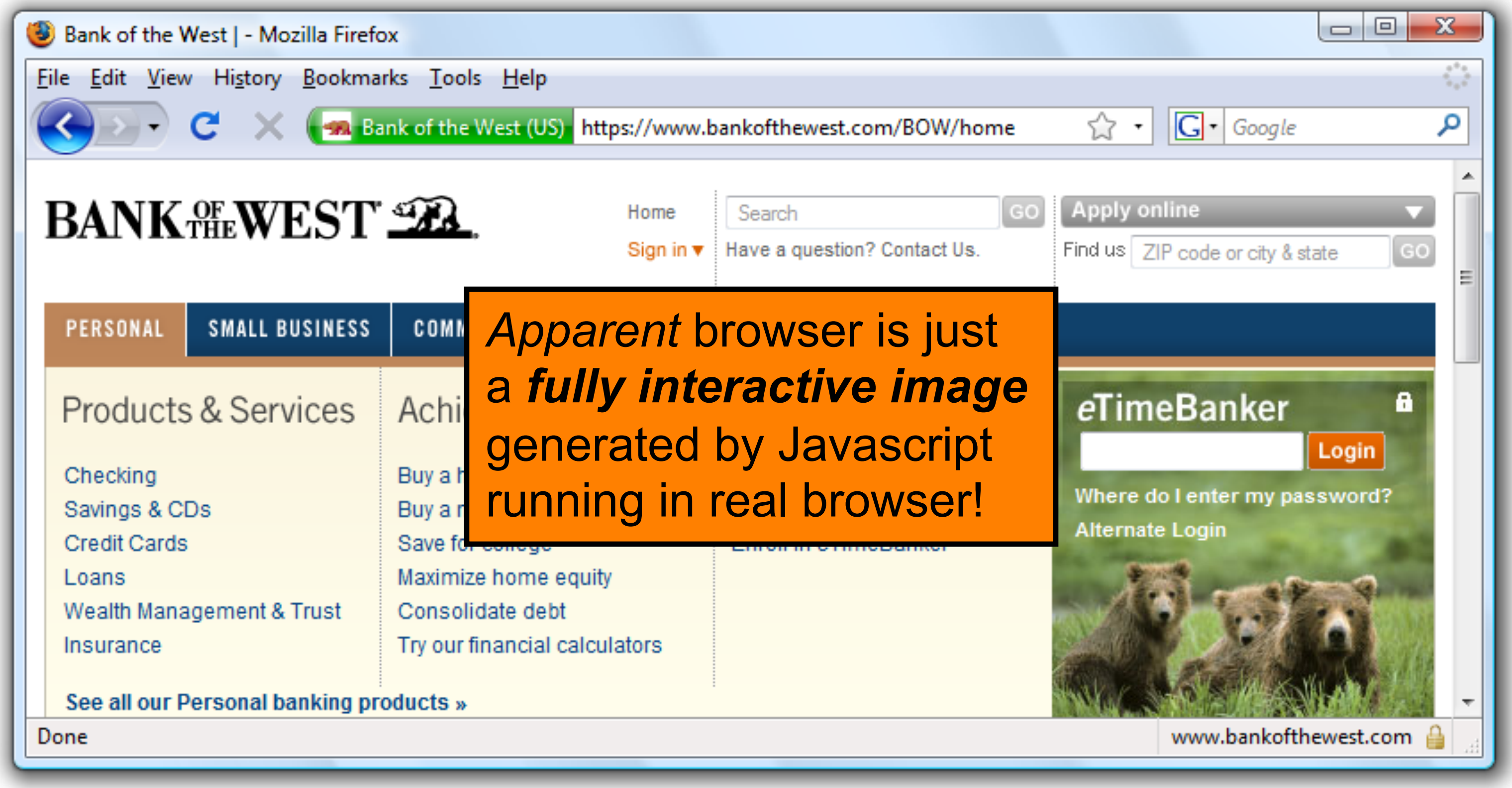
Instructions:
Please double-click o

Clickjacking is requesting permission to:

Other Forms of UI Sneakiness

- Users might find themselves living in *The Matrix …*

“Browser in Browser”

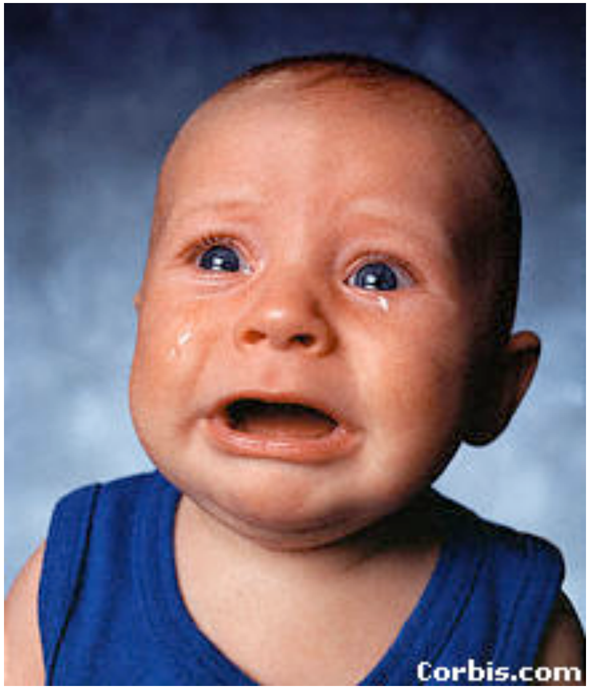


Apparent browser is just a ***fully interactive image*** generated by Javascript running in real browser!

Discussion

- So, how do these lessons apply to desktop applications?
- Compare the security model for desktop apps:
  - Are desktop apps safer against these attacks?
  - Are desktop apps riskier against these attacks?

Is there any hope?



Other defense: X-Frames-Options (IE8, Safari, FF3.7)

- Web server attaches HTTP header to response
  - Two possible values: DENY and SAMEORIGIN
    - DENY: browser will not render page in framed context
    - SAMEORIGIN: browser will only render if top frame is same origin as page giving directive
- Good defense … but poor adoption by sites (4 of top 10,000)
- Coarse policies: no whitelisting of partner sites, which should be allowed to frame our site

Summary

- Clickjacking is an attack on our perception of a page based on the UI

- Framebusting is tricky to get right
  - All currently deployed code can be defeated

- Use X-Frame-Options

Tracking on the Web

What does a site learn about you when you visit them?

`Discuss with your neighbor`

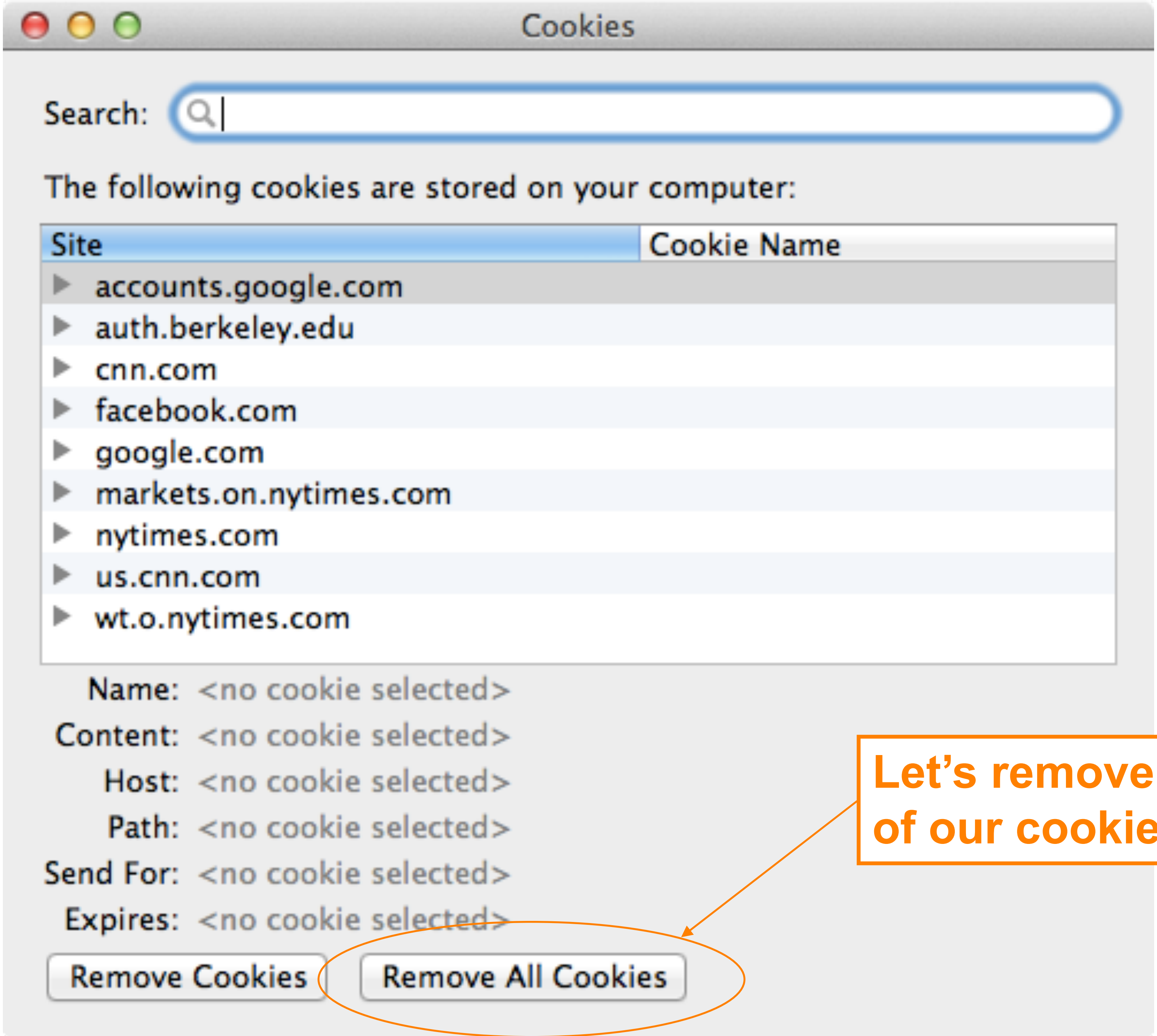
The sites you visit learn:

- The URLs you’re interested in
  - Google/Bing also learns *what you’re searching for*
- Your IP address
  - Thus, your service provider & geo-location
  - Can often link you to other activity including at other sites
- Your browser’s capabilities, which OS you run, which language you prefer
- Which URL you looked at that took you there
  - Via the HTTP “`Referer`” header

`They also learn cookies!`

They also learn cookies

Why is that harmful?



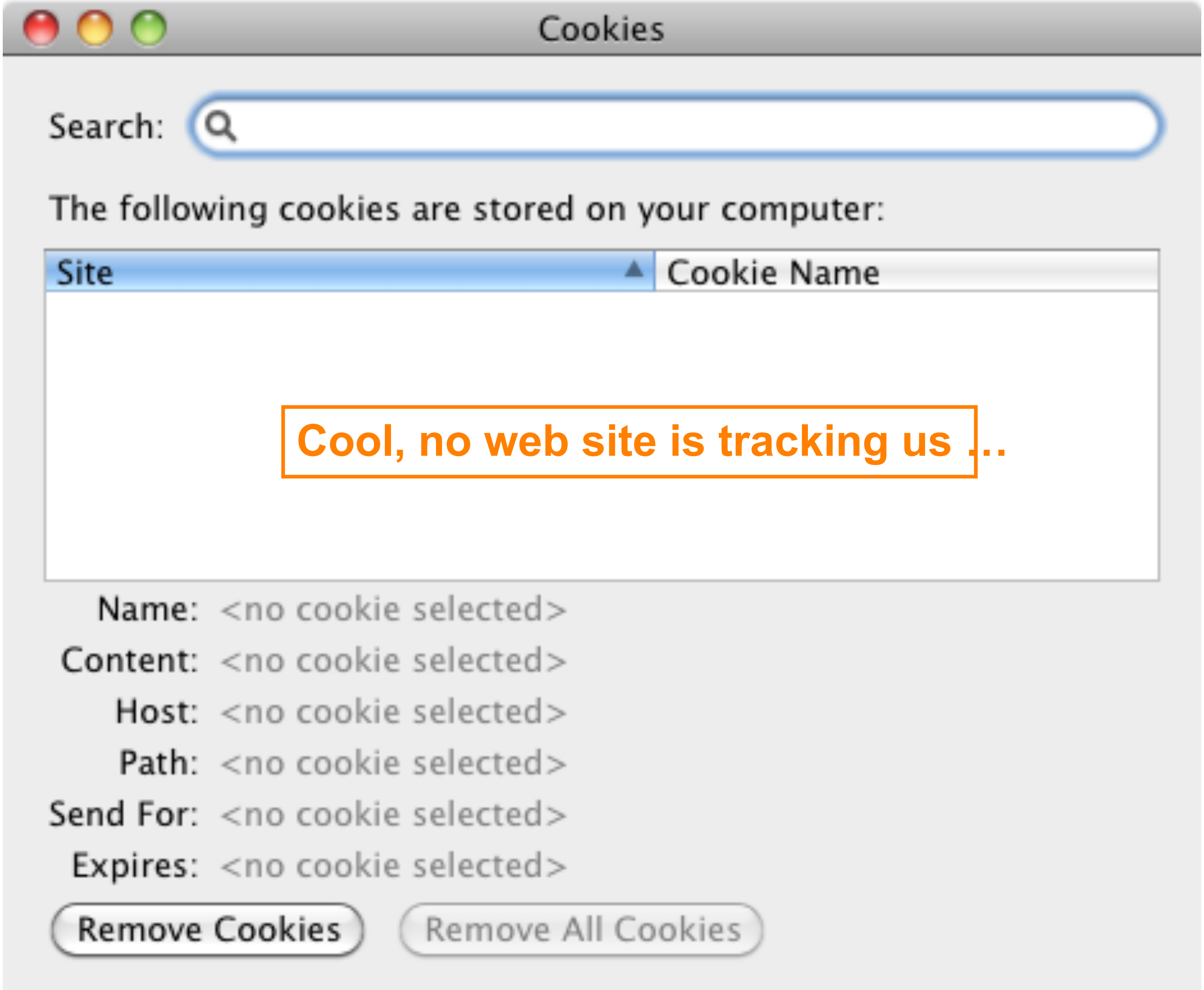
Search:

The following cookies are stored on your computer:

Site	Cookie Name
▶ accounts.google.com	
▶ auth.berkeley.edu	
▶ cnn.com	
▶ facebook.com	
▶ google.com	
▶ markets.on.nytimes.com	
▶ nytimes.com	
▶ us.cnn.com	
▶ wt.o.nytimes.com	

Name: <no cookie selected>
Content: <no cookie selected>
Host: <no cookie selected>
Path: <no cookie selected>
Send For: <no cookie selected>
Expires: <no cookie selected>

Let’s remove all of our cookies



The following cookies are stored on your computer:

Site	Cookie Name

Name: <no cookie selected>

Content: <no cookie selected>

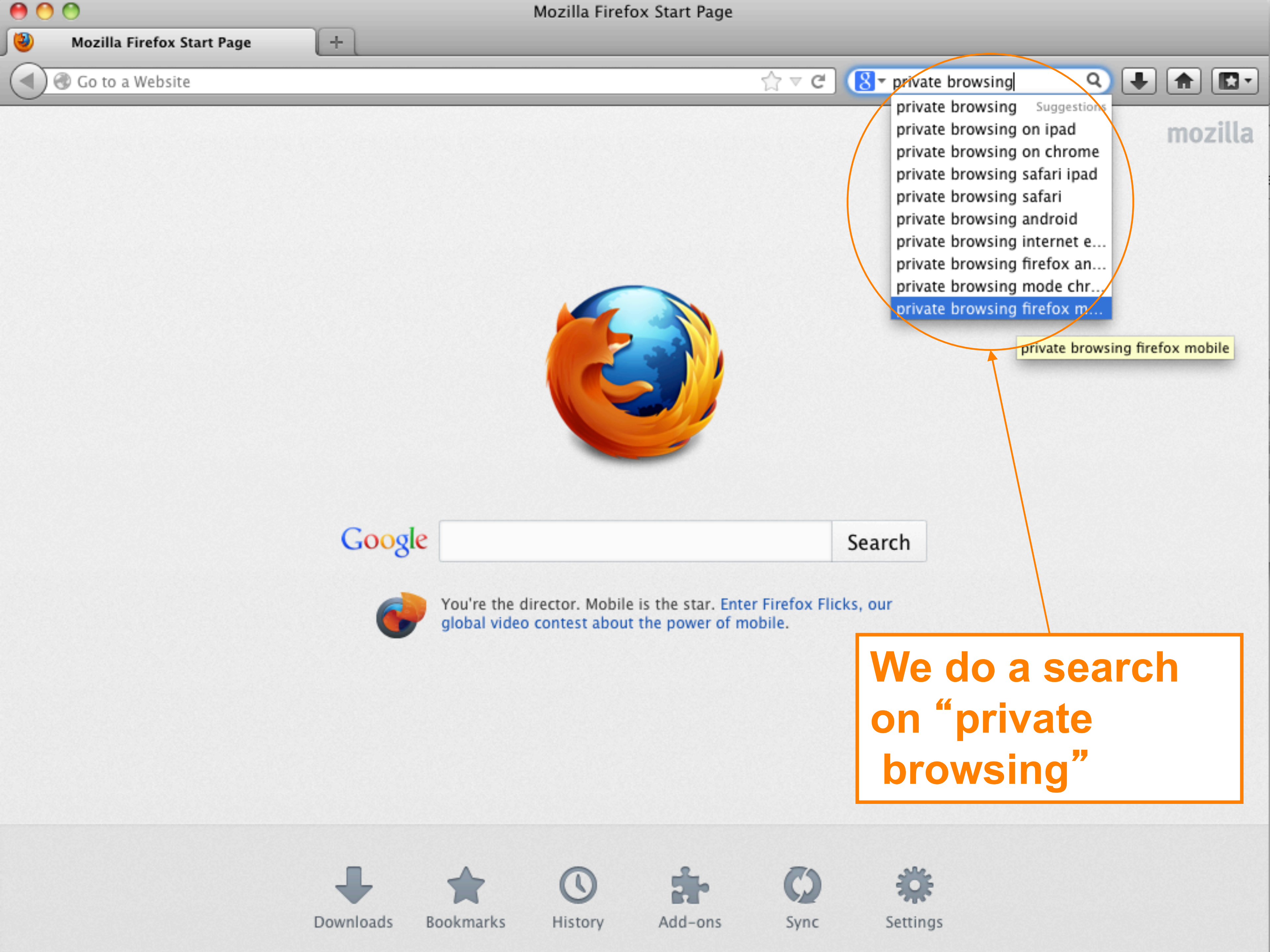
Host: <no cookie selected>

Path: <no cookie selected>

Send For: <no cookie selected>

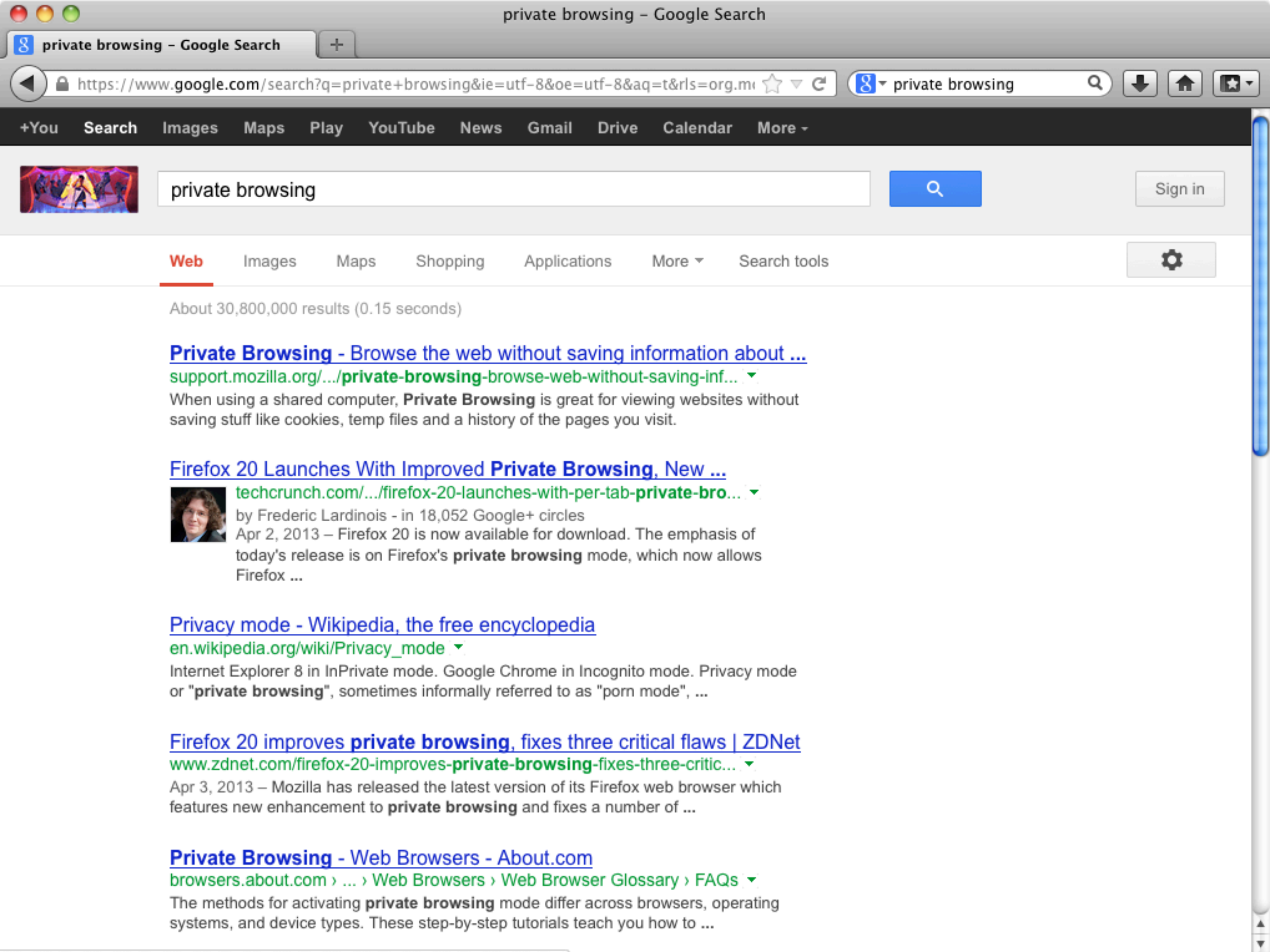
Expires: <no cookie selected>

Cool, no web site is tracking us …


Mozilla Firefox Start Page
Mozilla Firefox Start Page
Go to a Website
private browsing
private browsing Suggestions
private browsing on ipad
private browsing on chrome
private browsing safari ipad
private browsing safari
private browsing android
private browsing internet e…
private browsing firefox an…
private browsing mode chr…
private browsing firefox m…
private browsing firefox mobile
mozilla
Google
Search
Downloads
Bookmarks
History
Add-ons
Sync
Settings

You're the director. Mobile is the star. Enter Firefox Flicks, our global video contest about the power of mobile.

We do a search on “private browsing”



private browsing - Google Search
private browsing - Google Search
https://www.google.com/search?q=private+browsing&ie=utf-8&oe=utf-8&aq=t&rls=org.m
private browsing
+You
Search
Images
Maps
Play
YouTube
News
Gmail
Drive
Calendar
More
Sign in
Web
Images
Maps
Shopping
Applications
More
Search tools

private browsing

About 30,800,000 results (0.15 seconds)

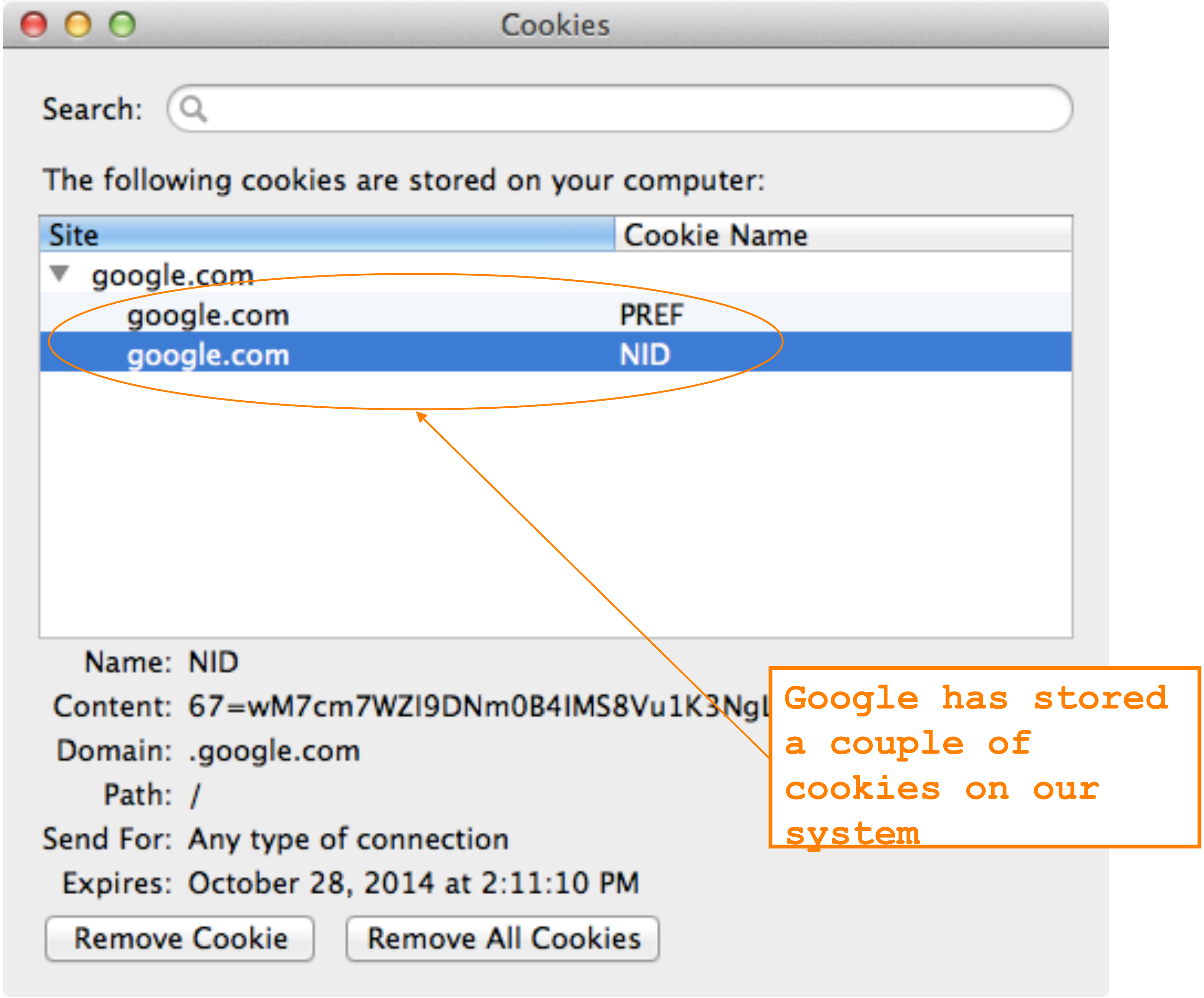
Private Browsing - Browse the web without saving information about ...
support.mozilla.org/.../**private-browsing**-browse-web-without-saving-inf...
When using a shared computer, **Private Browsing** is great for viewing websites without saving stuff like cookies, temp files and a history of the pages you visit.

Firefox 20 Launches With Improved **Private Browsing**, New ...
techcrunch.com/.../firefox-20-launches-with-per-tab-**private-bro**...
by Frederic Lardinois - in 18,052 Google+ circles
Apr 2, 2013 – Firefox 20 is now available for download. The emphasis of today's release is on Firefox's **private browsing** mode, which now allows Firefox ...

Privacy mode - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Privacy_mode
Internet Explorer 8 in InPrivate mode. Google Chrome in Incognito mode. Privacy mode or "**private browsing**", sometimes informally referred to as "porn mode", ...

Firefox 20 improves **private browsing**, fixes three critical flaws | ZDNet
www.zdnet.com/firefox-20-improves-**private-browsing**-fixes-three-critic...
Apr 3, 2013 – Mozilla has released the latest version of its Firefox web browser which features new enhancement to **private browsing** and fixes a number of ...

Private Browsing - Web Browsers - About.com
browsers.about.com › ... › Web Browsers › Web Browser Glossary › FAQs
The methods for activating **private browsing** mode differ across browsers, operating systems, and device types. These step-by-step tutorials teach you how to ...



The following cookies are stored on your computer:

Site	Cookie Name
▼ google.com	
google.com	PREF
google.com	NID

Name: NID

Content: 67=wM7cm7WZI9DNm0B4IMS8Vu1K3NgL

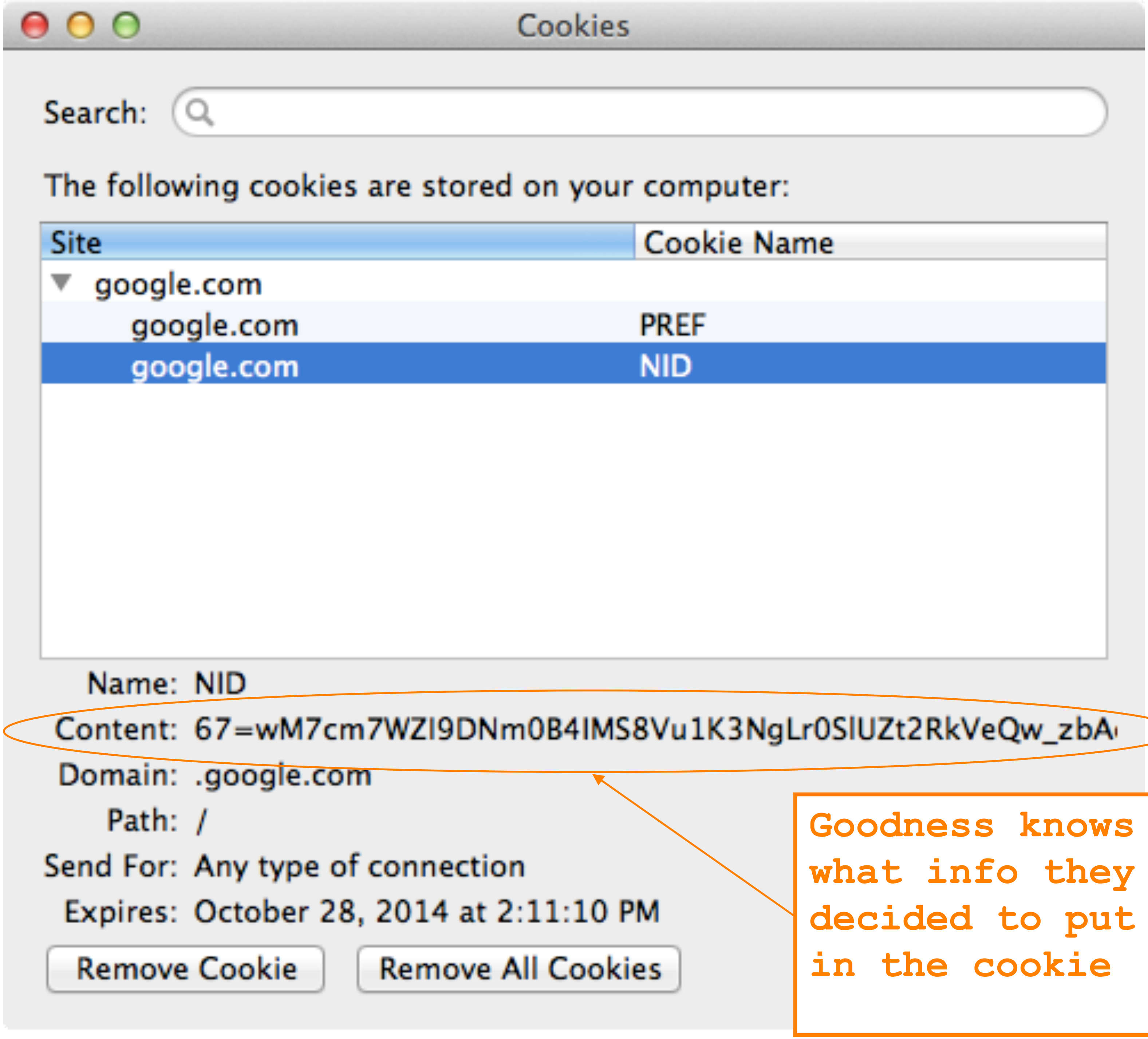
Domain: .google.com

Path: /

Send For: Any type of connection

Expires: October 28, 2014 at 2:11:10 PM

Google has stored a couple of cookies on our system



The following cookies are stored on your computer:

Site	Cookie Name
▼ google.com	
google.com	PREF
google.com	NID

Name: NID

Content: 67=wM7cm7WZI9DNm0B4IMS8Vu1K3NgLr0SlUZt2RkVeQw_zbA

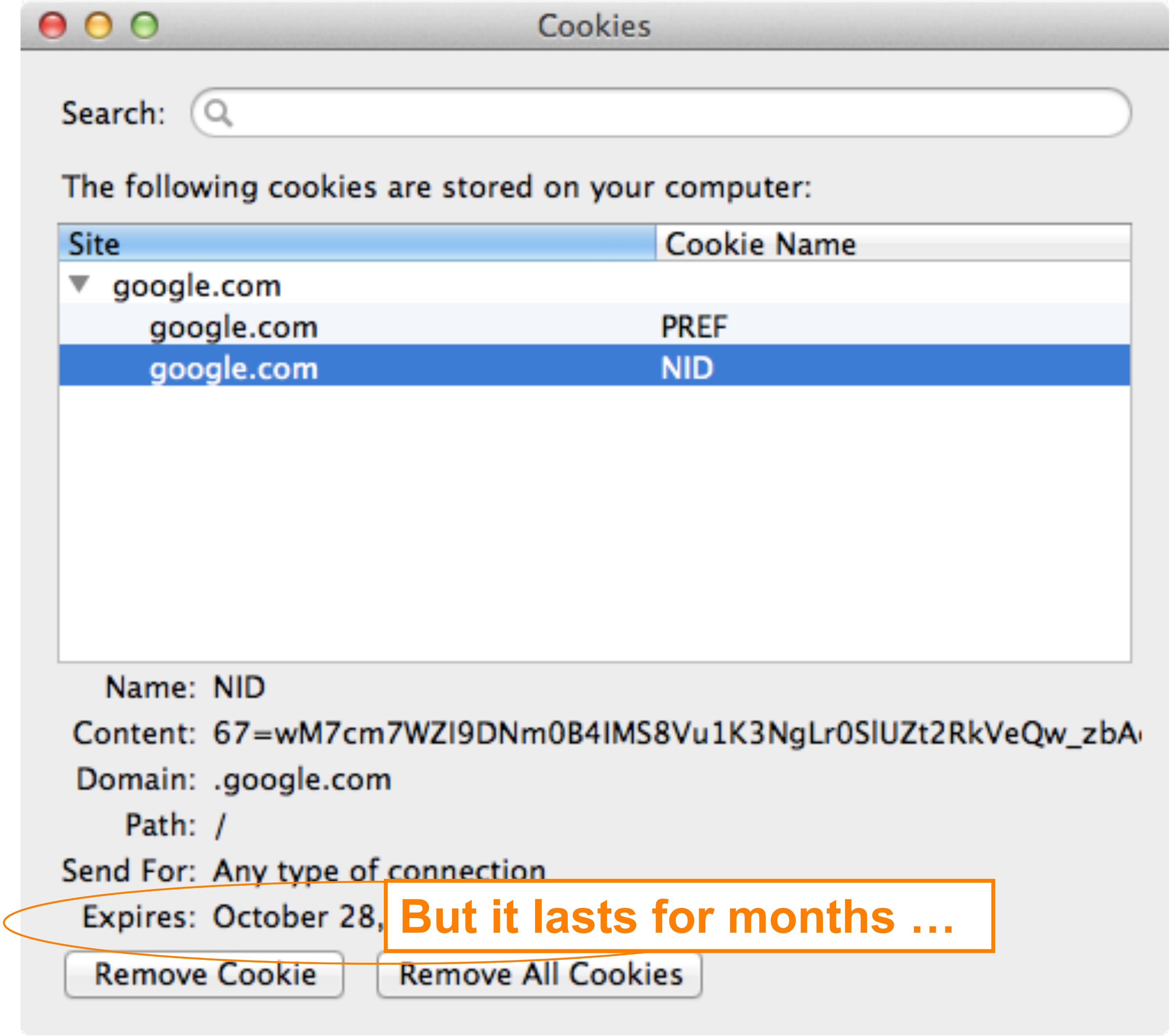
Domain: .google.com

Path: /

Send For: Any type of connection

Expires: October 28, 2014 at 2:11:10 PM

Goodness knows what info they decided to put in the cookie



The following cookies are stored on your computer:

Site	Cookie Name
▼ google.com	
google.com	PREF
google.com	NID

Name: NID

Content: 67=wM7cm7WZI9DNm0B4IMS8Vu1K3NgLr0SlUZt2RkVeQw_zbA

Domain: .google.com

Path: /

Send For: Any type of connection

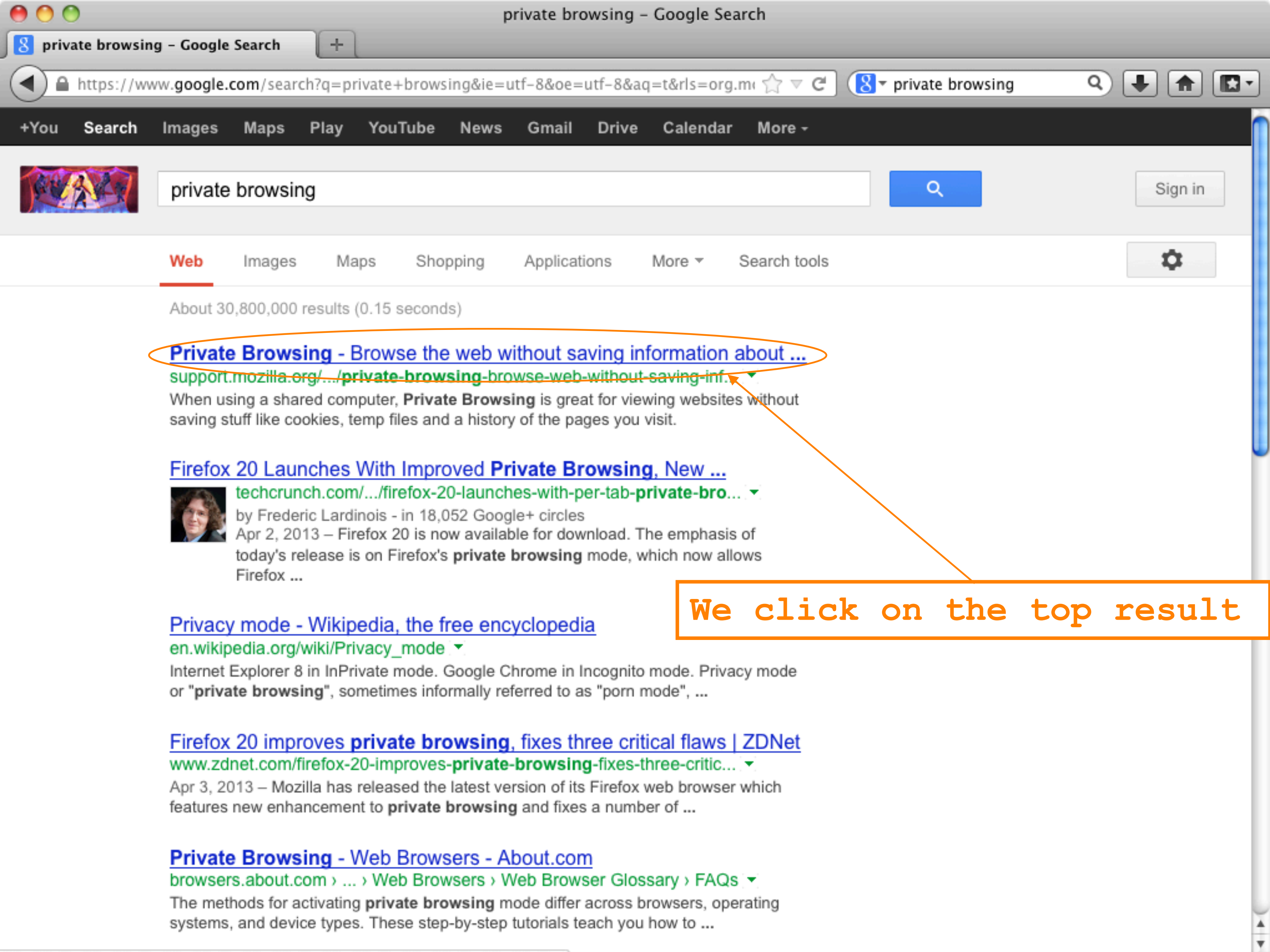
Expires: October 28,

But it lasts for months …

Private browsing

You can turn on a mode called private browsing on your browser

What is this?
Does it protect you against tracking?



About 30,800,000 results (0.15 seconds)

Private Browsing - Browse the web without saving information about ...
support.mozilla.org/.../**private-browsing**-browse-web-without-saving-inf...
When using a shared computer, **Private Browsing** is great for viewing websites without saving stuff like cookies, temp files and a history of the pages you visit.

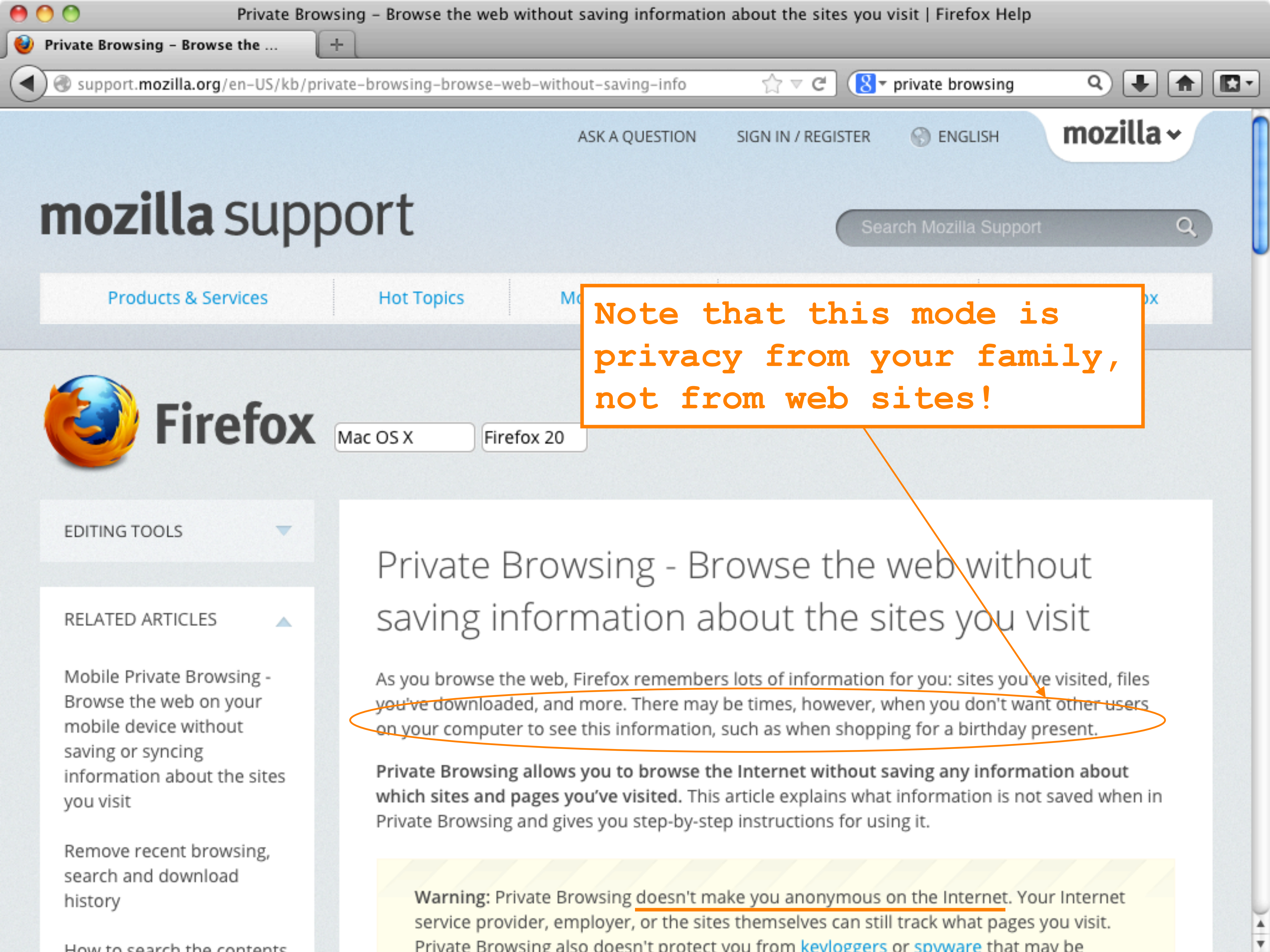
Firefox 20 Launches With Improved **Private Browsing**, New ...
techcrunch.com/.../firefox-20-launches-with-per-tab-**private-bro**...
by Frederic Lardinois - in 18,052 Google+ circles
Apr 2, 2013 – Firefox 20 is now available for download. The emphasis of today's release is on Firefox's **private browsing** mode, which now allows Firefox ...

Privacy mode - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Privacy_mode
Internet Explorer 8 in InPrivate mode. Google Chrome in Incognito mode. Privacy mode or "**private browsing**", sometimes informally referred to as "porn mode", ...

Firefox 20 improves **private browsing**, fixes three critical flaws | ZDNet
www.zdnet.com/firefox-20-improves-**private-browsing**-fixes-three-critic...
Apr 3, 2013 – Mozilla has released the latest version of its Firefox web browser which features new enhancement to **private browsing** and fixes a number of ...

Private Browsing - Web Browsers - About.com
browsers.about.com › ... › Web Browsers › Web Browser Glossary › FAQs
The methods for activating **private browsing** mode differ across browsers, operating systems, and device types. These step-by-step tutorials teach you how to ...

We click on the top result


Private Browsing – Browse the web without saving information about the sites you visit | Firefox Help
Private Browsing – Browse the ...
support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info
private browsing
ASK A QUESTION
SIGN IN / REGISTER
ENGLISH
mozilla
mozilla support
Search Mozilla Support
Products & Services
Hot Topics
Firefox
Mac OS X
Firefox 20
EDITING TOOLS
RELATED ARTICLES

Note that this mode is privacy from your family, not from web sites!

Mobile Private Browsing - Browse the web on your mobile device without saving or syncing information about the sites you visit

Remove recent browsing, search and download history

How to search the contents

Private Browsing - Browse the web without saving information about the sites you visit

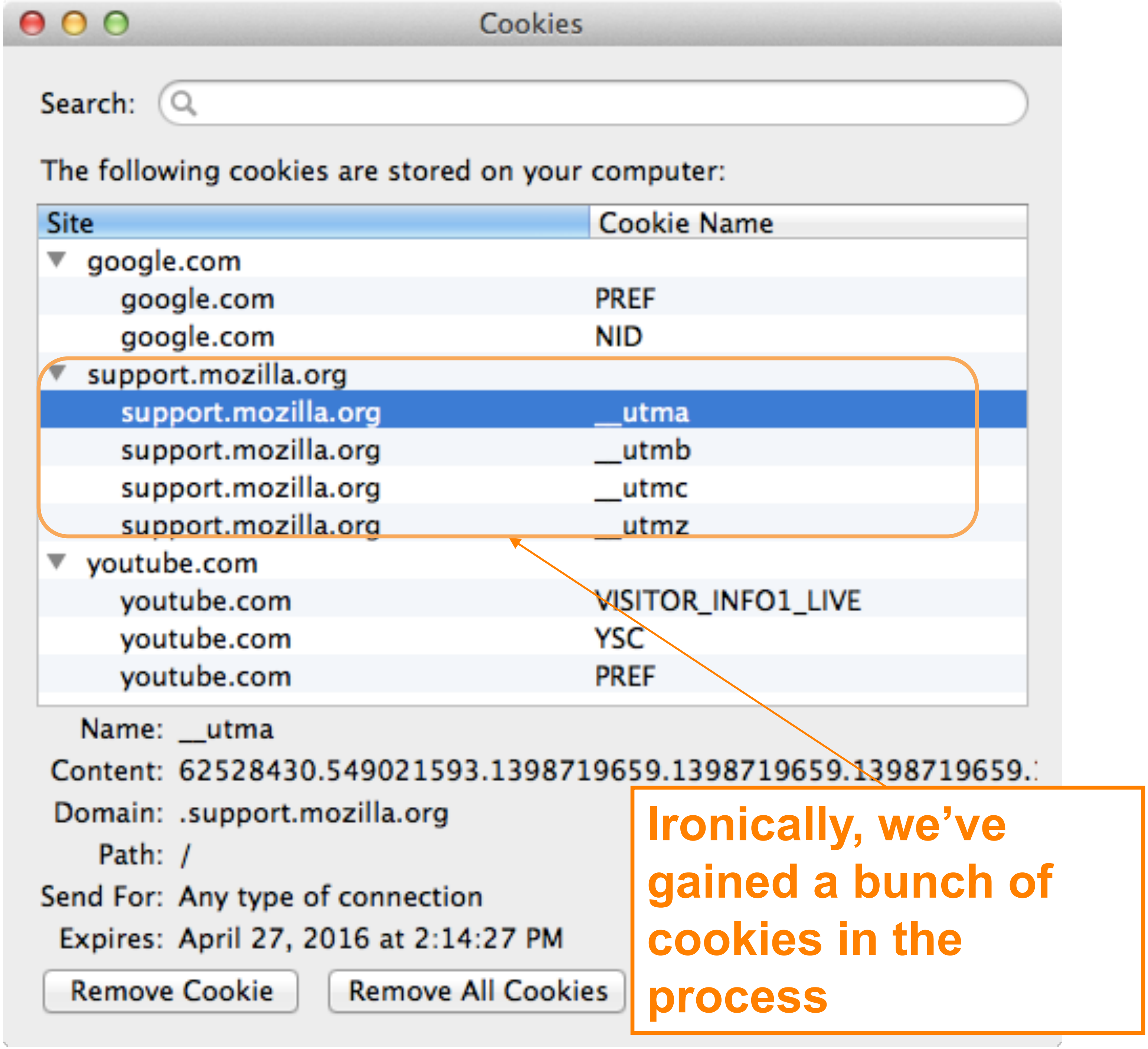
As you browse the web, Firefox remembers lots of information for you: sites you've visited, files you've downloaded, and more. There may be times, however, when you don't want other users on your computer to see this information, such as when shopping for a birthday present.

Private Browsing allows you to browse the Internet without saving any information about which sites and pages you've visited. This article explains what information is not saved when in Private Browsing and gives you step-by-step instructions for using it.

Warning: Private Browsing doesn't make you anonymous on the Internet. Your Internet service provider, employer, or the sites themselves can still track what pages you visit. Private Browsing also doesn't protect you from keyloggers or spyware that may be

Private browsing

- "Private Browsing allows you to browse the Internet without saving any information about which sites and pages you've visited."
  - deletes history of URL visits, passwords, cookies too
  - Private Browsing maintains cookies for as long as the private browsing window is open. Once you quit the browser, it gets deleted
    - So still tracked for a good while!



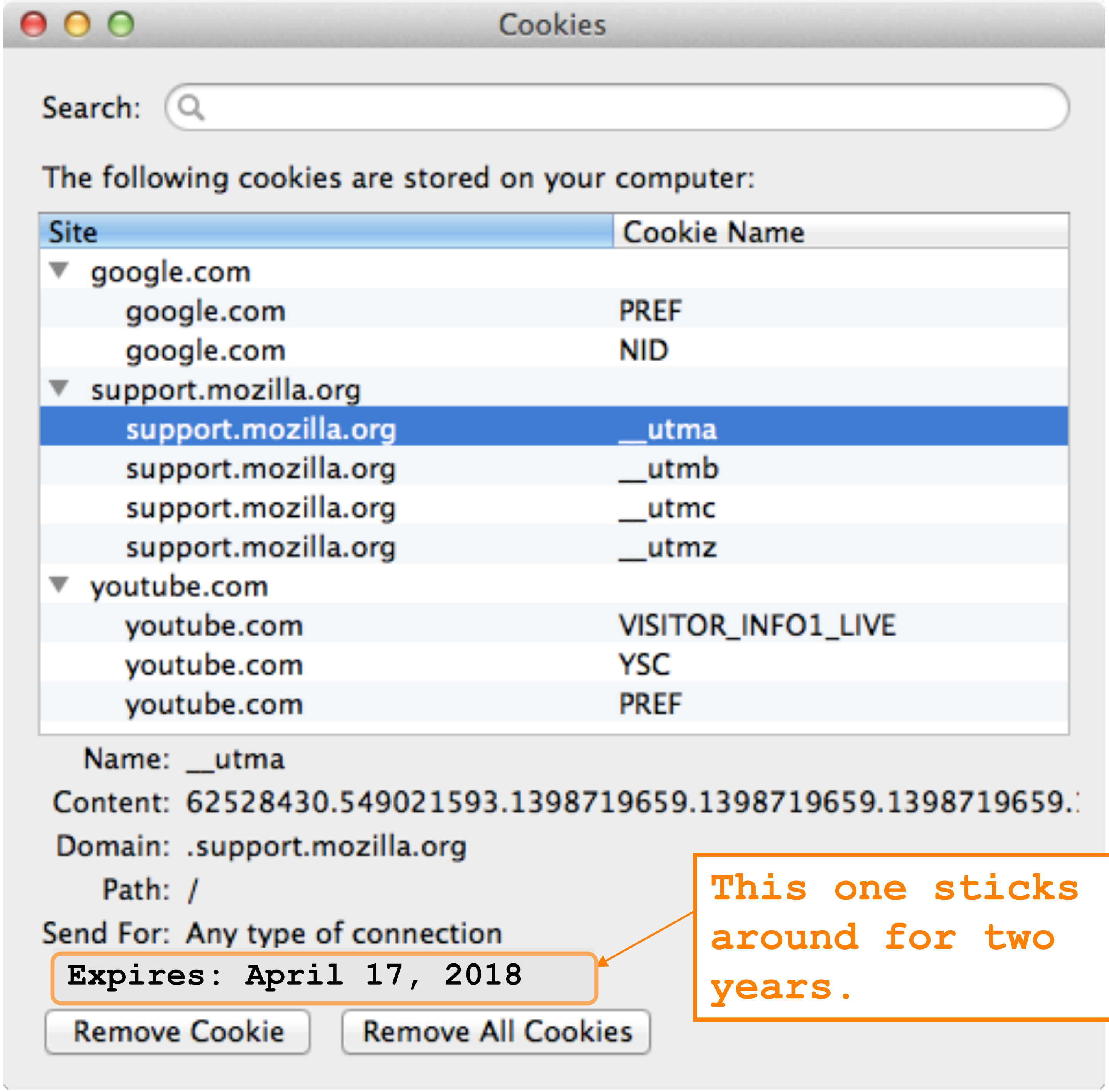
Search:

The following cookies are stored on your computer:

Site	Cookie Name
▼ google.com	
google.com	PREF
google.com	NID
▼ support.mozilla.org	
support.mozilla.org	__utma
support.mozilla.org	__utmb
support.mozilla.org	__utmc
support.mozilla.org	__utmz
▼ youtube.com	
youtube.com	VISITOR_INFO1_LIVE
youtube.com	YSC
youtube.com	PREF

Name: __utma
Content: 62528430.549021593.1398719659.1398719659.1398719659.
Domain: .support.mozilla.org
Path: /
Send For: Any type of connection
Expires: April 27, 2016 at 2:14:27 PM

Ironically, we've gained a bunch of cookies in the process

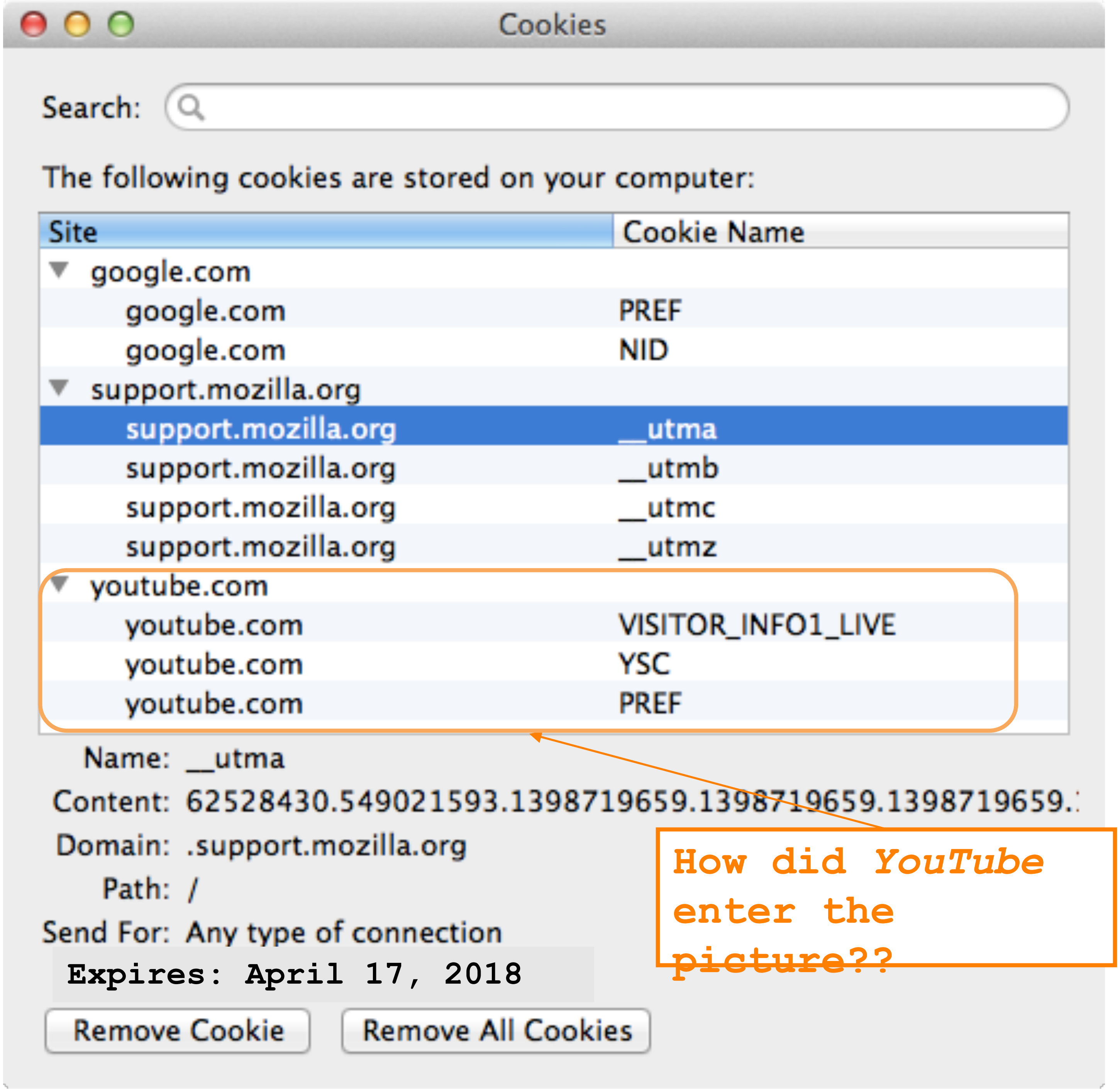


The following cookies are stored on your computer:

Site	Cookie Name
▼ google.com	
google.com	PREF
google.com	NID
▼ support.mozilla.org	
support.mozilla.org	__utma
support.mozilla.org	__utmb
support.mozilla.org	__utmc
support.mozilla.org	__utmz
▼ youtube.com	
youtube.com	VISITOR_INFO1_LIVE
youtube.com	YSC
youtube.com	PREF

Name: __utma
Content: 62528430.549021593.1398719659.1398719659.1398719659.
Domain: .support.mozilla.org
Path: /
Send For: Any type of connection
Expires: April 17, 2018

This one sticks around for two years.



Search:

The following cookies are stored on your computer:

Site	Cookie Name
google.com	
google.com	PREF
google.com	NID
support.mozilla.org	
support.mozilla.org	__utma
support.mozilla.org	__utmb
support.mozilla.org	__utmc
support.mozilla.org	__utmz
youtube.com	
youtube.com	VISITOR_INFO1_LIVE
youtube.com	YSC
youtube.com	PREF

Name: __utma

Content: 62528430.549021593.1398719659.1398719659.1398719659.

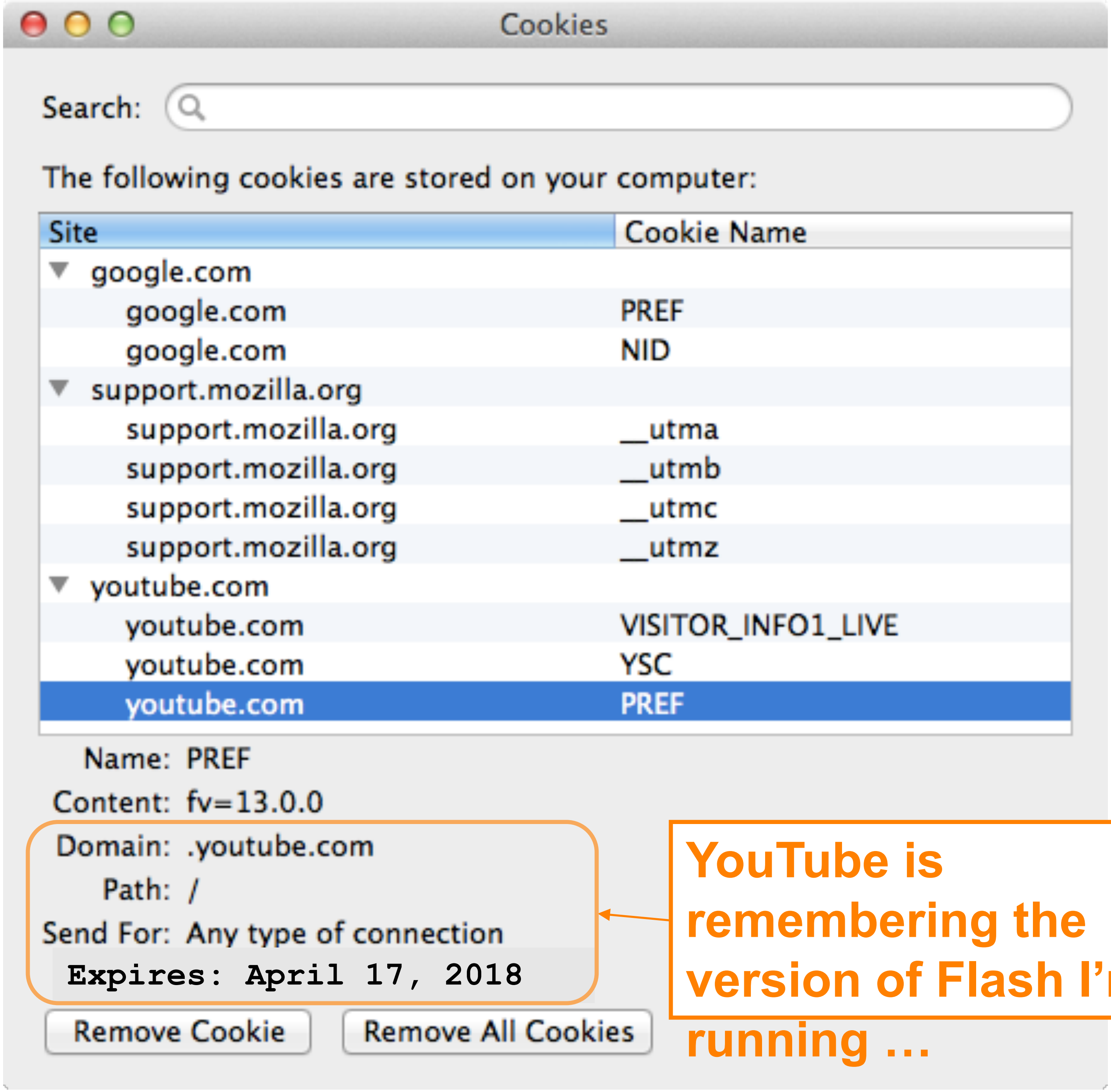
Domain: .support.mozilla.org

Path: /

Send For: Any type of connection

Expires: April 17, 2018

How did *YouTube* enter the picture??



The following cookies are stored on your computer:

Site	Cookie Name
▼ google.com	
google.com	PREF
google.com	NID
▼ support.mozilla.org	
support.mozilla.org	__utma
support.mozilla.org	__utmb
support.mozilla.org	__utmc
support.mozilla.org	__utmz
▼ youtube.com	
youtube.com	VISITOR_INFO1_LIVE
youtube.com	YSC
youtube.com	PREF

Name: PREF

Content: fv=13.0.0

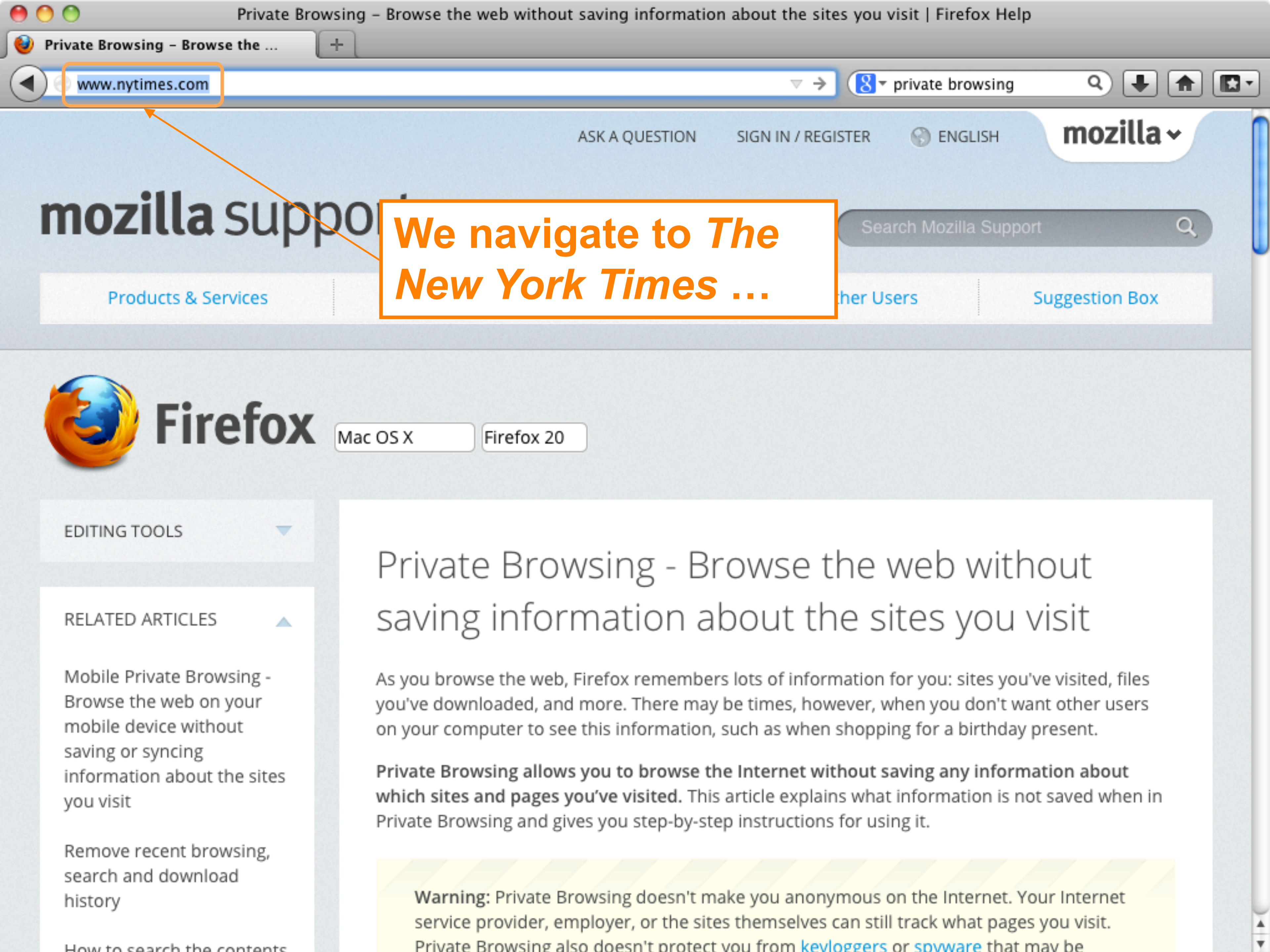
Domain: .youtube.com

Path: /

Send For: Any type of connection

Expires: April 17, 2018

YouTube is remembering the version of Flash I'm running …



We navigate to *The New York Times* …

Mobile Private Browsing - Browse the web on your mobile device without saving or syncing information about the sites you visit

Remove recent browsing, search and download history

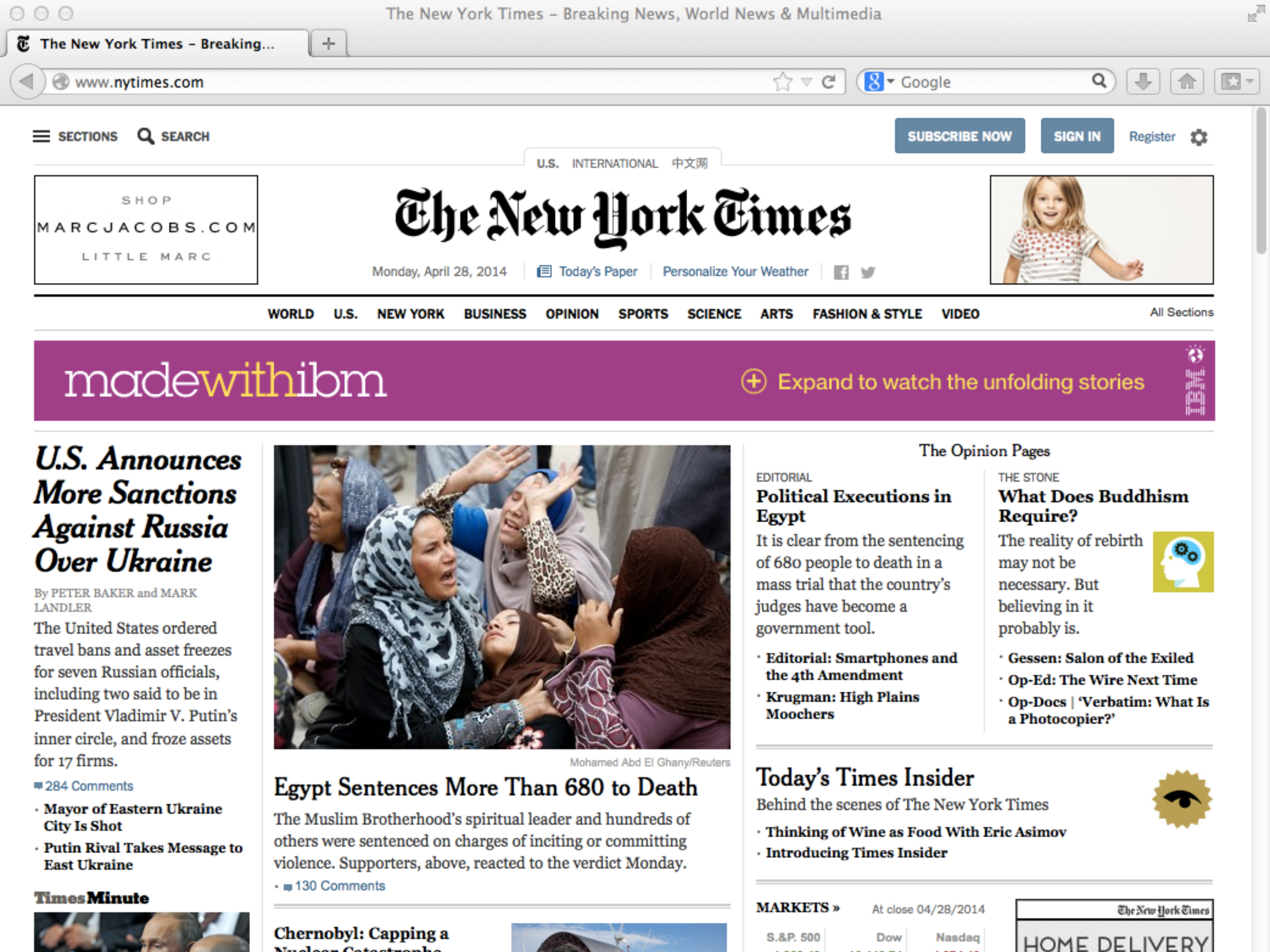
How to search the contents

Private Browsing - Browse the web without saving information about the sites you visit

As you browse the web, Firefox remembers lots of information for you: sites you've visited, files you've downloaded, and more. There may be times, however, when you don't want other users on your computer to see this information, such as when shopping for a birthday present.

Private Browsing allows you to browse the Internet without saving any information about which sites and pages you've visited. This article explains what information is not saved when in Private Browsing and gives you step-by-step instructions for using it.

Warning: Private Browsing doesn't make you anonymous on the Internet. Your Internet service provider, employer, or the sites themselves can still track what pages you visit. Private Browsing also doesn't protect you from keyloggers or spyware that may be



The New York Times – Breaking News, World News & Multimedia
The New York Times – Breaking...
www.nytimes.com
Google
SECTIONS
SEARCH
SUBSCRIBE NOW
SIGN IN
Register
U.S.
INTERNATIONAL
中文网

The New York Times

Monday, April 28, 2014 | Today's Paper | Personalize Your Weather

U.S. Announces More Sanctions Against Russia Over Ukraine

By PETER BAKER and MARK LANDLER

The United States ordered travel bans and asset freezes for seven Russian officials, including two said to be in President Vladimir V. Putin's inner circle, and froze assets for 17 firms.

284 Comments

- Mayor of Eastern Ukraine City Is Shot
- Putin Rival Takes Message to East Ukraine

TimesMinute

Mohamed Abd El Ghany/Reuters

Egypt Sentences More Than 680 to Death

The Muslim Brotherhood's spiritual leader and hundreds of others were sentenced on charges of inciting or committing violence. Supporters, above, reacted to the verdict Monday.

- 130 Comments

Chernobyl: Capping a Nuclear Catastrophe

The Opinion Pages

EDITORIAL

Political Executions in Egypt

It is clear from the sentencing of 680 people to death in a mass trial that the country's judges have become a government tool.

- Editorial: Smartphones and the 4th Amendment
- Krugman: High Plains Moochers

THE STONE

What Does Buddhism Require?

The reality of rebirth may not be necessary. But believing in it probably is.

- Gessen: Salon of the Exiled
- Op-Ed: The Wire Next Time
- Op-Docs | 'Verbatim: What Is a Photocopier?'

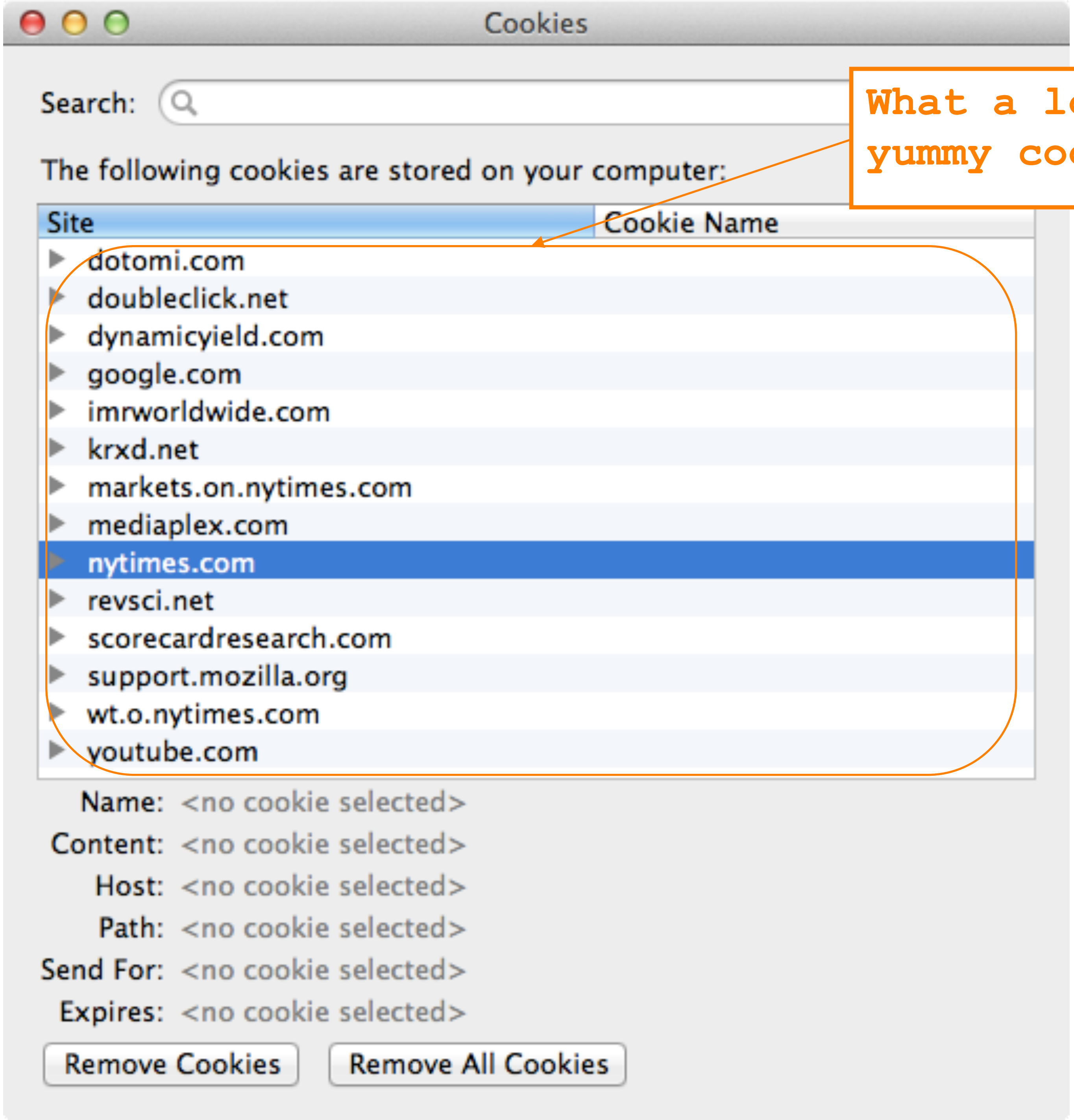
Today's Times Insider

Behind the scenes of The New York Times

- Thinking of Wine as Food With Eric Asimov
- Introducing Times Insider

MARKETS » At close 04/28/2014

S.&P. 500 | Dow | Nasdaq



Cookies

Search:

The following cookies are stored on your computer:

Site	Cookie Name
dotomi.com	
doubleclick.net	
dynamicyield.com	
google.com	
imrworldwide.com	
krxd.net	
markets.on.nytimes.com	
mediaplex.com	
nytimes.com	
revsci.net	
scorecardresearch.com	
support.mozilla.org	
wt.o.nytimes.com	
youtube.com	

Name: <no cookie selected>

Content: <no cookie selected>

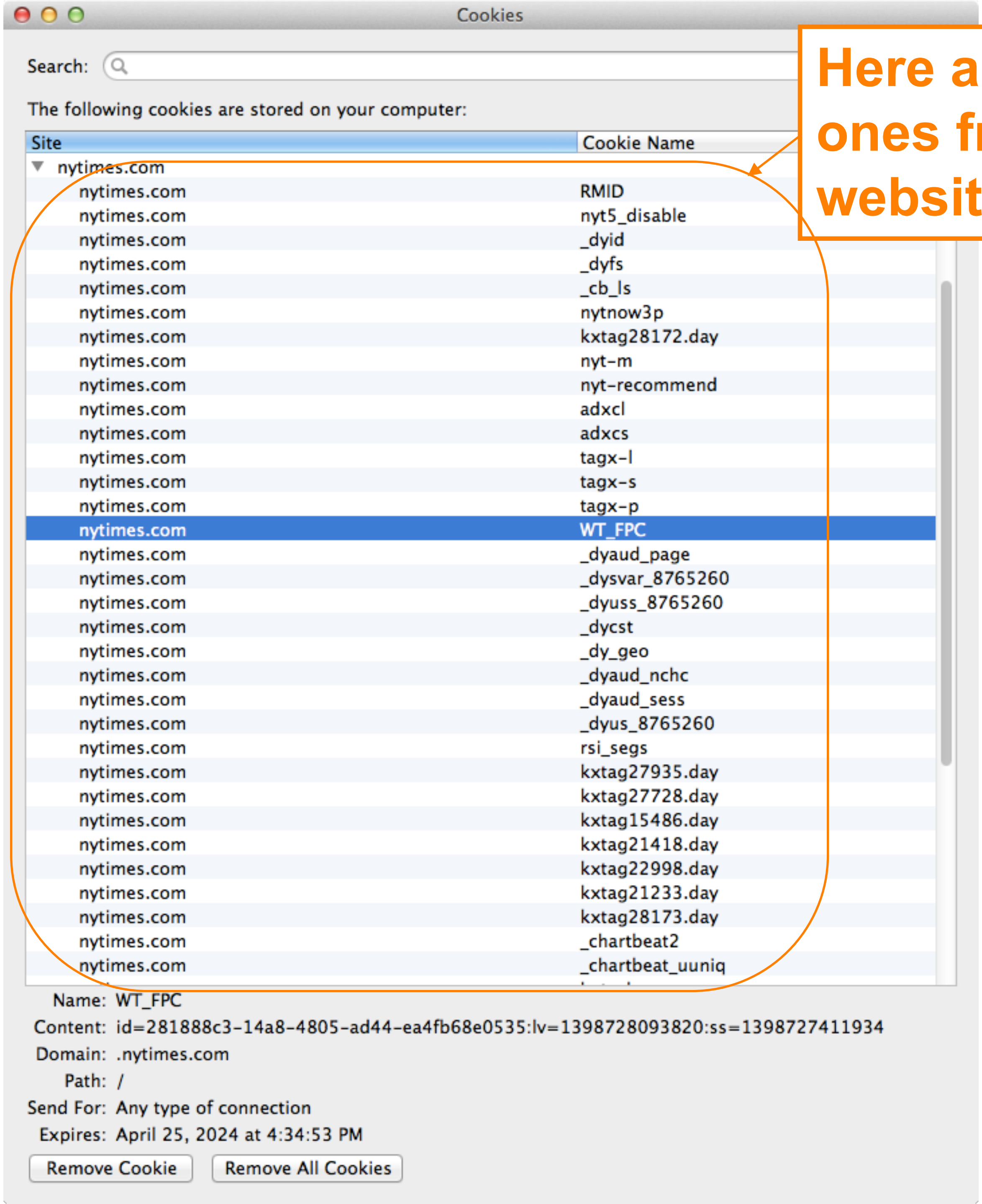
Host: <no cookie selected>

Path: <no cookie selected>

Send For: <no cookie selected>

Expires: <no cookie selected>

What a lot of yummy cookies!

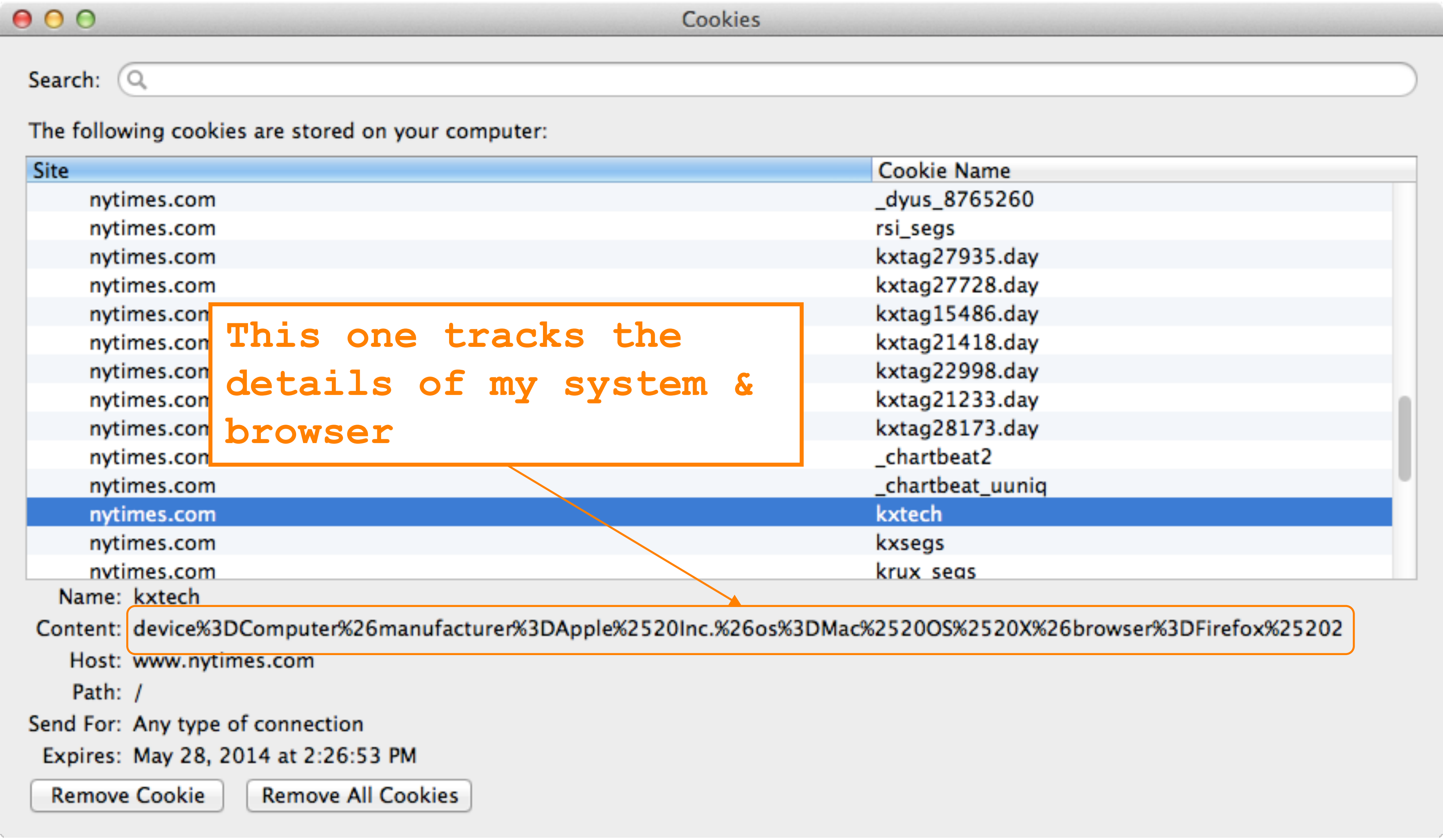


The following cookies are stored on your computer:

Site	Cookie Name
▼ nytimes.com	
nytimes.com	RMID
nytimes.com	nyt5_disable
nytimes.com	_dyid
nytimes.com	_dyfs
nytimes.com	_cb_ls
nytimes.com	nytnow3p
nytimes.com	kxtag28172.day
nytimes.com	nyt-m
nytimes.com	nyt-recommend
nytimes.com	adxcl
nytimes.com	adxcs
nytimes.com	tagx-l
nytimes.com	tagx-s
nytimes.com	tagx-p
nytimes.com	WT_FPC
nytimes.com	_dyaud_page
nytimes.com	_dysvar_8765260
nytimes.com	_dyuss_8765260
nytimes.com	_dycst
nytimes.com	_dy_geo
nytimes.com	_dyaud_nchc
nytimes.com	_dyaud_sess
nytimes.com	_dyus_8765260
nytimes.com	rsi_segs
nytimes.com	kxtag27935.day
nytimes.com	kxtag27728.day
nytimes.com	kxtag15486.day
nytimes.com	kxtag21418.day
nytimes.com	kxtag22998.day
nytimes.com	kxtag21233.day
nytimes.com	kxtag28173.day
nytimes.com	_chartbeat2
nytimes.com	_chartbeat_uuniq

Name: WT_FPC
Content: id=281888c3-14a8-4805-ad44-ea4fb68e0535:lv=1398728093820:ss=1398727411934
Domain: .nytimes.com
Path: /
Send For: Any type of connection
Expires: April 25, 2024 at 4:34:53 PM

Here are the ones from the website itself …



The following cookies are stored on your computer:

Site	Cookie Name
nytimes.com	_dyus_8765260
nytimes.com	rsi_segs
nytimes.com	kxtag27935.day
nytimes.com	kxtag27728.day
nytimes.com	kxtag15486.day
nytimes.com	kxtag21418.day
nytimes.com	kxtag22998.day
nytimes.com	kxtag21233.day
nytimes.com	kxtag28173.day
nytimes.com	_chartbeat2
nytimes.com	_chartbeat_uuniq
nytimes.com	kxtech
nytimes.com	kxsegs
nytimes.com	krux_segs

This one tracks the details of my system & browser

Name: kxtech

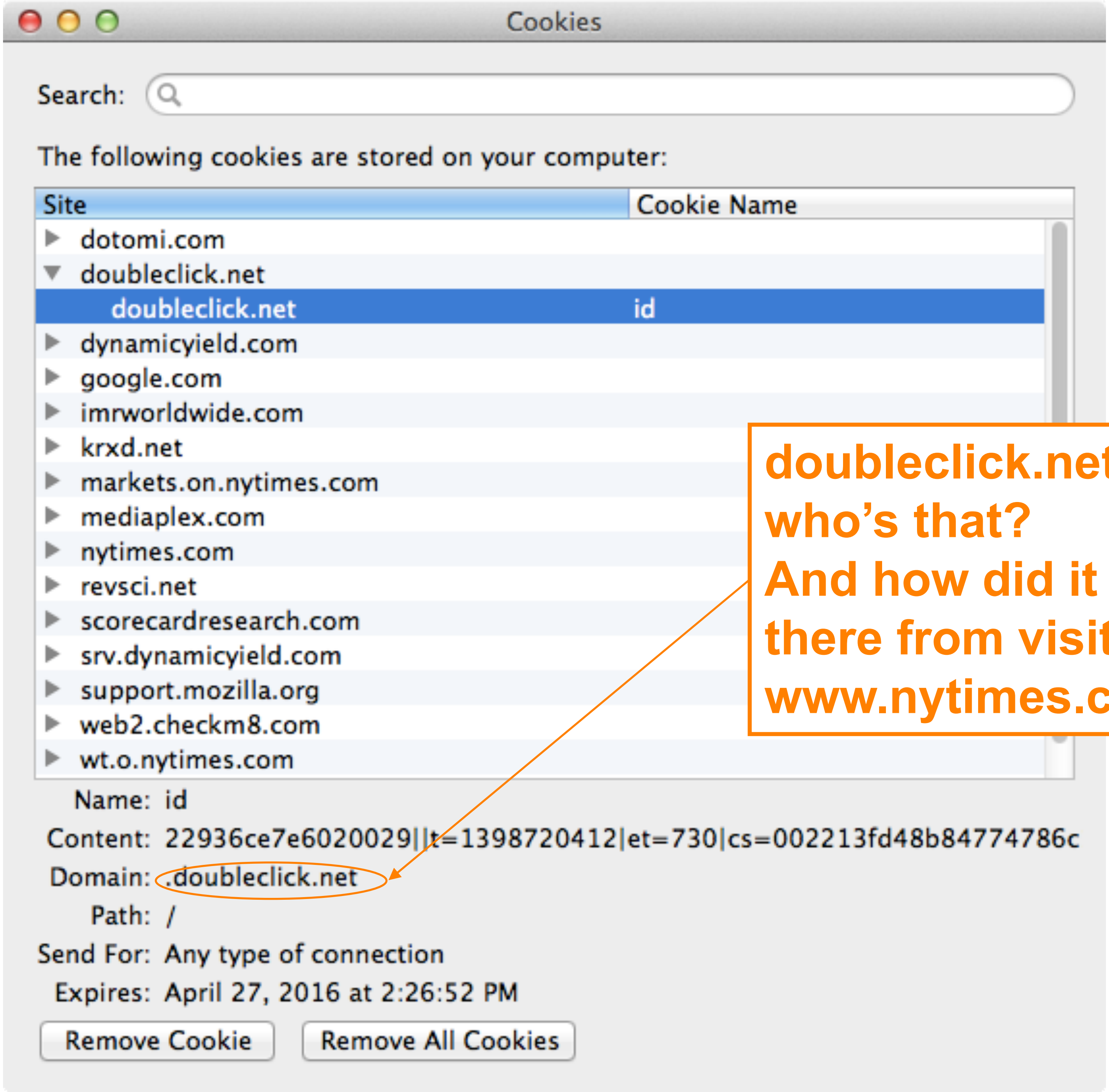
Content: device%3DComputer%26manufacturer%3DApple%2520Inc.%26os%3DMac%2520OS%2520X%26browser%3DFirefox%25202

Host: www.nytimes.com

Path: /

Send For: Any type of connection

Expires: May 28, 2014 at 2:26:53 PM



The following cookies are stored on your computer:

Site	Cookie Name
▶ dotomi.com	
▼ doubleclick.net	
doubleclick.net	id
▶ dynamicyield.com	
▶ google.com	
▶ imrworldwide.com	
▶ krxd.net	
▶ markets.on.nytimes.com	
▶ mediaplex.com	
▶ nytimes.com	
▶ revsci.net	
▶ scorecardresearch.com	
▶ srv.dynamicyield.com	
▶ support.mozilla.org	
▶ web2.checkm8.com	
▶ wt.o.nytimes.com	

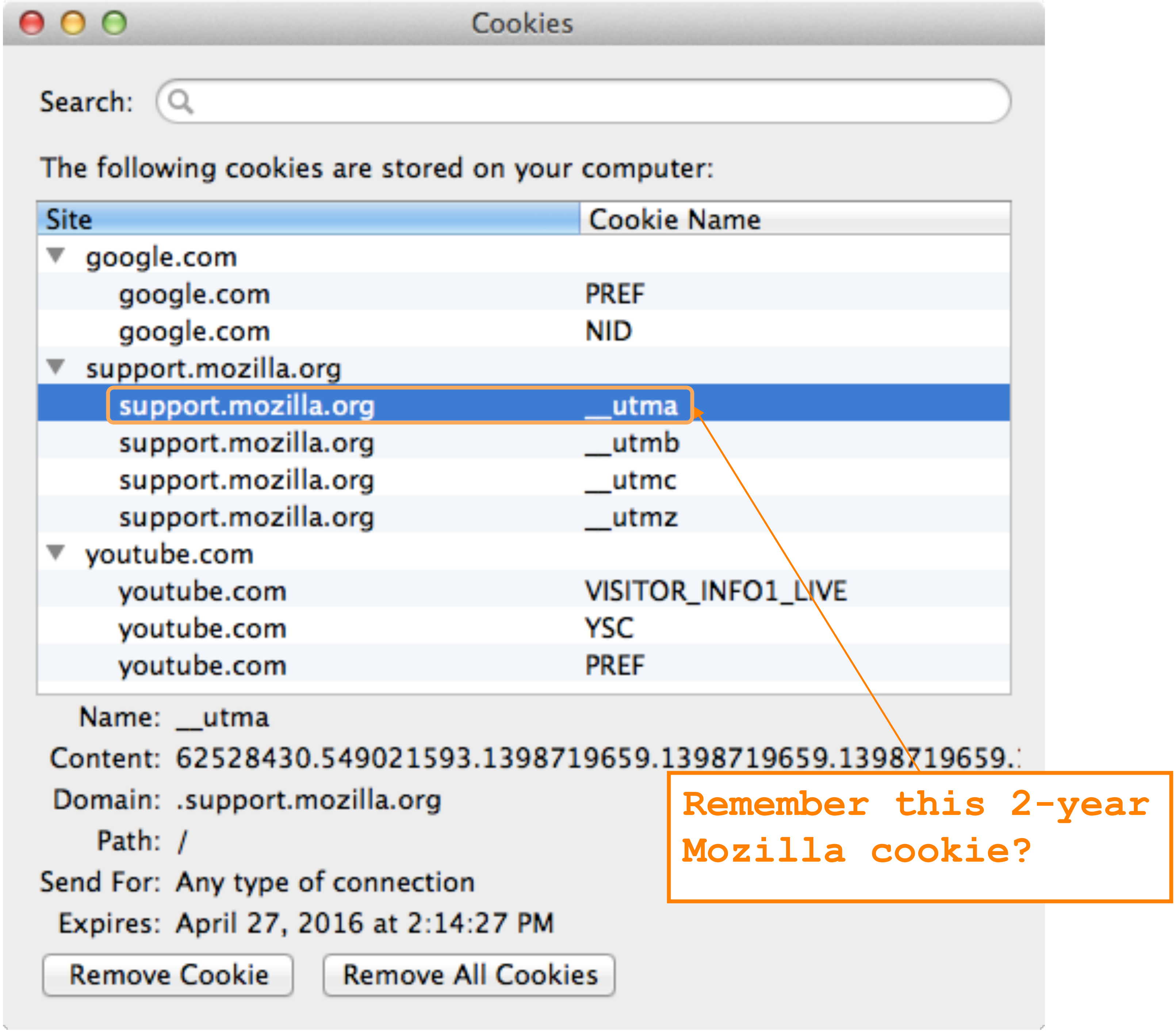
Name: id
Content: 22936ce7e6020029||t=1398720412|et=730|cs=002213fd48b84774786c
Domain: .doubleclick.net
Path: /
Send For: Any type of connection
Expires: April 27, 2016 at 2:26:52 PM

doubleclick.net - who's that? And how did it get there from visiting www.nytimes.com?

Third-Party Cookies

- How can a web site enable a third party to plant cookies in your browser & later retrieve them?
  - Include on the site's page (for example):
    - `<img src="http://doubleclick.net/ad.gif" width=1 height=1>`
- Why would a site do that?
  - Site has a business relationship w/ DoubleClick *
- Why can this track you?
  - Now DoubleClick sees all of your activity that involves their web sites
  - Because your browser dutifully sends them their cookies for any web page that has that img
  - Identifier in cookie ties together activity as = YOU

- Owned by Google, by the way



Cookies

Search:

The following cookies are stored on your computer:

Site	Cookie Name
▼ google.com	
google.com	PREF
google.com	NID
▼ support.mozilla.org	
support.mozilla.org	__utma
support.mozilla.org	__utmb
support.mozilla.org	__utmc
support.mozilla.org	__utmz
▼ youtube.com	
youtube.com	VISITOR_INFO1_LIVE
youtube.com	YSC
youtube.com	PREF

Name: __utma

Content: 62528430.549021593.1398719659.1398719659.1398719659.

Domain: .support.mozilla.org

Path: /

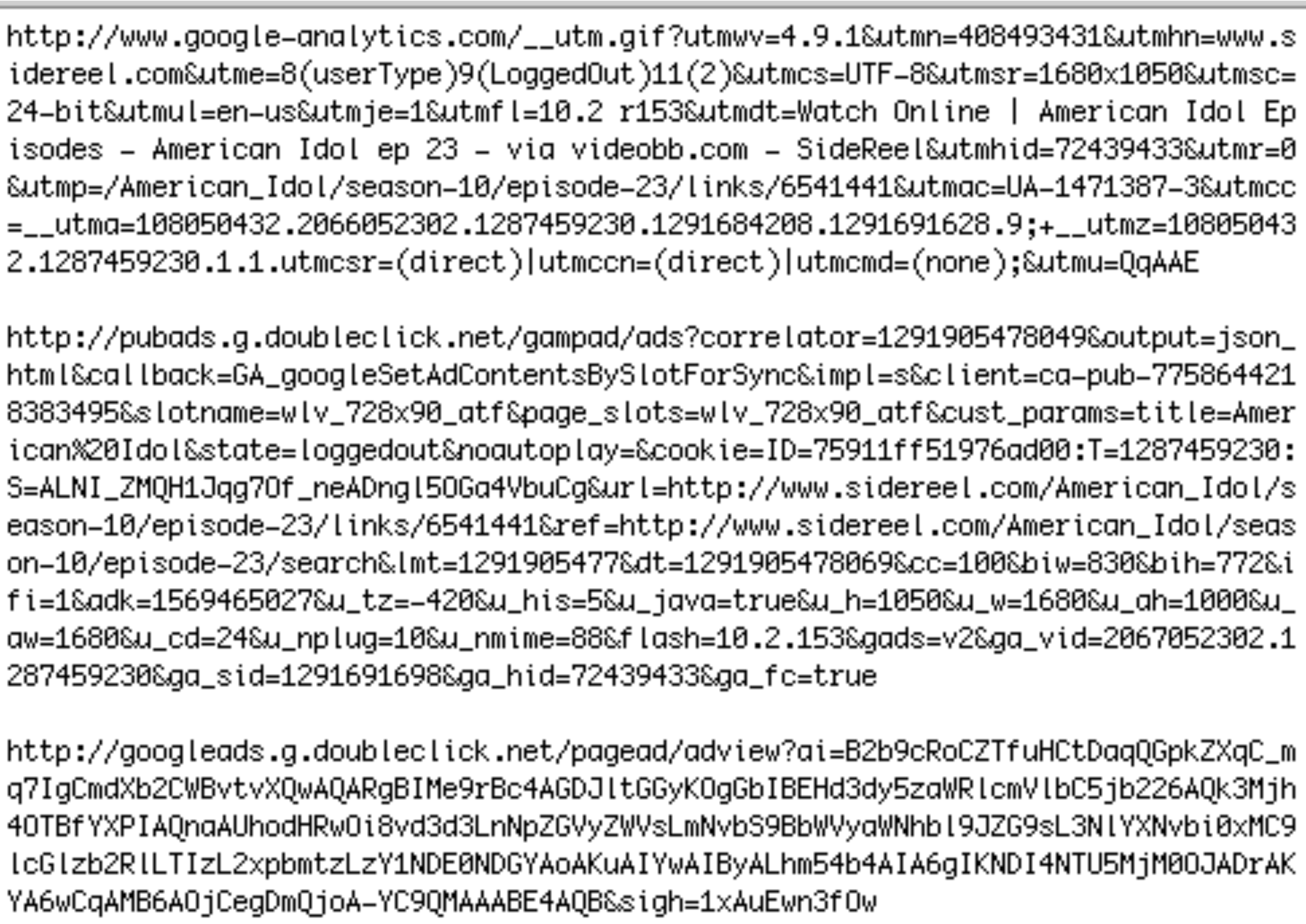
Send For: Any type of connection

Expires: April 27, 2016 at 2:14:27 PM

Remember this 2-year Mozilla cookie?

Google Analytics

- Any web site can (anonymously) register with Google to instrument their site for *analytics*
  - Gather information about who visits, what they do when they visit
- To do so, site adds a small Javascript snippet that loads http://www.google-analytics.com/ga.js
  - You can see sites that do this because they introduce a "`__utma`" cookie
- Code ships off to Google information associated with your visit to the web site
  - Shipped by fetching a GIF w/ values encoded in URL
  - Web site can use it to analyze their ad "campaigns"
  - Not a small amount of info …



```
http://www.google-analytics.com/__utm.gif?utmwv=4.9.1&utmn=408493431&utmhn=www.s
idereel.com&utme=8(userType)9(LoggedOut)11(2)&utmcs=UTF-8&utmsr=1680x1050&utmsc=
24-bit&utmul=en-us&utmje=1&utmfl=10.2 r153&utmdt=Watch Online | American Idol Ep
isodes - American Idol ep 23 - via videobb.com - SideReel&utmhid=72439433&utmr=0
&utmp=/American_Idol/season-10/episode-23/links/6541441&utmac=UA-1471387-3&utmcc
=__utma=108050432.2066052302.1287459230.1291684208.1291691628.9;+__utmz=10805043
2.1287459230.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);&utmu=QqAAE

http://pubads.g.doubleclick.net/gampad/ads?correlator=1291905478049&output=json_
html&callback=GA_googleSetAdContentsBySlotForSync&impl=s&client=ca-pub-775864421
8383495&slotname=wlv_728x90_atf&page_slots=wlv_728x90_atf&cust_params=title=Amer
ican%20Idol&state=loggedout&noautoplay=&cookie=ID=75911ff51976ad00:T=1287459230:
S=ALNI_ZMQH1Jqg7Of_neADngl5OGa4VbuCg&url=http://www.sidereel.com/American_Idol/s
eason-10/episode-23/links/6541441&ref=http://www.sidereel.com/American_Idol/seas
on-10/episode-23/search&lmt=1291905477&dt=1291905478069&cc=100&biw=830&bih=772&i
fi=1&adk=1569465027&u_tz=-420&u_his=5&u_java=true&u_h=1050&u_w=1680&u_ah=1000&u_
aw=1680&u_cd=24&u_nplug=10&u_nmime=88&flash=10.2.153&gads=v2&ga_vid=2067052302.1
287459230&ga_sid=1291691698&ga_hid=72439433&ga_fc=true

http://googleads.g.doubleclick.net/pagead/adview?ai=B2b9cRoCZTfuHCtDaqQGpkZXqC_m
q7IgCmdXb2CWBvtvXQwAQARgBIMe9rBc4AGDJltGGyKOgGbIBEHd3dy5zaWRlcmVlbC5jb226AQk3Mjh
4OTBfYXPIAQnaAUhodHRwOi8vd3d3LnNpZGVyZWVsLmNvbS9BbWVyaWNhbl9JZG9sL3NlYXNvbi0xMC9
lcGlzb2RlLTIzL2xpbmtzLzY1NDE0NDGYAoAKuAIYwAIByALhm54b4AIA6gIKNDI4NTU5MjM0OJADrAK
YA6wCqAMB6AOjCegDmQjoA-YC9QMAAABE4AQB&sigh=1xAuEwn3fOw
```

Values Reportable via Google Analytics

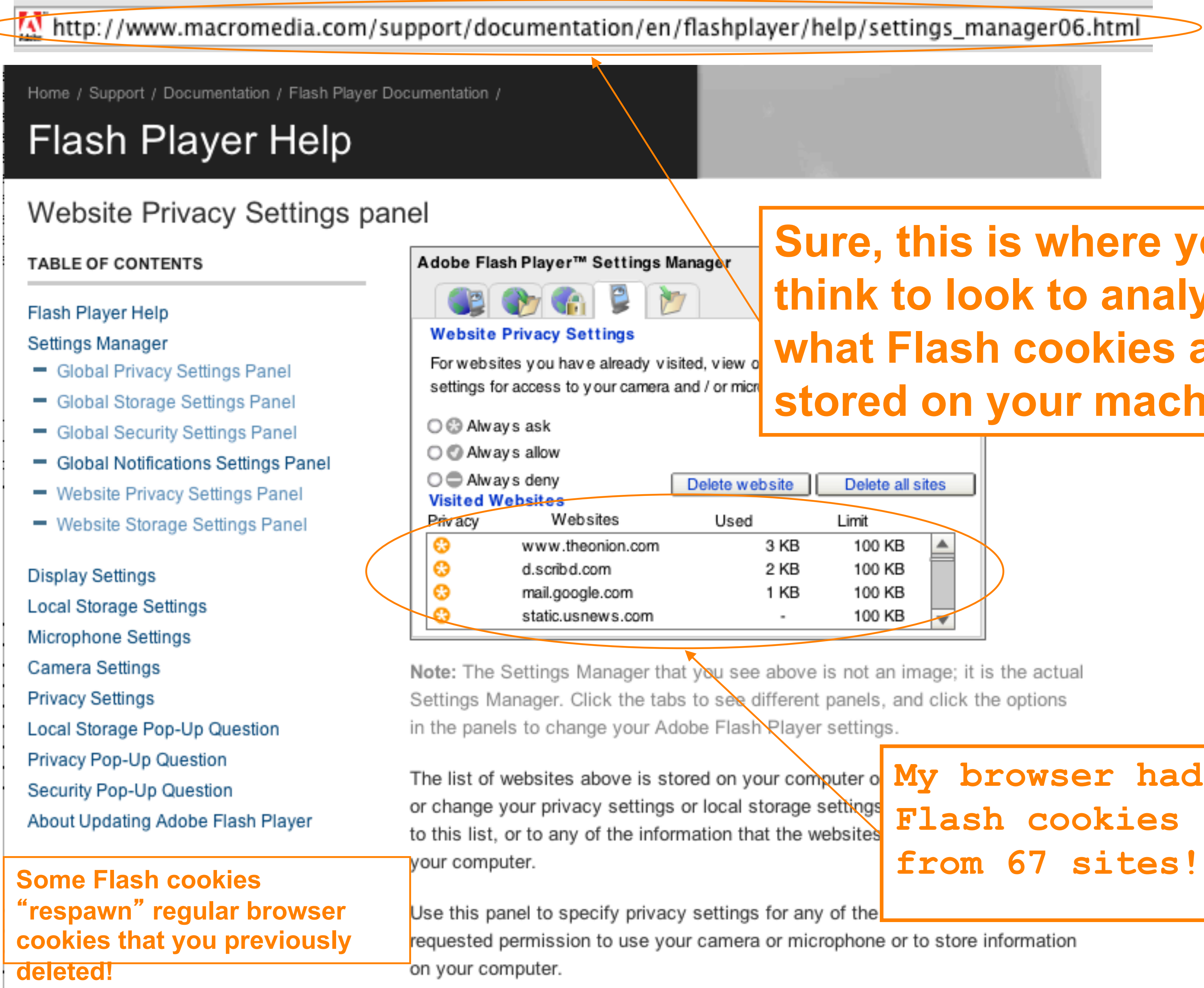
Affiliation
Billing City
Billing Country
Billing Region
Browser Lang.
Complete URL
Cookie Values
Current Page
Event Tracking
Flash Version
Grand Total

Host Name
Java-enabled
Language Encoding
Order ID
Page Title
Product Code
Product Name
Profile Number
Repeat Campaign Visit
Quantity
Screen Color Depth

Screen Resolution
Shipping Cost
Special Event
Start Campaign Sess.
Tax
Tracking Code Version
Unique GIF ID
Unit Price
User Defined Var
Variations on an Item

Still More Tracking Techniques …

- Any scenario where browsers execute programs that manage persistent state can support tracking by cookies
  - Such as …. *Flash ?*



http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager06.html

Home / Support / Documentation / Flash Player Documentation /

Flash Player Help

Website Privacy Settings panel

TABLE OF CONTENTS

Adobe Flash Player™ Settings Manager

Website Privacy Settings

For websites you have already visited, view o
settings for access to your camera and / or micr

○ Always ask
○ Always allow
○ Always deny

Delete website | Delete all sites

Visited Websites

Privacy	Websites	Used	Limit
✲	www.theonion.com	3 KB	100 KB
✲	d.scribd.com	2 KB	100 KB
✲	mail.google.com	1 KB	100 KB
✲	static.usnews.com	-	100 KB

Note: The Settings Manager that you see above is not an image; it is the actual Settings Manager. Click the tabs to see different panels, and click the options in the panels to change your Adobe Flash Player settings.

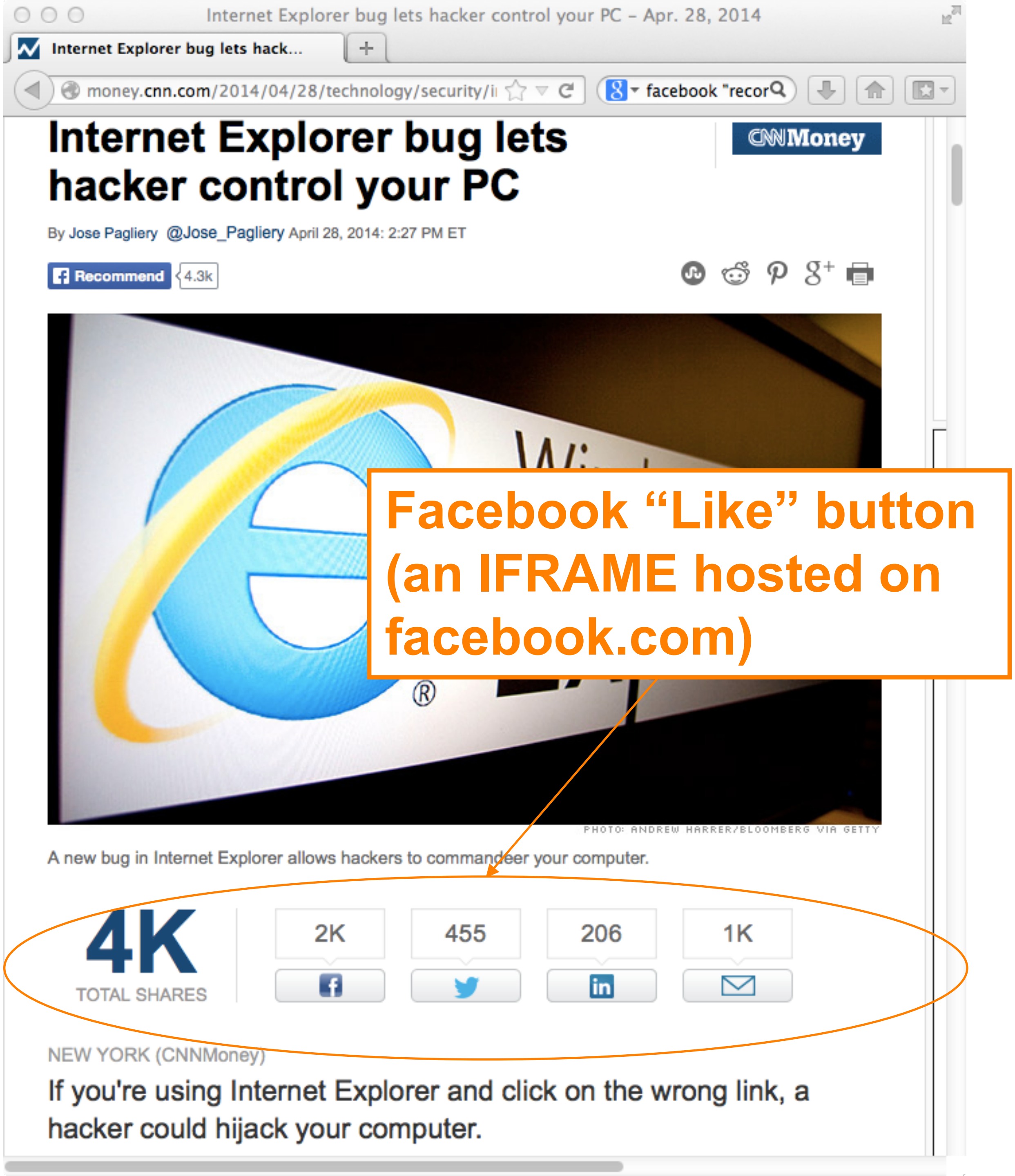
The list of websites above is stored on your computer o
or change your privacy settings or local storage settings
to this list, or to any of the information that the websites
your computer.

Use this panel to specify privacy settings for any of the
requested permission to use your camera or microphone or to store information on your computer.

Sure, this is where you'd think to look to analyze what Flash cookies are stored on your machine

My browser had Flash cookies from 67 sites!

Some Flash cookies "respawn" regular browser cookies that you previously deleted!



Internet Explorer bug lets hacker control your PC - Apr. 28, 2014

Internet Explorer bug lets hack...
money.cnn.com/2014/04/28/technology/security/i
facebook "recor

Internet Explorer bug lets hacker control your PC

By Jose Pagliery @Jose_Pagliery April 28, 2014: 2:27 PM ET

PHOTO: ANDREW HARRER/BLOOMBERG VIA GETTY

A new bug in Internet Explorer allows hackers to commandeer your computer.

4K
TOTAL SHARES
2K
455
206
1K

NEW YORK (CNNMoney)

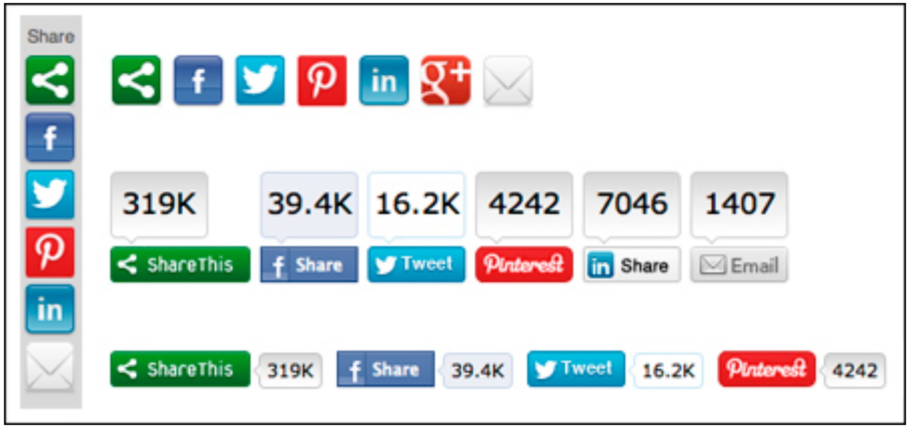
If you're using Internet Explorer and click on the wrong link, a hacker could hijack your computer.

Facebook "Like" button (an IFRAME hosted on facebook.com)

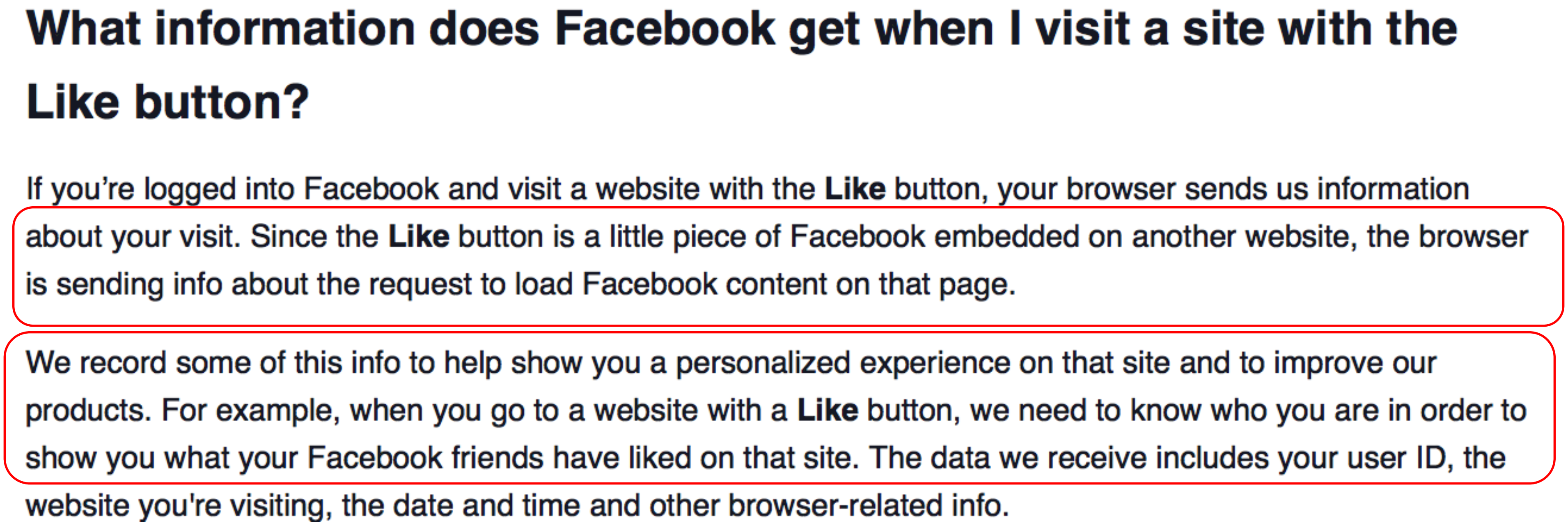
What does Facebook learn?

- Many pages include a Facebook “Like” button.
- What are the implications, for user tracking?

- Facebook can track you on every site that you visit that embeds such a button



From Facebook:



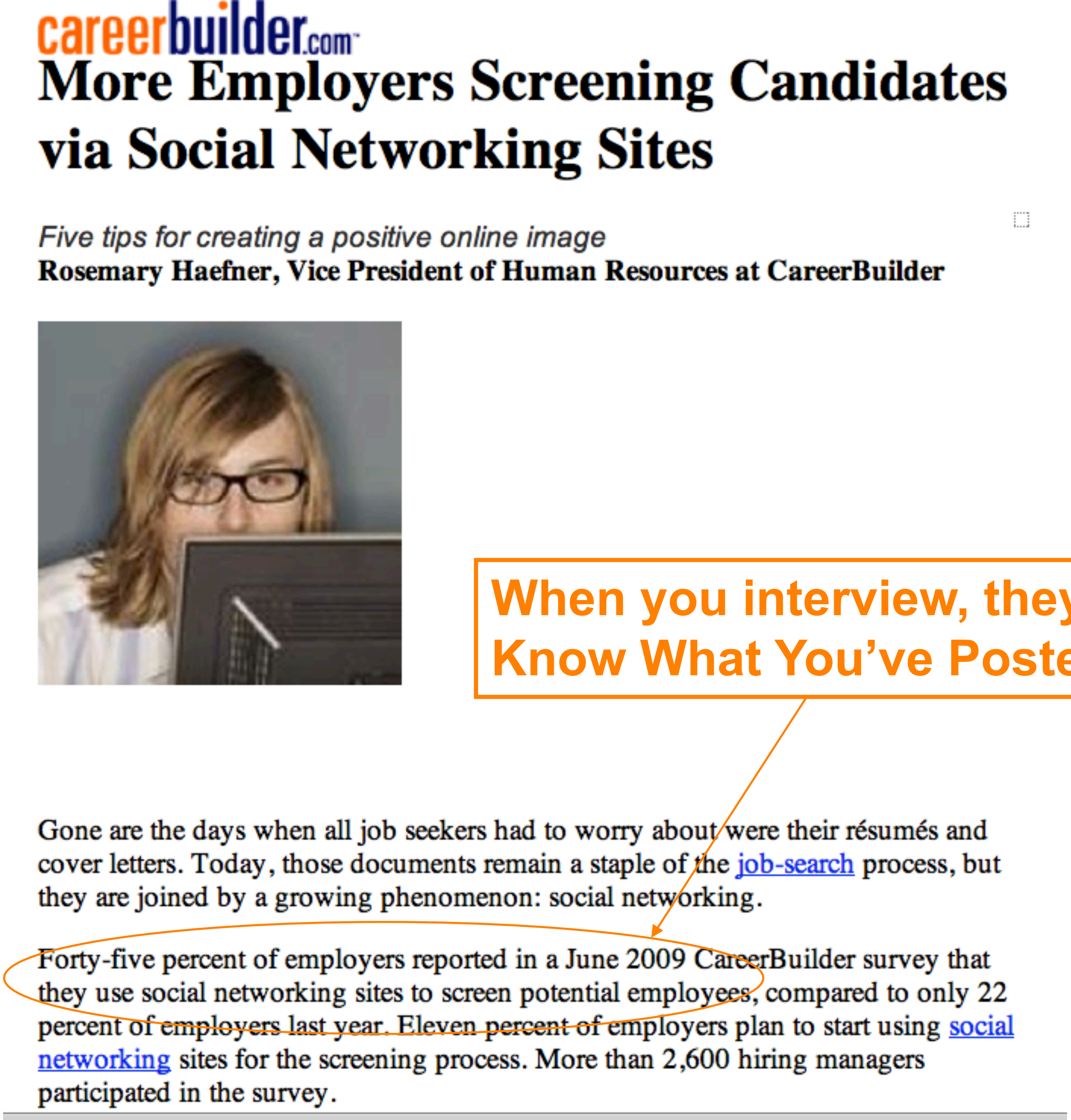
What information does Facebook get when I visit a site with the Like button?

If you’re logged into Facebook and visit a website with the **Like** button, your browser sends us information about your visit. Since the **Like** button is a little piece of Facebook embedded on another website, the browser is sending info about the request to load Facebook content on that page.

We record some of this info to help show you a personalized experience on that site and to improve our products. For example, when you go to a website with a **Like** button, we need to know who you are in order to show you what your Facebook friends have liked on that site. The data we receive includes your user ID, the website you're visiting, the date and time and other browser-related info.

Tracking – So What?

- Cookies form the core of how Internet advertising works today
  - Without them, arguably you'd have to pay for content up front a lot more
    - (and payment would mean you'd lose anonymity anyway)
  - A "better ad experience" is not necessarily bad
    - Ads that reflect your interests; not seeing repeated ads
- But: ease of gathering so much data so easily ⇒ concern of losing control how it's used
  - Privacy concerns
  - Large amounts of private data in one place



careerbuilder.com

More Employers Screening Candidates via Social Networking Sites

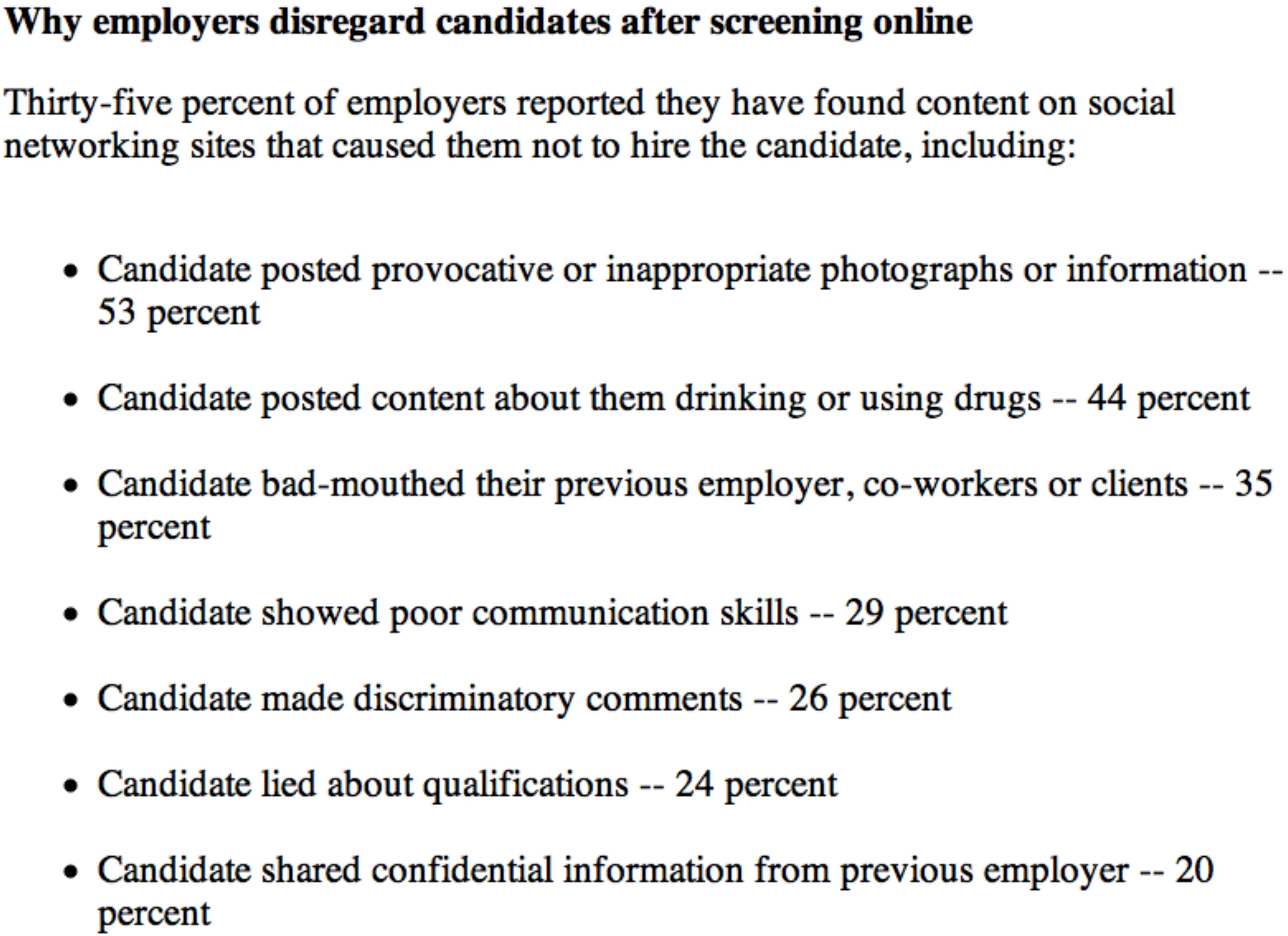
Five tips for creating a positive online image

Rosemary Haefner, Vice President of Human Resources at CareerBuilder

Gone are the days when all job seekers had to worry about were their résumés and cover letters. Today, those documents remain a staple of the job-search process, but they are joined by a growing phenomenon: social networking.

Forty-five percent of employers reported in a June 2009 CareerBuilder survey that they use social networking sites to screen potential employees, compared to only 22 percent of employers last year. Eleven percent of employers plan to start using social networking sites for the screening process. More than 2,600 hiring managers participated in the survey.

When you interview, they Know What You've Posted



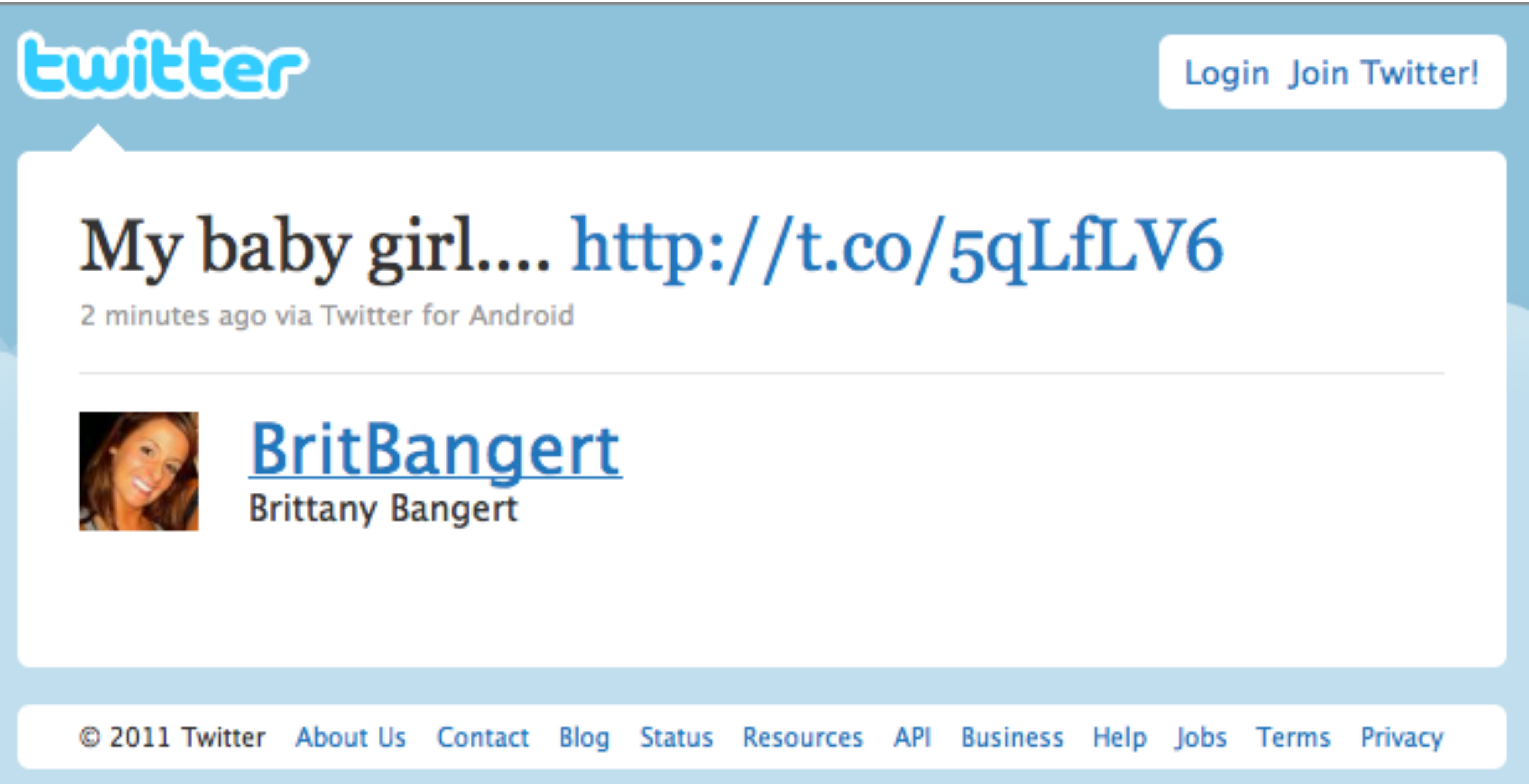
Why employers disregard candidates after screening online

Thirty-five percent of employers reported they have found content on social networking sites that caused them not to hire the candidate, including:

- Candidate posted provocative or inappropriate photographs or information -- 53 percent
- Candidate posted content about them drinking or using drugs -- 44 percent
- Candidate bad-mouthed their previous employer, co-workers or clients -- 35 percent
- Candidate showed poor communication skills -- 29 percent
- Candidate made discriminatory comments -- 26 percent
- Candidate lied about qualifications -- 24 percent
- Candidate shared confidential information from previous employer -- 20 percent

Tracking – So What?

- Cookies etc. form the core of how Internet advertising works today
  - Without them, arguably you'd have to pay for content up front a lot more
    - (and payment would mean you'd lose anonymity anyway)
  - A "better ad experience" is not necessarily bad
    - Ads that reflect your interests; not seeing repeated ads
- But: ease of gathering so much data so easily ⇒ concern of losing control how it's used
  - Content shared with friends doesn't just stay with friends …
  - You really don't have a good sense of just what you're giving away …

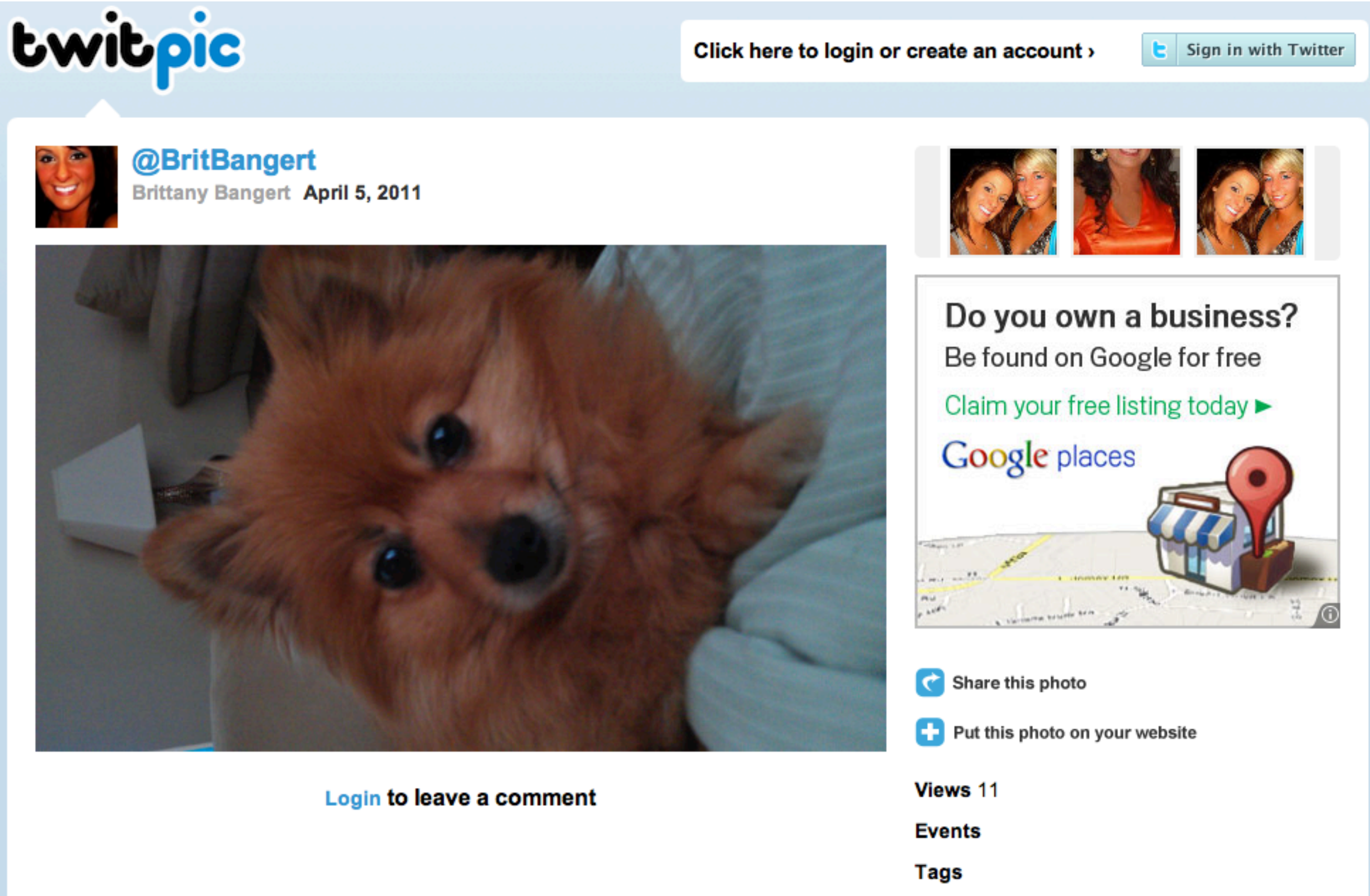


My baby girl.... http://t.co/5qLfLV6

2 minutes ago via Twitter for Android

BritBangert

Brittany Bangert



twitpic
Click here to login or create an account ›
Sign in with Twitter

@BritBangert

Brittany Bangert April 5, 2011

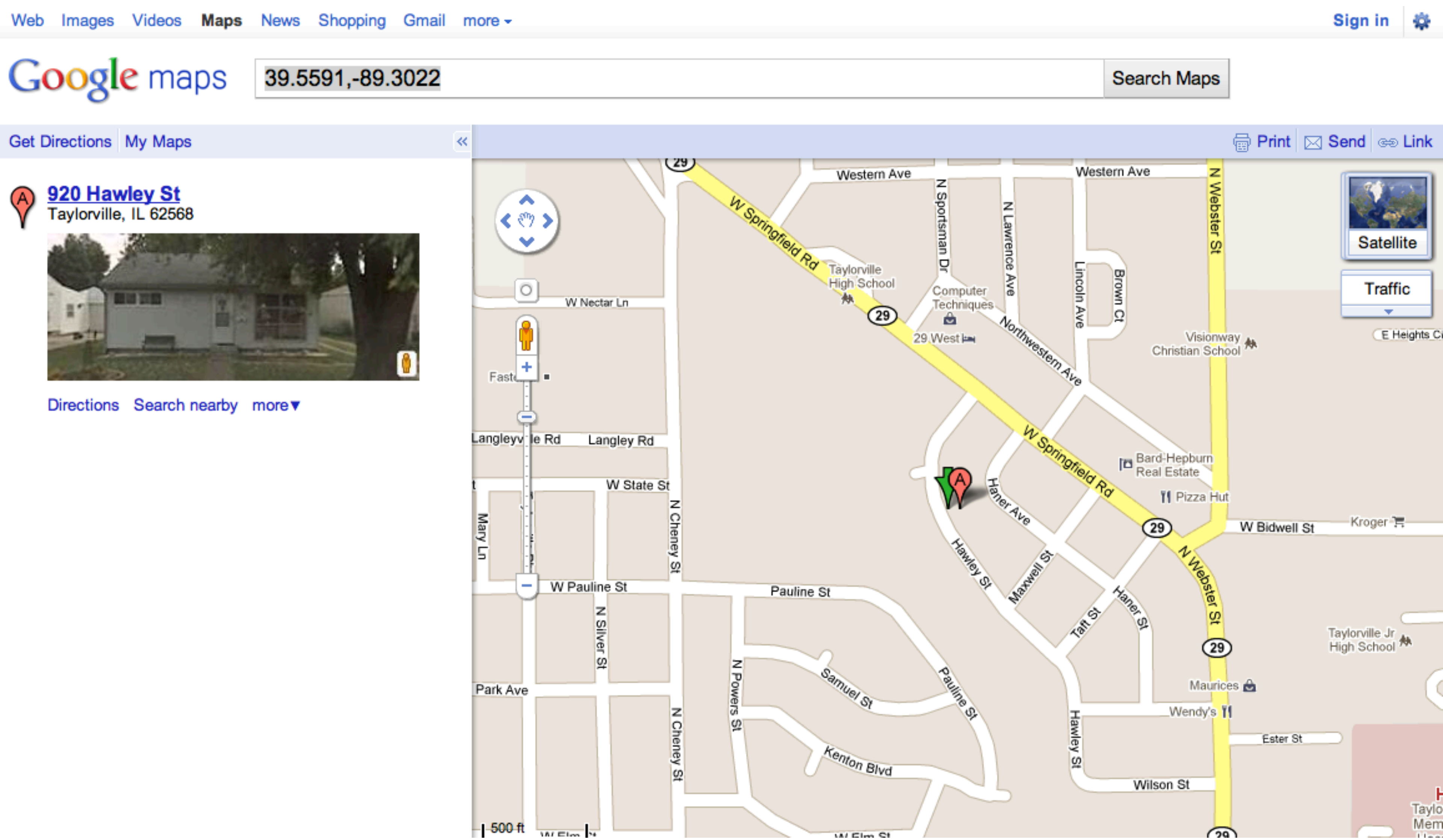
Share this photo
Put this photo on your website

Views 11

Events

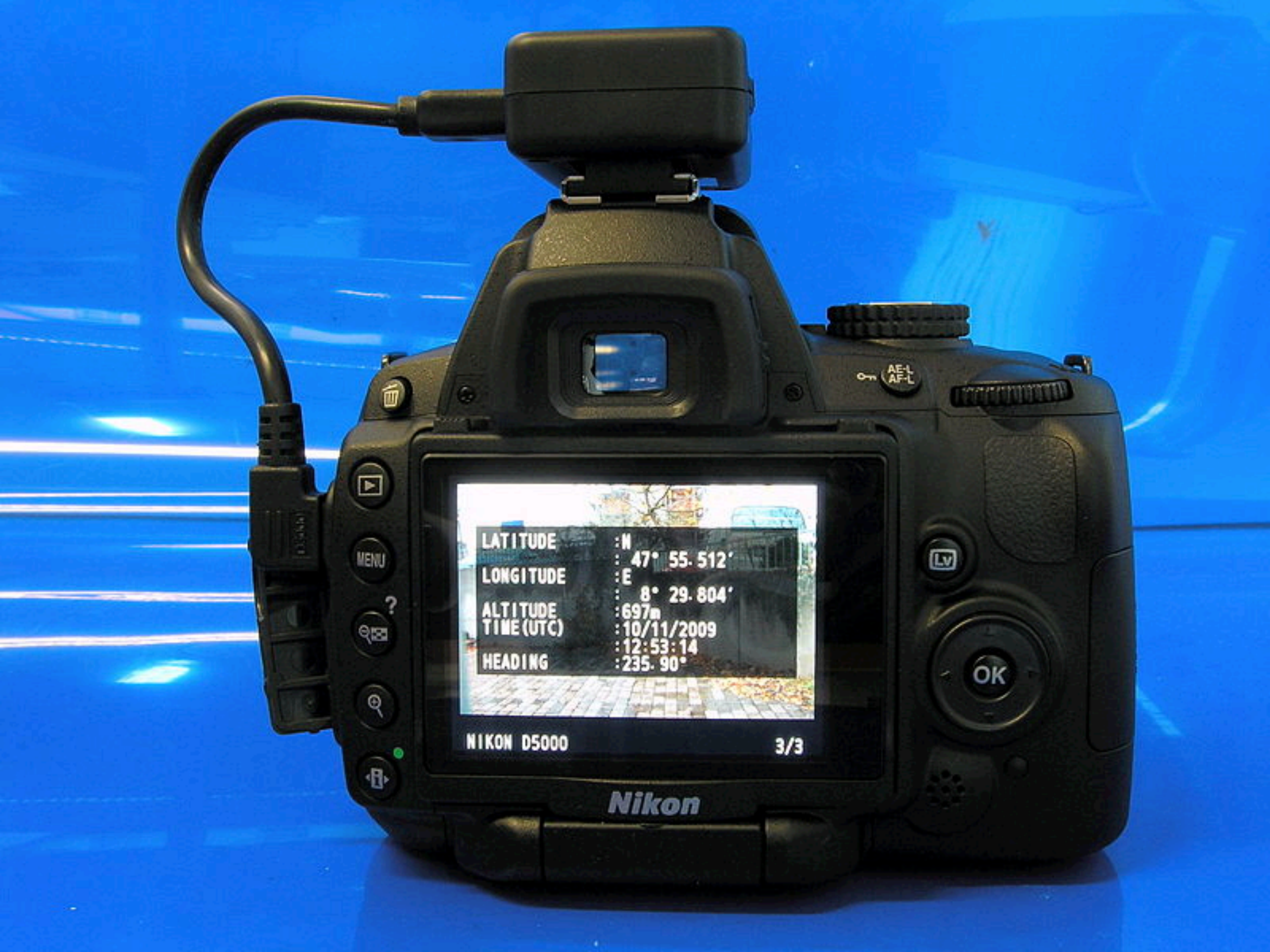
Tags

Login to leave a comment

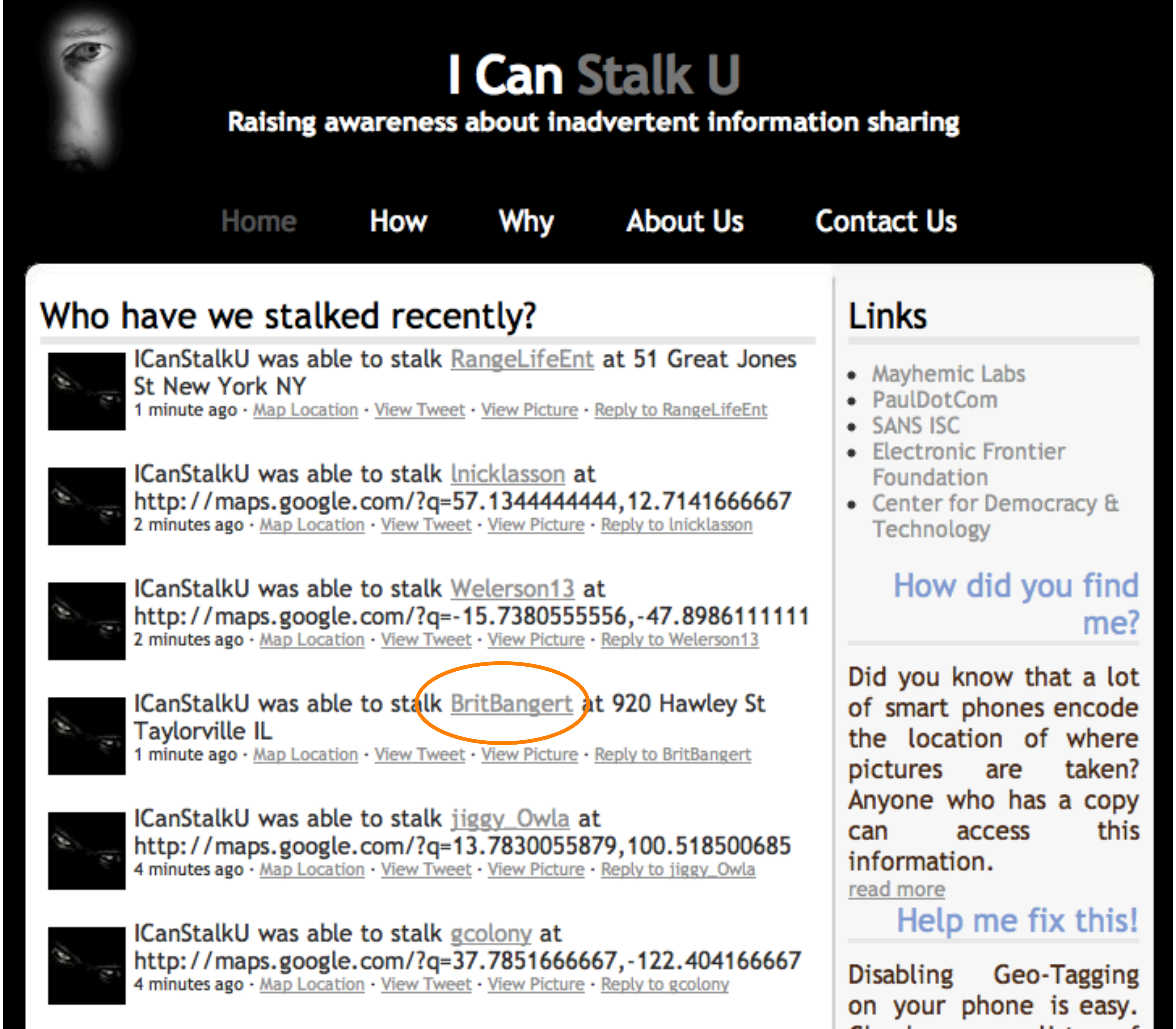


39.5591,-89.3022

920 Hawley St
Taylorville, IL 62568



```
LATITUDE    :N
            :  47° 55.512'
LONGITUDE   :E
            :   8° 29.804'
ALTITUDE    :697m
TIME(UTC)   :10/11/2009
            :12:53:14
HEADING     :235.90°
NIKON D5000                    3/3
```



I Can Stalk U

Raising awareness about inadvertent information sharing

Who have we stalked recently?

ICanStalkU was able to stalk RangeLifeEnt at 51 Great Jones St New York NY
1 minute ago · Map Location · View Tweet · View Picture · Reply to RangeLifeEnt

ICanStalkU was able to stalk lnicklasson at http://maps.google.com/?q=57.1344444444,12.7141666667
2 minutes ago · Map Location · View Tweet · View Picture · Reply to lnicklasson

ICanStalkU was able to stalk Welerson13 at http://maps.google.com/?q=-15.7380555556,-47.8986111111
2 minutes ago · Map Location · View Tweet · View Picture · Reply to Welerson13

ICanStalkU was able to stalk BritBangert at 920 Hawley St Taylorville IL
1 minute ago · Map Location · View Tweet · View Picture · Reply to BritBangert

ICanStalkU was able to stalk jiggy_Owla at http://maps.google.com/?q=13.7830055879,100.518500685
4 minutes ago · Map Location · View Tweet · View Picture · Reply to jiggy_Owla

ICanStalkU was able to stalk gcolony at http://maps.google.com/?q=37.7851666667,-122.404166667
4 minutes ago · Map Location · View Tweet · View Picture · Reply to gcolony

Links

- Mayhemic Labs
- PaulDotCom
- SANS ISC
- Electronic Frontier Foundation
- Center for Democracy & Technology

How did you find me?

Did you know that a lot of smart phones encode the location of where pictures are taken? Anyone who has a copy can access this information.
read more

Help me fix this!

Disabling Geo-Tagging on your phone is easy.

How To Gain Better Privacy?

discuss with your neighbor

How To Gain Better Privacy?

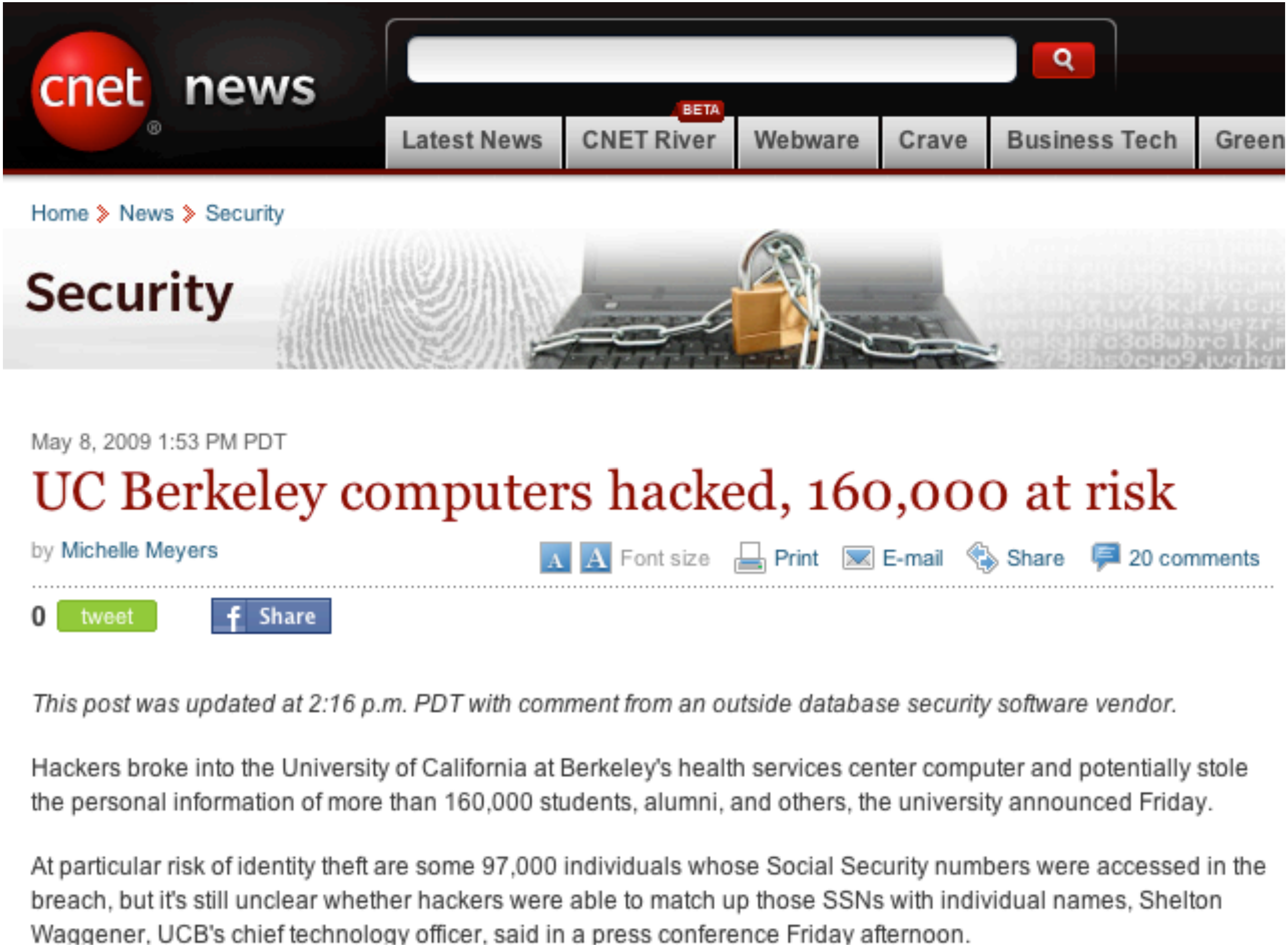
- Force of law
  - Example #1: web site privacy policies
    - US sites that violate them commit false advertising
    - But: policy might be “*Yep, we sell everything about you, Ha Ha!*”

THE NEW YORKER’ s Privacy Policy (when you buy their archives)

7. *Collection of Viewing Information. You acknowledge that you are aware of and consent to the collection of your viewing information during your use of the Software and/or Content. Viewing information may include, without limitation, the time spent viewing specific pages, the order in which pages are viewed, the time of day pages are accessed, IP address and user ID. This viewing information may be linked to personally identifiable information, such as name or address and shared with third parties.*

How To Gain Better Privacy?

- Force of law
  - Example #1: web site privacy policies
    - US sites that violate them commit false advertising
    - But: policy might be "*Yep, we sell everything about you, Ha Ha!*"
  - Example #2: SB 1386
    - *Requires an agency, person or business that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed)*
    - Quite effective at getting sites to pay attention to securing personal information



May 8, 2009 1:53 PM PDT

UC Berkeley computers hacked, 160,000 at risk

by Michelle Meyers

This post was updated at 2:16 p.m. PDT with comment from an outside database security software vendor.

Hackers broke into the University of California at Berkeley's health services center computer and potentially stole the personal information of more than 160,000 students, alumni, and others, the university announced Friday.

At particular risk of identity theft are some 97,000 individuals whose Social Security numbers were accessed in the breach, but it's still unclear whether hackers were able to match up those SSNs with individual names, Shelton Waggener, UCB's chief technology officer, said in a press conference Friday afternoon.

How To Gain Better Privacy?

- Technology
  - Various browser additions
  - Special browser extensions
  - Tor and anonymizers – later in course

Browser: “Tracking protection”

Private browsing includes tracking protection

Blocks third-party trackers based on Disconnect.me

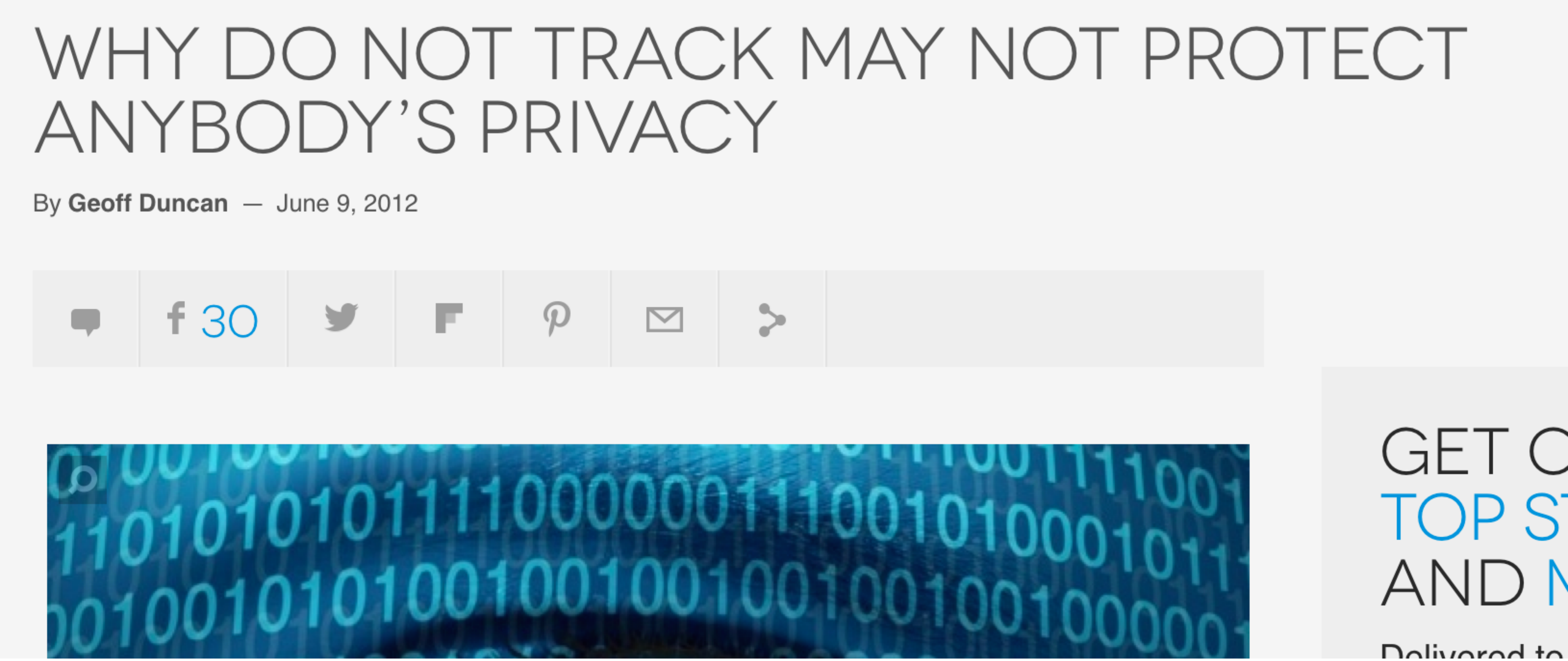
- basic: blocks commonly known analytics trackers, social sharing trackers, and advertising trackers, but allows some known content trackers to reduce website breakage.
- strict: blocks all known trackers, including analytics, trackers, social sharing trackers, and advertising trackers as well as content trackers. The strict list will break some videos, photo slideshows, and some social networks.

Browsers: Do not track flag

You can turn on this flag in your browser

What does it do?
- Tells web servers you want to opt-out of tracking
- It does this by transmitting a Do Not Track HTTP header every time your data is requested from a web server

It does not enforce that there is no tracking, it is up to the web servers whether they decide to track or not



WHY DO NOT TRACK MAY NOT PROTECT ANYBODY'S PRIVACY

By **Geoff Duncan** — June 9, 2012

Some ad companies do provide more generic ads as a result of this flag

Browser extension: Ghostery

User installs browser extension:

1. Recognizes third-party tracking scripts on a web page based on an actively curated database of such scripts

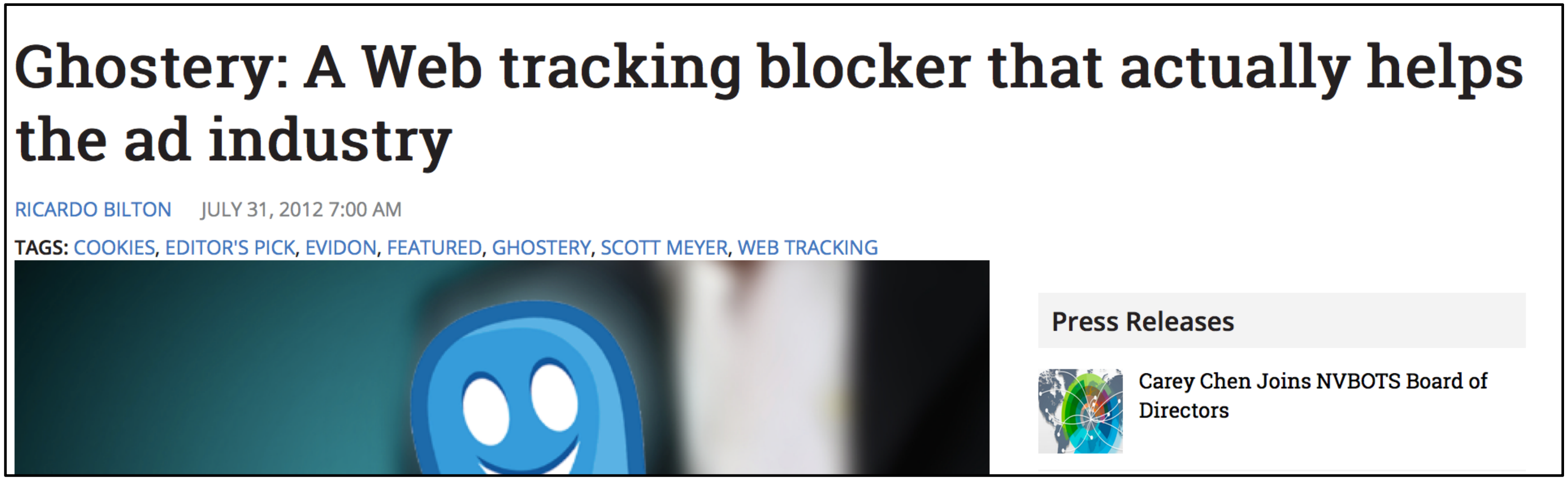
2. Blocks HTTP requests to these sites

- as a result, Facebook buttons don't even show

3. Users can create "Whitelists" of allowed sites

- e.g., allow FB button but note that you allow tracking by FB too

But you have to be careful…



Ghostery: A Web tracking blocker that actually helps the ad industry

RICARDO BILTON JULY 31, 2012 7:00 AM

TAGS: COOKIES, EDITOR'S PICK, EVIDON, FEATURED, GHOSTERY, SCOTT MEYER, WEB TRACKING

Press Releases

Carey Chen Joins NVBOTS Board of Directors

- Users can opt-in to sending anonymously data back to Evidon, the parent company, to improve its tracking database
- Evidon sells this data to ad companies..
- But strategy is transparent, users opt into this

Conclusions

- Third-party apps can track us even if when we don’t visit their website
- Tracking is very common on the web and can collect a lot of data about you
- Some solutions exist, but have caveats