

09. Web Security & Privacy

Blase Ur, April 24th, 2017
CMSC 23210 / 33210



THE UNIVERSITY OF
CHICAGO



Security, Usability, & Privacy
Education & Research

Today's class

- Trust on the web
 - SSL notifications
- Online tracking
 - Privacy tools

Trust on the web

Overview

- Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS) enable secure communication
- Frequently encountered with web browsing (HTTPS) and more behind the scenes in app, VOIP, etc.

What we want to defend against

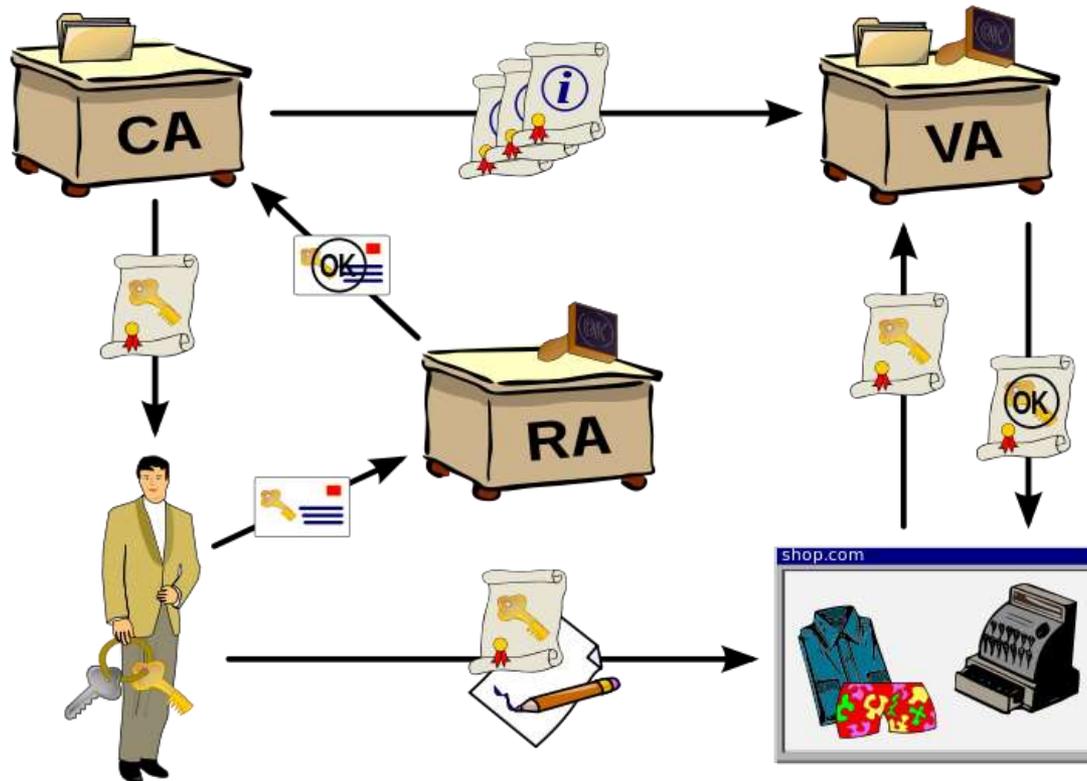
- People snooping on our communications
 - The contents of what we're sending
 - Session tokens (see, e.g., Firesheep)
- Man-in-the-middle attacks
 - We want to authenticate that we are talking to the right site, not an imposter
 - Use certificates inside a public-key infrastructure

How we could obtain trust

- Web of trust
 - People you already trust introduce you to people they trust
 - Can get complicated, doesn't scale well
 - Infrequently seen in practice
- Public-Key Infrastructure (PKI)
 - Certificates are issued by certificate authorities that bind cryptographic keys to identities

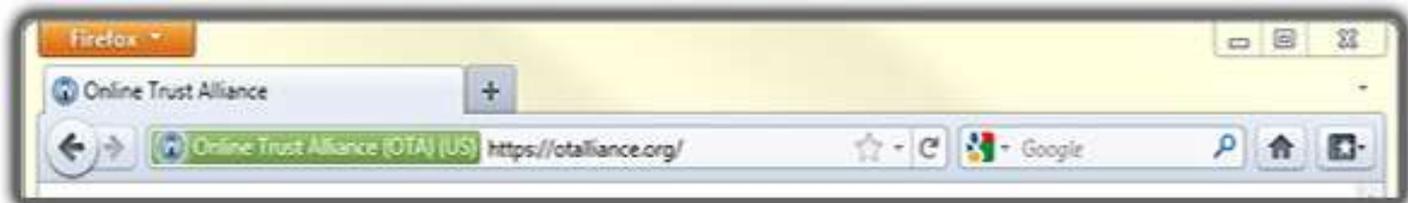
Public-Key Infrastructure

- Binding of keys to identities



What does SSL look like to users?

- Compare, e.g., the following:
 - <https://www.google.com> (normal certificate)
 - Go to Google images and then click on an image and see what happens (mixed content)
 - <https://www.thawte.com> (EV certificate)



What does SSL look like to users?

Browser	HTTPS	HTTPS minor error	HTTPS major error	HTTP	EV	Malware
Chrome 48 Win	https://www	https://mixe	https://wro	www.exam	Symantec Co	https://dow
Edge 20 Win	example.	https://mix	wrong.host.badssl	example.com	Symantec Co	Unsafe website den
Firefox 44 Win	https://www.e	https://mixec	https://expire	www.example	Symantec Corpo	https://spacet
Safari 9 Mac	example.com	mixed.badssl.c	URL hidden	example.com	Symantec Cor	downloadgam
Chrome 48 And	https://v	https://mixe	https://v	www.examp	https://v	https://spac
Opera Mini 14 And	www.exam	mixed.badssl.c	wrong.host.ba	www.example	www.syma	Unavailable
UC Mini 10 And	Example D	mixed.badssl	Blocked	Example D	Endpoint, C	Blocked
UC Browser 2 iOS	Example Do.	mixed.bads..	wrong.host..	Example Do.	Endpoint, C.	Unavailable
Safari 9 iOS	example.c	mixed.badssl	wrong.host	example.com	Symantec	Unavailable

(From Felt et al. SOUPS 2016)

How does PKI look to browsers?

- Hundreds of trusted certificate authorities
 - Certificate authorities (CAs) sign the certificates binding identities to keys
 - See, e.g., Firefox's advanced settings

How does PKI look to site admins?

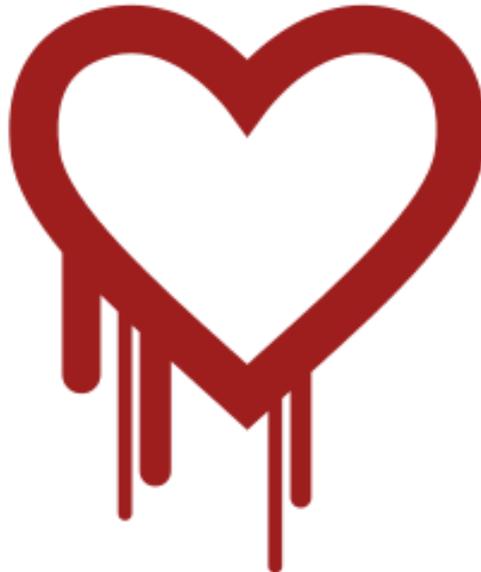
- Apply for a certificate
 - Validation process
 - Certificate authorities (CAs) delegate trust (“chain of trust”)
 - CAs sell you a certificate

Issues with SSL/TLS/PKIs

- Implementation issues
- Communicating to users what is happening
- Compromised Certificate Authorities
- Man-in-the-middle attacks
 - Downgrade/dumbing-down attacks
 - Addition of “rogue” certificates
- Revocation
- Timing attacks and other side channels

One famous implementation issue

- OpenSSL bug
 - Heartbleed (CVE-2014-0160)
 - TLS heartbeat extension misses a bounds check and thus lets an attacker “read” memory



Compromised CAs

- Comodo and Diginotar both suffered breaches in 2011 that let attackers issue rogue certificates
- What about untrustworthy CAs?
 - Compelled certificate creation attacks (see, e.g., Soghoian and Stamm FC '11)

Man-in-the-middle attacks (MITM)

- Effectively, many corporations perform MITM attacks by adding certificates to users' computers and presenting “fake” certificates to users.
- A man in the middle can also tell you a site doesn't support SSL/TLS (downgrade) or any strong ciphers (dumbing down)
 - Why does this create a huge problem?
 - Why is this hard to deal with?

Important question 1

- How do you know if a site supports HTTPS?
 - EFF's HTTPS Everywhere
 - HTTP Strict Transport Security (HSTS)
 - In both cases, how do you bootstrap/maintain?



Important question 2

- How do you know you have the right certificate for a site?
 - Certificate transparency
 - Public key pinning
 - Perspectives (originally a CMU project)



How do you know a cert is valid?

- Certificates can be revoked in case of a compromise
- Certificate Revocation Lists (CRLs) were used, but they got really large
 - Incremental updates were better
- Online Certificate Status Protocol (OCSP)
 - How does this impact privacy?
- OCSP Stapling

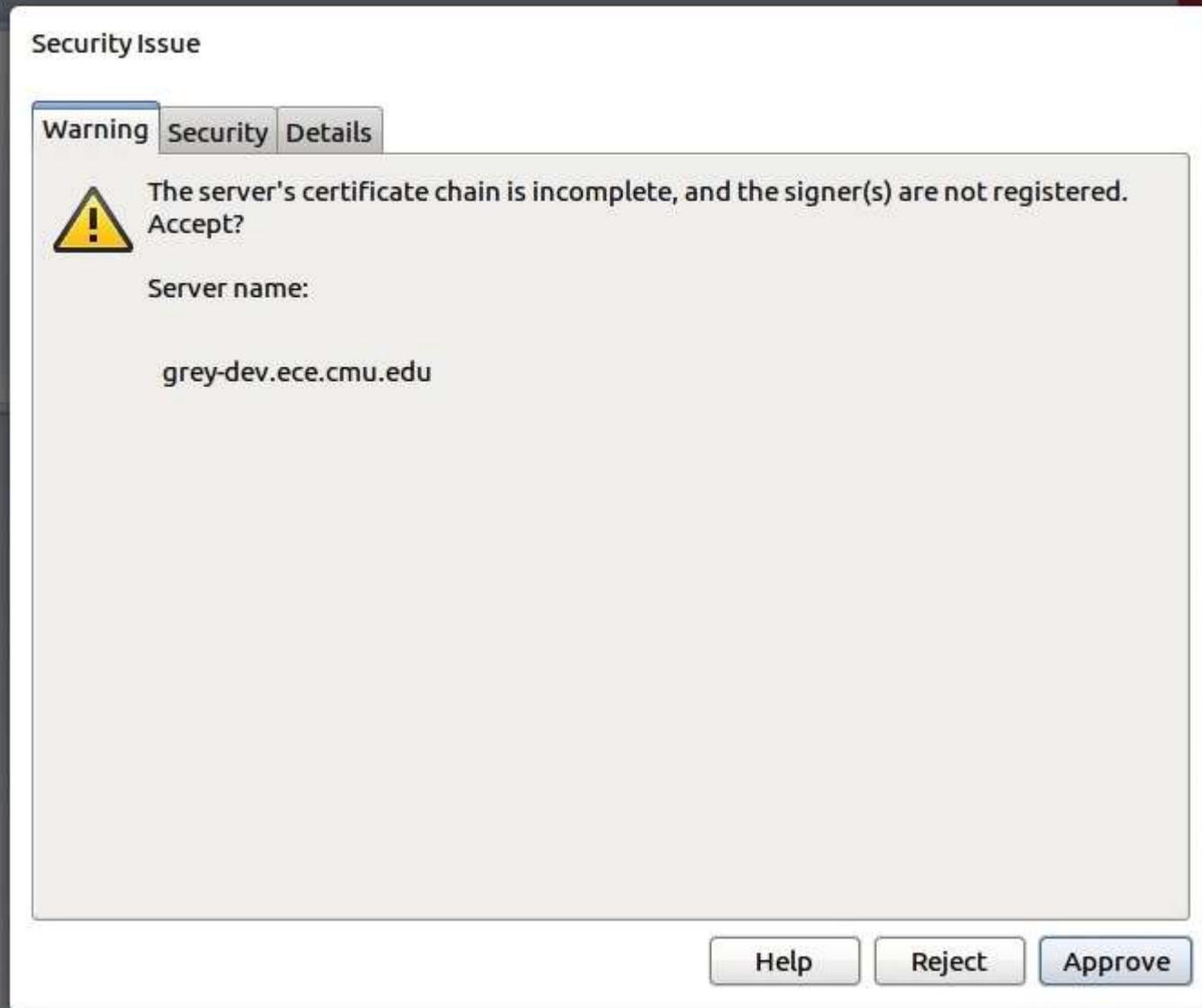
Self-signed certificates

- What happens if someone signs their own certificate and chooses not to use the PKI infrastructure?
 - You get a warning!

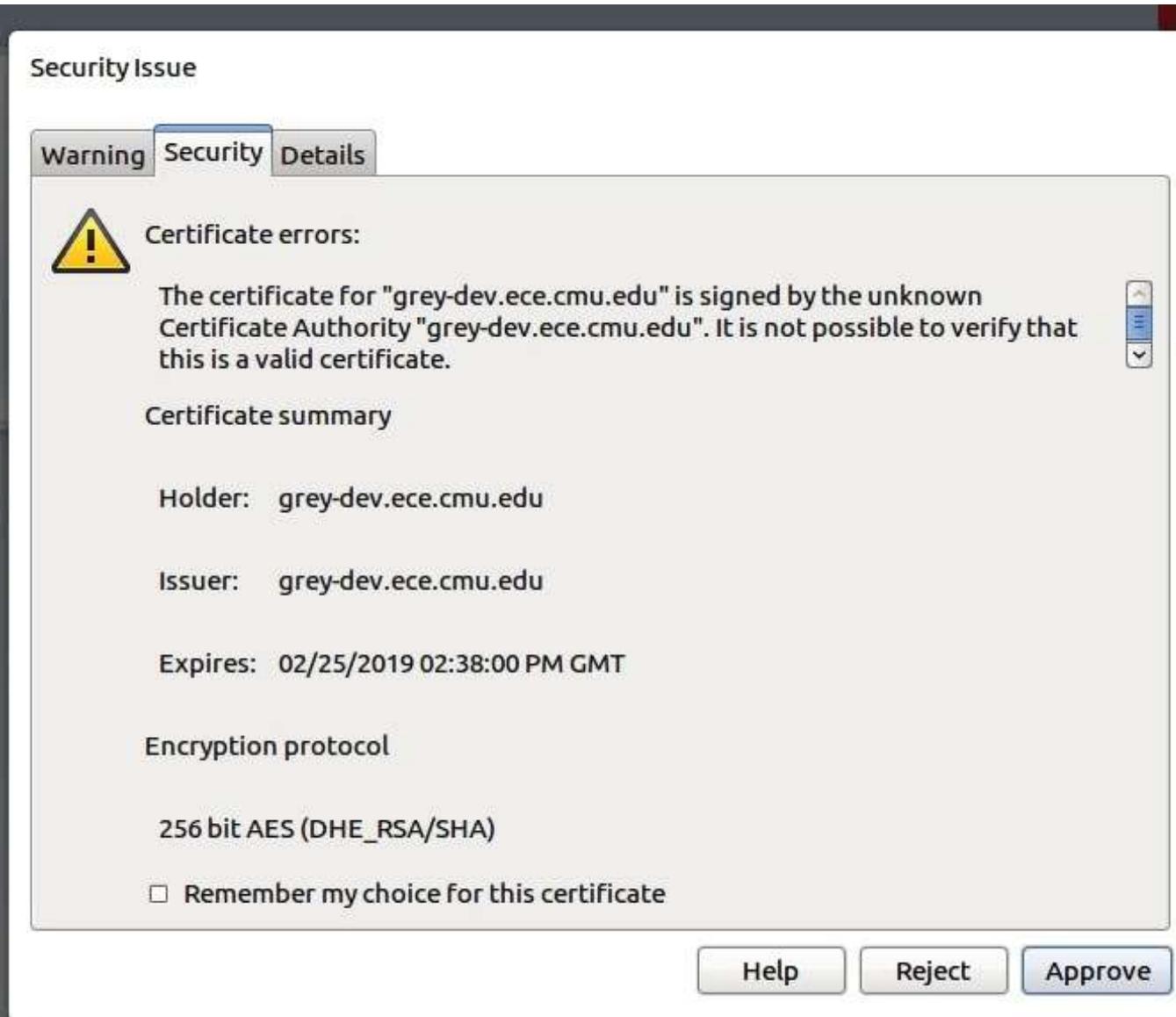
Warnings



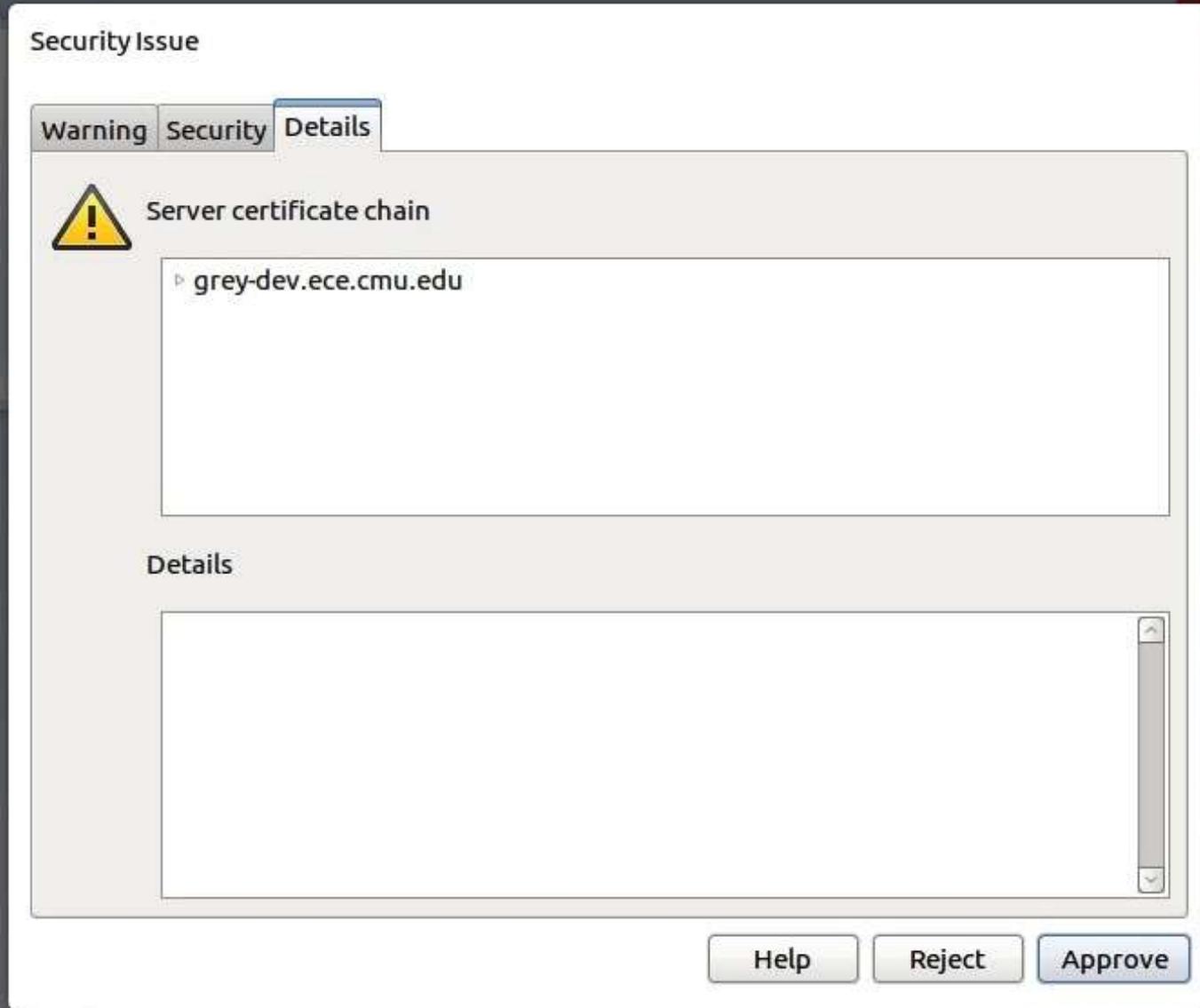
Opera



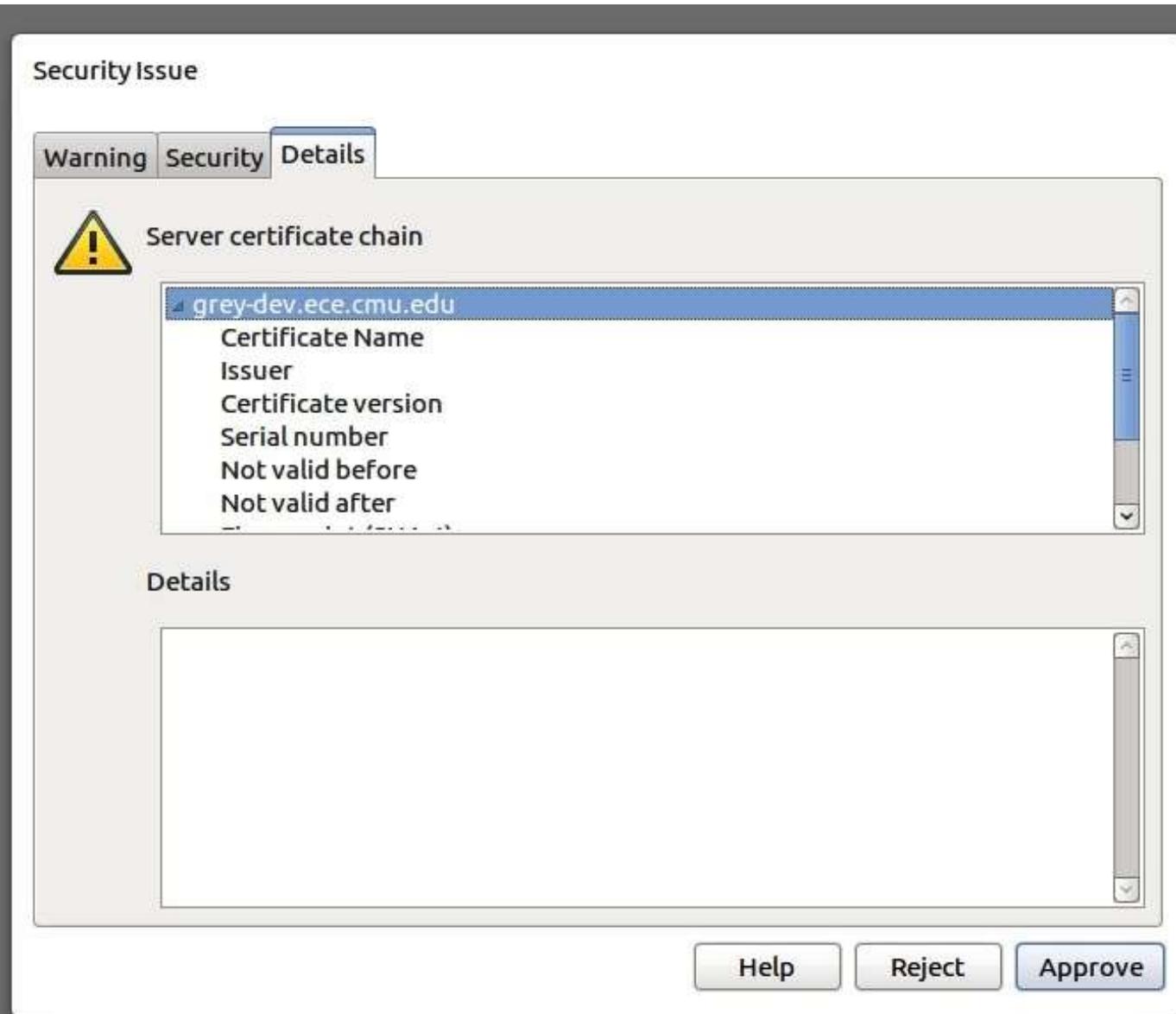
Opera



Opera



Opera



Chromium



The site's security certificate is not trusted!

You attempted to reach **grey-dev.ece.cmu.edu**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chromium cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

Proceed anyway

Back to safety

▶ [Help me understand](#)

Chromium



You attempted to reach **grey-dev.ece.cmu.edu**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chromium cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

Proceed anyway

Back to safety

▼ [Help me understand](#)

When you connect to a secure website, the server hosting that site presents your browser with something called a "certificate" to verify its identity. This certificate contains identity information, such as the address of the website, which is verified by a third party that your computer trusts. By checking that the address in the certificate matches the address of the website, it is possible to verify that you are securely communicating with the website you intended, and not a third party (such as an attacker on your network).

In this case, the certificate has not been verified by a third party that your computer trusts. Anyone can create a certificate claiming to be whatever website they choose, which is why it must be verified by a trusted third party. Without that verification, the identity information in the certificate is meaningless. It is therefore not possible to verify that you are communicating with **grey-dev.ece.cmu.edu** instead of an attacker who generated his own certificate claiming to be **grey-dev.ece.cmu.edu**. You should not proceed past this point.

If, however, you work in an organization that generates its own certificates, and you are trying to connect to an internal website of that organization using such a certificate, you may be able to solve this problem securely. You can import your organization's root certificate as a "root certificate", and then certificates issued or verified by your organization will be trusted and you will not see this error next time you try to connect to an internal website. Contact your organization's help staff for assistance in adding a new root certificate to your computer.

Mozilla Firefox



This Connection is Untrusted

You have asked Firefox to connect securely to **grey-dev.ece.cmu.edu**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

Mozilla Firefox

You have asked Firefox to connect securely to **grey-dev.ece.cmu.edu**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

▼ Technical Details

grey-dev.ece.cmu.edu uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

(Error code: sec_error_untrusted_issuer)

▼ I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...

Discuss Felt et al. 2016

- Coding process
- Scale
 - Not at all to Extremely
- Recruitment

Deploying certs more widely

- EFF's Let's Encrypt
 - <https://letsencrypt.org/>

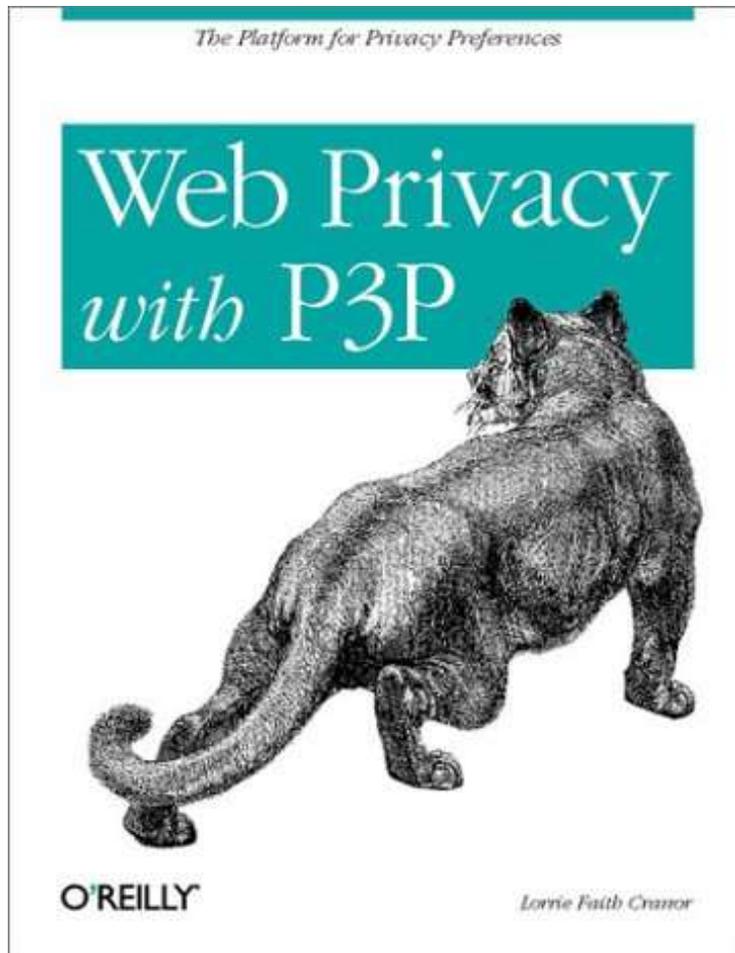
Online tracking

Online Tracking

- First party = the site you are visiting (whose address is in the URL bar)
- Third party = other sites contacted as a result of your visit to that site
- First-party tracking (e.g., for search)
 - Consider DuckDuckGo and alternatives

Online Behavioral Advertising (OBA)

Let your computer read for you



- Platform for Privacy Preferences (P3P)
- W3C specification for XML privacy policies
 - Proposed 1996
 - Adopted 2002
- Optional P3P compact policy HTTP headers to accompany cookies
- Lacks incentives for adoption



merrell primo chill slide

Search Engine: Google Yahoo! Shopping
Preference Level:



[Privacy Report](#)

Merrell Primo Chill Slide - Men's Tan: Merrell Shoes

Buy Merrell Primo Chill Slide - Men's Tan and find Spring trends at Onlineshoes. Free Shipping and Exchanges on all Merrell!...
<http://yhs.trafficdashboard.com/track.htm?pid=1031...> - [Privacy Policy](#) - [Similar Pages](#)



\$89.95



[Privacy Report](#)

merrell" Primo Chill Slide Shoes, Chocolate, Women's

Italian styled winter slide for convenience and warmth. Easy-on and water resistant, the Primo Chill gives your feet after-sport comfort in casual style. Water-resistant pigskin leather upper with sheepskin lining. Removable wool fleece footbed. Injection-molded nylon shank for increased arch support. Air Cushion EVA midsole for softer flex and increased comfort. Merrell Pilot sole with sticky rubber sports a weight-saving design that is siped and barred for traction....
<http://clickserve.cc-dt.com/link/ddiprod?lid=41000...> - [Privacy Policy](#) - [Similar Pages](#)



\$90.00



[Privacy Report](#)

Merrell Primo Chill Slide

We heated up our stylish Italian standout slide with a sheepskin lining with removable footbed and a water resistant pigskin upper. Merrell Pilot Sole has a weight-saving cutaway configuration but is boldly siped and barred for wet and dry surface traction. Slip Lasted Construction. Water Resistant Pigskin Upper. Sheepskin Lining. Wool Fleece Footbed. Nylon 6.6 Injection Molded Arch Shank. Compression Molded EVA Footframe. Air Cushion Midsole. Merrell Pilot Sole/Sticky Rubber....
<http://shopping.yahoo.com/p:Merrell%20Primo%20Chil...> - [Privacy Policy](#) - [Similar Pages](#)



\$89.95 - \$89.95



[Privacy Report](#)

Merrell Primo Chill Slide (Men's)

We heated up our stylish Italian standout slide with a sheepskin lining with removable footbed and water resistant pigskin upper. Merrell Pilot Sole has a weight-saving cutaway configuration but is boldly siped and barred for wet and dry surface traction. FEATURES: Slip Lasted Construction, Water Resistant Pigskin Upper, Sheepskin Lining, Wool Fleece Foot-Bed, Nylon 6.6 Injection Molded Arch Shank, Compression Molded EVA Foot-Frame, Air Cushion Mid-Sole, Merrell Pilot Sole/Sticky Rubber. Available Colors: Black, Chocolate, Natural, Tan. J63253....
<http://www.shoebuy.com/cgi-bin/sbref.cgi?link=yys&...> - [Privacy Policy](#) - [Similar Pages](#)



\$99.95

Merrell Shoes Primo Chill Slide - Men's

Why limit your casual winter footwear wardrobe to unimaginative, straight-laced shoes? Merrell's Primo Chill Slides offer the slip-in convenience of traditional post-sport footwear

Impact of privacy information on decision making

- Online shopping study conducted at CMU lab
- Paid participants to make online purchases with their own credit cards, exposing their own personal information
- Participants paid fixed amount and told to keep the change – real tradeoff between money and privacy
- Studies demonstrate that when readily accessible and comparable privacy information is presented in search results, many people will pay more for better privacy

J. Tsai, S. Egelman, L. Cranor, and A. Acquisti. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. WEIS 2007. <http://weis2007.econinfosec.org/papers/57.pdf>

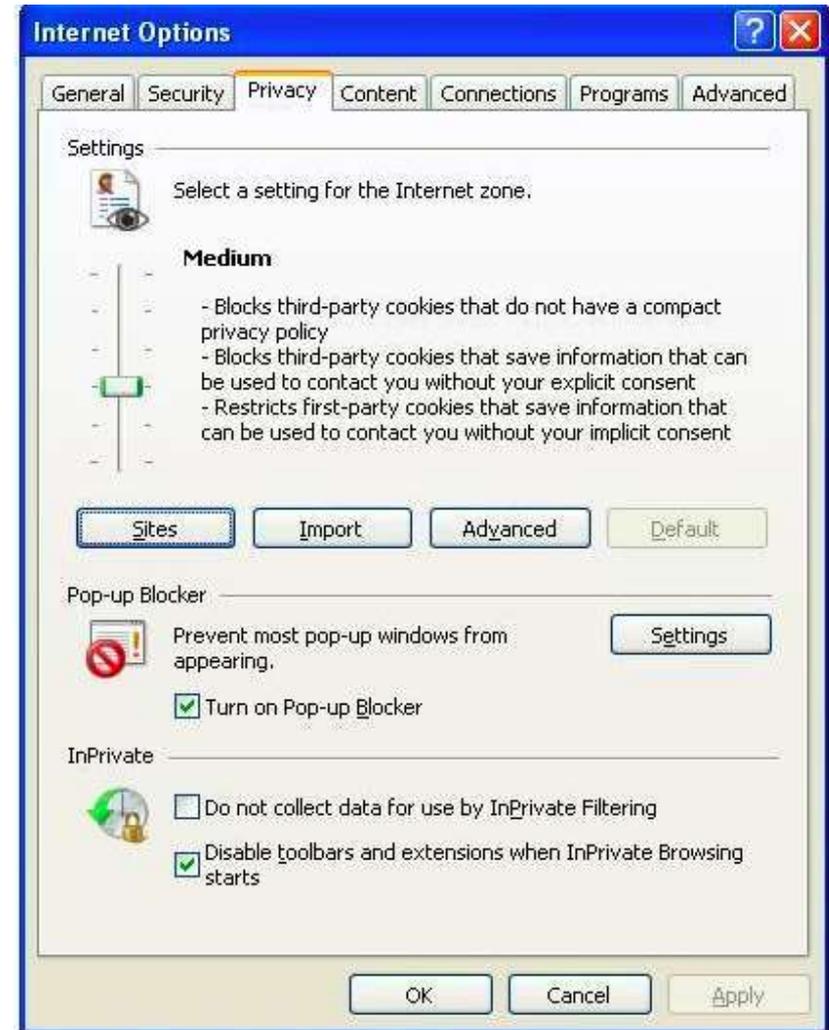
S. Egelman, J. Tsai, L. Cranor, and A. Acquisti. 2009. Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators. CHI2009. <http://www.guanotronic.com/~serge/papers/chi09a.pdf>



<http://privacyfinder.org/>

P3P in Internet Explorer

- P3P implemented in IE 6, 7, 8, 9, 10 ...
- Default privacy setting
 - Rejects third-party cookies without a CP
 - Rejects unsatisfactory third-party cookies



No P3P syntax checking in IE

- IE accepts P3P policies containing bogus tokens or missing required tokens
- Example of valid compact policy:

 **CAO DSP COR CURa ADMa DEVa OUR
IND PHY ONL UNI COM NAV INT DEM PRE**

- Examples of invalid policies accepted by IE:

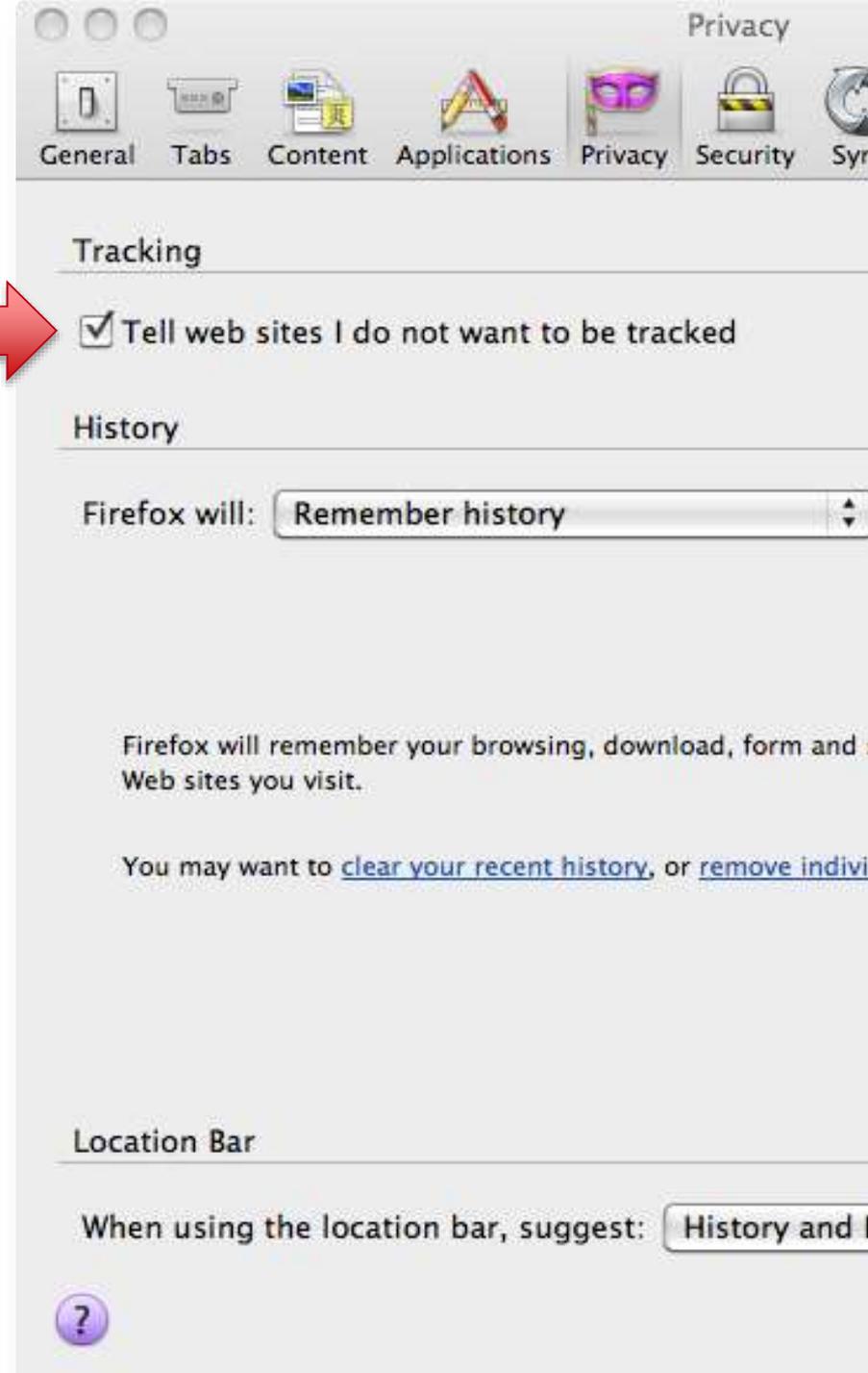
 **AMZN**

 **Facebook does not have a P3P policy.
Learn why here: <http://fb.me/p3p>**

P. Leon, L. Cranor, A. McDonald, and R. McGuire. Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens. WPES 2010.

Do not track

- Proposed W3C standard
- User checks a box
- Browser sends “do not track” header to website
- Website stops “tracking”
- W3C working group trying to define what that means



Tools to stop tracking, effective?

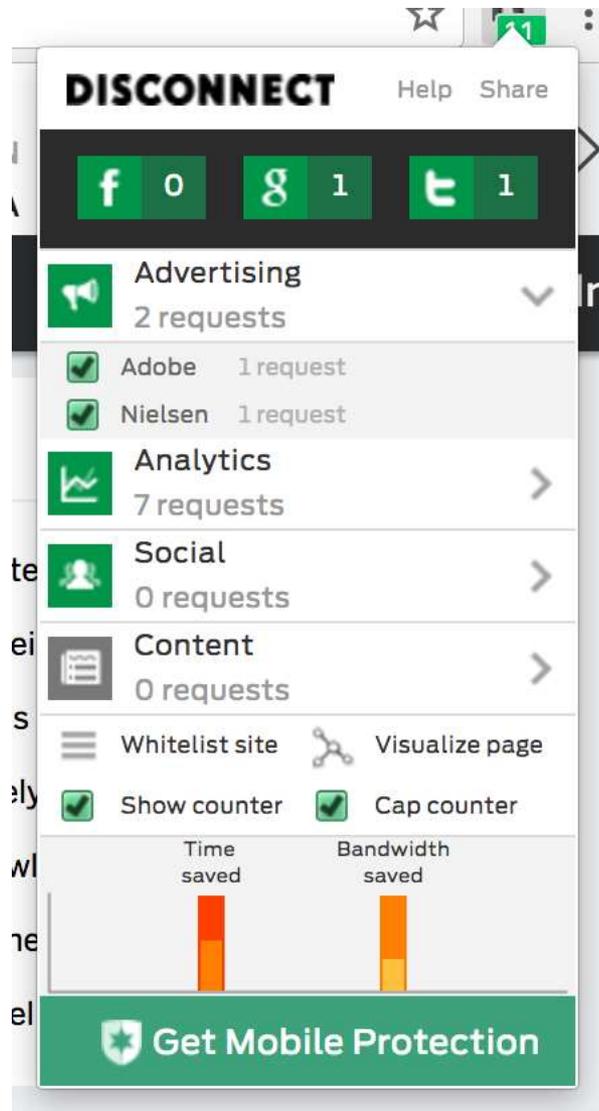
- Browser privacy settings
 - Cookie blocking
 - P3P
 - Tracking Protection Lists
 - Do Not Track
- Browser add-ons
- Opt-out cookies
- Digital Advertising Alliance (DAA) AdChoices icon and associated opt-out pages



DoNotTrackMe



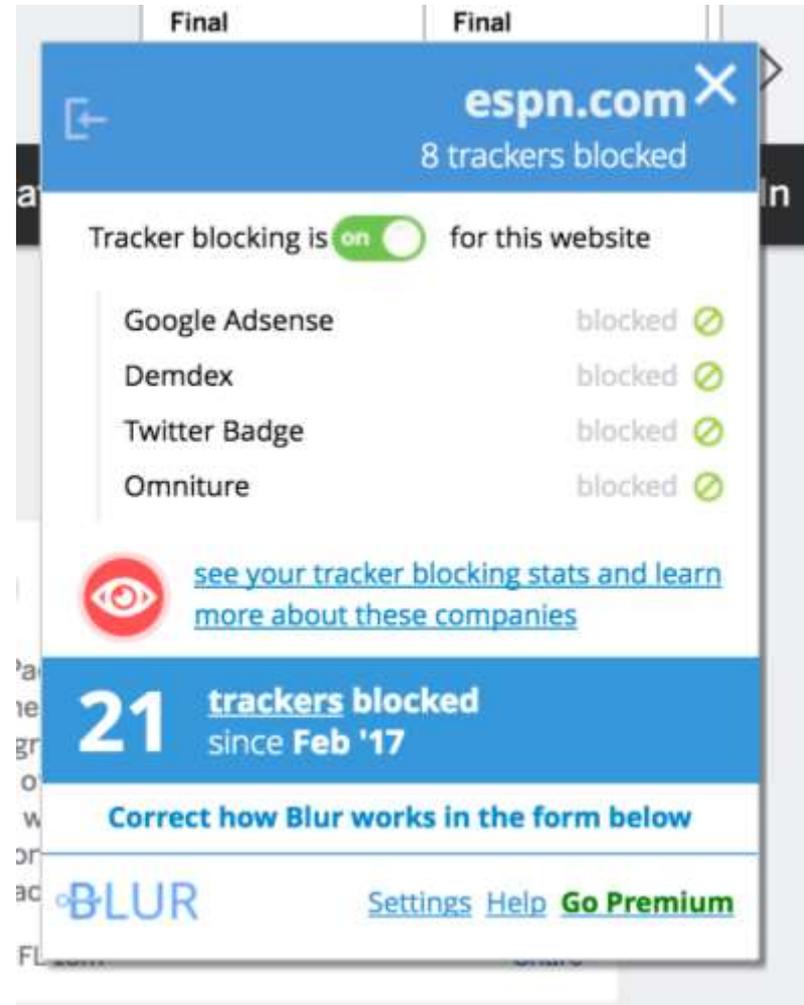
Existing Privacy Tools



The screenshot shows the Disconnect browser extension interface. At the top, it says "DISCONNECT" with "Help" and "Share" links. Below this are social media sharing buttons for Facebook (0), Google+ (1), and Twitter (1). The main interface is divided into several categories, each with a green icon and a dropdown arrow:

- Advertising**: 2 requests. Includes a list of blocked items: Adobe (1 request) and Nielsen (1 request).
- Analytics**: 7 requests.
- Social**: 0 requests.
- Content**: 0 requests.

At the bottom, there are utility options: "Whitelist site" (with a share icon), "Visualize page", "Show counter" (checked), and "Cap counter" (checked). Below these are two bar charts labeled "Time saved" and "Bandwidth saved". At the very bottom is a green button that says "Get Mobile Protection".



The screenshot shows the Blur browser extension interface on the website espn.com. The top bar is blue and says "espn.com" with a close button and "8 trackers blocked". Below this, it states "Tracker blocking is on" with a green toggle switch. A list of blocked trackers is shown:

Google AdSense	blocked	🚫
Demdex	blocked	🚫
Twitter Badge	blocked	🚫
Omniure	blocked	🚫

Below the list is a red eye icon and a link: "see your tracker blocking stats and learn more about these companies". A blue bar at the bottom of the interface says "21 trackers blocked since Feb '17". Below that is a link: "Correct how Blur works in the form below". At the bottom left is the "oBLUR" logo, and at the bottom right are links for "Settings", "Help", and "Go Premium".

Existing Privacy Tools

Privacy Badger detected 45 potential trackers on this page. These sliders let you control how Privacy Badger handles each one. You shouldn't need to adjust them unless something is broken.

weather.api.cnn.io

rtax.criteo.com

ad.doubleclick.net

googleads.g.doubleclick.net

securepubads.g.doubleclick.net

Disable Privacy Badger for This Site

Did Privacy Badger break this site? Let us know!

Donate to EFF

GHOSTERY

15 Trackers found on www.cnn.com

15

14 Blocked

Trust Site

Restrict Site

Pause Ghostery

Map These Trackers

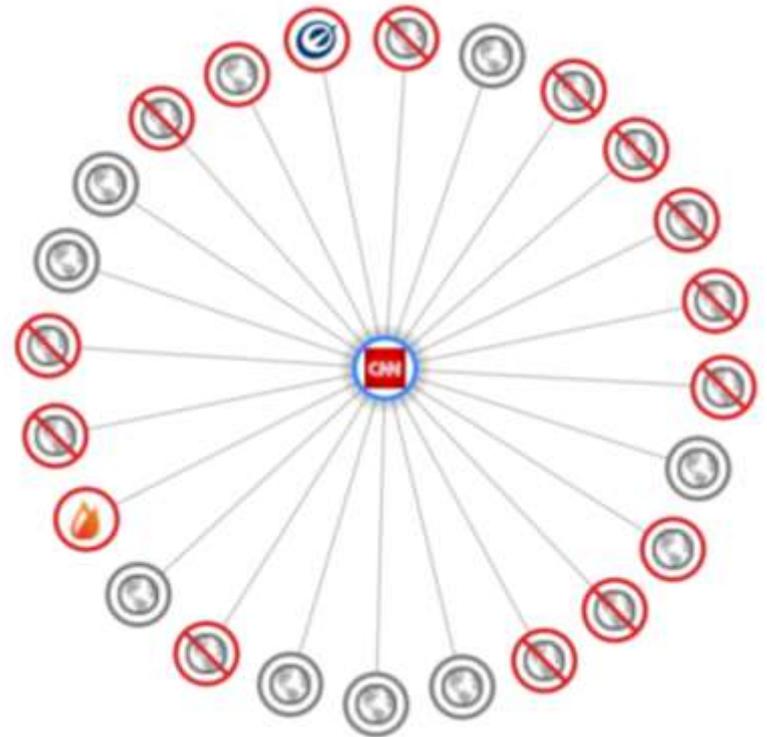
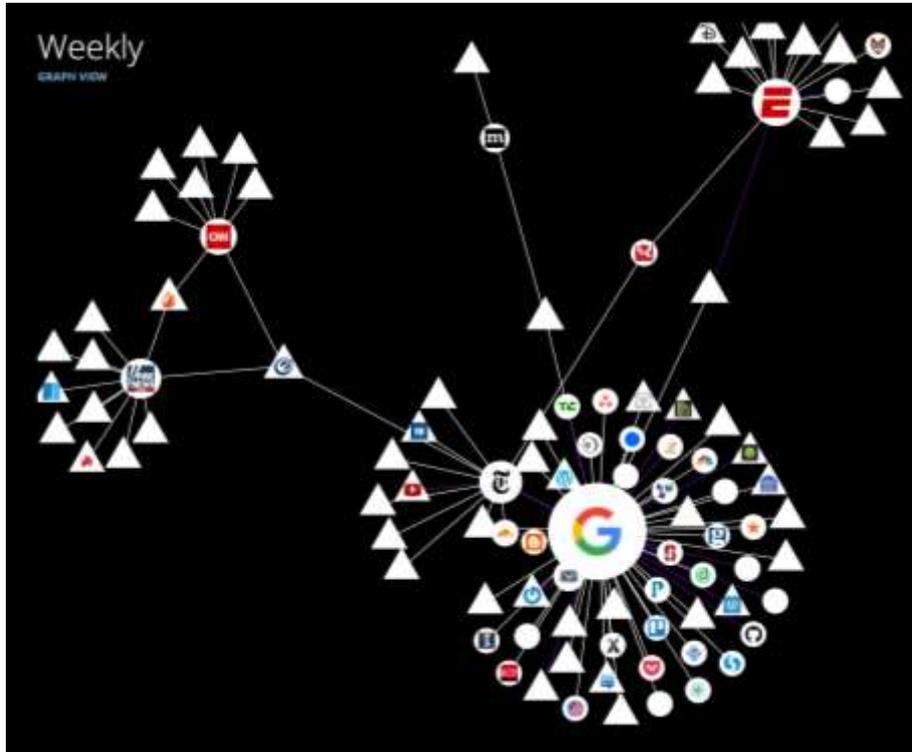
Trackers Block All

Advertising
10 Trackers 10 Blocked

- Amazon-Associates
- ChartBeat
- Criteo
- DoubleClick
- Google-Publisher-Tags
- KruX-Digital
- NetRatings-SiteCensus
- Gutbrain
- Rubicon
- ShareThrough

Site Analytics
2 Trackers 2 Blocked

Existing Tools' Connection Graphs



User study results

- Problematic defaults
- Poorly designed interfaces and jargon
- Feedback
- Misconceptions about opt-out tools
- Users unable to make meaningful decisions on a per-company basis

Pedro G. Leon, Blase Ur, Rebecca Balebako, Lorrie Faith Cranor, Richard Shay, and Yang Wang. Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising. CHI 2012.

Do people understand OBA + tools?

- Opinions about OBA mixed – both useful and creepy
- Participants did not understand OBA technologies
- Some of the worst fears based on misconceptions
- Participants did not know how to effectively exercise choice

Blase Ur, Pedro G. Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. Smart, Useful, Scary, Creepy: Perceptions of Behavioral Advertising. SOUPS 2012.

What Do Online Behavioral Advertising Disclosures Communicate to Users?

Pedro Giovanni Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. WPES 2012



AdChoices



Pop in. Stand out.

Buy Now!

TARGET P&G eStore amazon.com

AT&T.

The nation's largest 4G network.



LEARN MORE

Rethink Possible

4G speeds not available everywhere.

It's 1702, a decade after...
The Crucible's infamous seductress
danced with the devil in Salem.

MAY 4-26, 2013

Abigail
1702

BY ROBERTO AGUIRRE-SACASA
DIRECTED BY TRACY BRIGDEN

CITY THEATRE

BUY TICKETS >

YAHOO!
--- ON THE ---
ROAD

Don't miss a beat

Ad Feedback

AdChoices

The industry claims total success

“The DAA has revolutionized consumer education and choice by delivering a real-time, in-ad notice more than 10 billion times every day through the increasingly ubiquitous DAA Advertising Option Icon (also known as the ‘Ad Choices’ Icon)”



Peter Kosmala, Former Managing Director of The Digital Advertising Alliance. *Yes, Johnny Can Benefit From Transparency and Control.* November 3, 2011.

Objectives

- Evaluate the effectiveness of different OBA disclosures at communicating notice and choice about OBA
- Find ways to improve effectiveness of OBA disclosures

Methodology

- Large scale between-subjects online study
 - 1,505 participants
 - Over 100 participants per treatment
- Participants recruited through Amazon Mechanical Turk
- Guided browsing scenario
- Online survey

First exposure to OBA disclosures

HOME PAGE TODAY'S PAPER VIDEO MOST POPULAR TIMES TOPICS

Subscribe: Home Delivery / Digital Log In Register Now

Why did I get this ad? 

The New York Times

Tuesday, October 25, 2011 Last Update: 11:21 PM ET

CLICK HERE Search Follow Us    Subscribe to Home Delivery Personalize Your Weather

Switch to Global Edition

JOBS REAL ESTATE AUTOS ALL CLASSIFIEDS

WORLD U.S. POLITICS NEW YORK BUSINESS DEALBOOK TECHNOLOGY SPORTS SCIENCE HEALTH OPINION ARTS Books Movies Music Television Theater STYLE Dining & Wine Fashion & Style Home & Garden Weddings/

Europe Faces New Hurdles in Crisis Over Debt

By STEVEN ERLANGER and RACHEL DONADIO 20 minutes ago

On the eve of a European Union summit meeting, crucial financial measures were still unresolved.

- Tempers Flare as European Meeting Nears

I.B.M. Names Virginia Rometty as New Chief Executive

By STEVE LOHR 22 minutes ago

The selection of Ms. Rometty, a senior vice president at I.B.M., will make her one of the highest-profile women executives in corporate America.



Baseball's Game of Telephone

By PAT BORZI 3 minutes ago

Monday night's bullpen debacle by the Cardinals has put a new spotlight on baseball's reliance on landlines.

New Poll Finds a Deep Distrust of Government

By JEFF ZELENY and MEGAN THREE-BRENAN 3 minutes ago

With Election Day just over a year away, a deep

THE WORLD SERIES



Dilip Vishwanath for The New York Times

OPINION »

OP-ED | CLIFFORD WINSTON

Are Law Schools and Bar Exams Necessary?

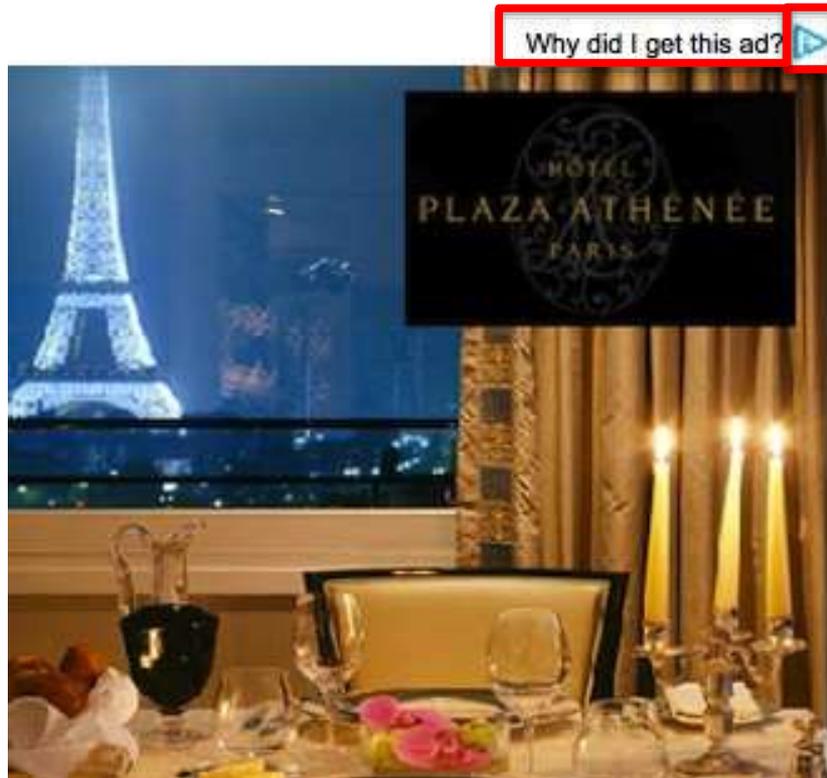
The barriers to entry for the legal industry exist to protect lawyers from competition with non-lawyers.

- Brooks: The Fighter Fallacy | Comments
- Nocera: Jobs's Biographer
- Cohen: Defending the E.U.
- Bruni: Have Glock
- Editorial: Refinancing
- Room for Debate: Will Amazon Kill Off Publishers?

Why did I get this ad? 



Second exposure to OBA disclosures

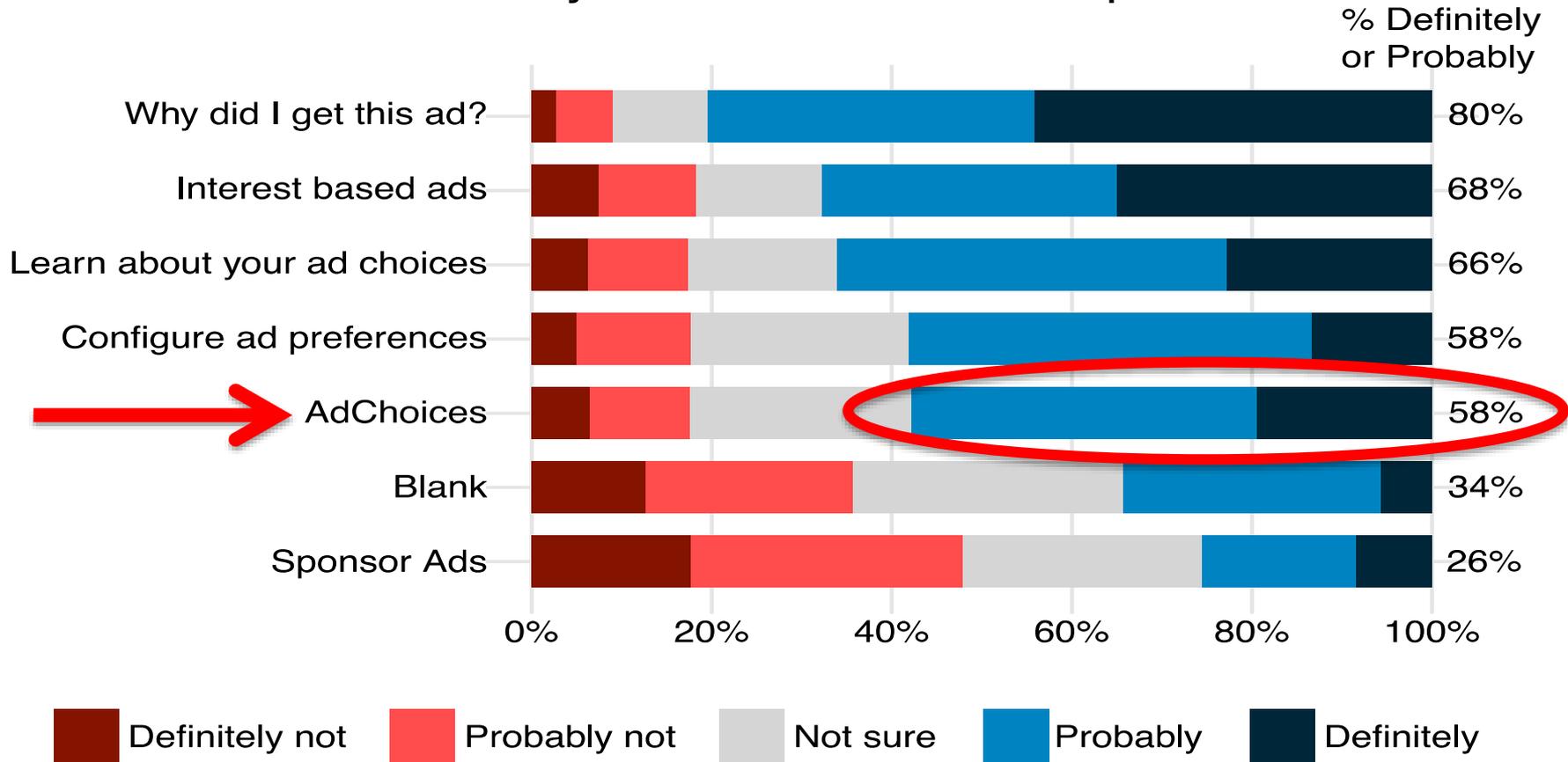


- Why did I get this ad?
- Interest based ads
- AdChoices
- Sponsor ads
- Learn about your ad choices
- Configure ad preferences
- 'No tagline'

Do icons and taglines suggest tailored ads?

- To what extent, if any, does this combination of the symbol and phrase, placed on the top right corner of the above ad suggest the following?
 - This ad has been tailored based on websites you have visited in the past. [true]

This ad has been tailored based on websites you have visited in the past



Takeaways

- OBA icons and taglines are not noticed
- “AdChoices” was outperformed by other tagline treatments at communicating notice and choice about OBA
- Users are afraid to click on icon

Browser fingerprinting

- Use features of the browser that are relatively unique to your machine
 - Fonts
 - GPU model anti-aliasing (Canvas fingerprinting)
 - User-agent string
 - *(Often not) IP address (Why not?)*

Browser fingerprinting

- <https://panopticklick.eff.org/>