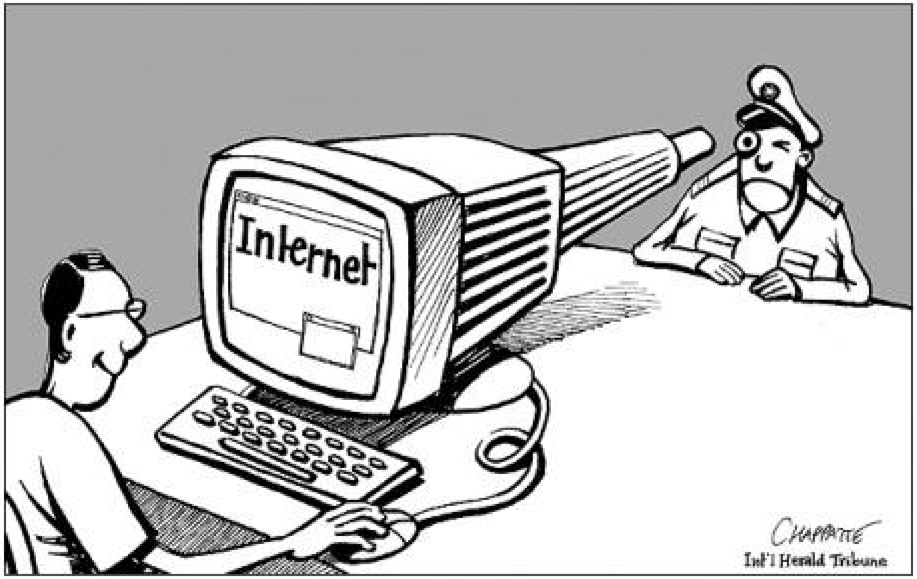
Preserving Privacy in a Connected World



Hugo Jonker
University of Luxembourg

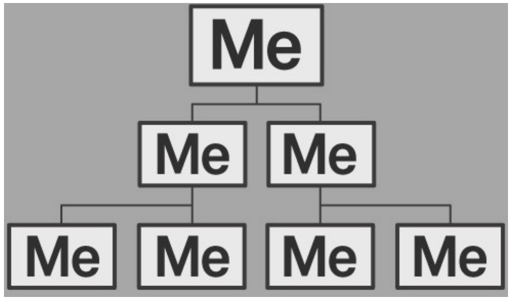
uni.lu
UNIVERSITÉ DU
LUXEMBOURG

Security and Trust of Software Systems

Background

- Former IPA student (TU/e)
- PhD thesis on Fair Sharing and Vote Privacy
- Interests:
  - vote privacy
  - healthcare privacy, e-health
  - auction verifiability & privacy
  - privacy
  - …
  - practical security

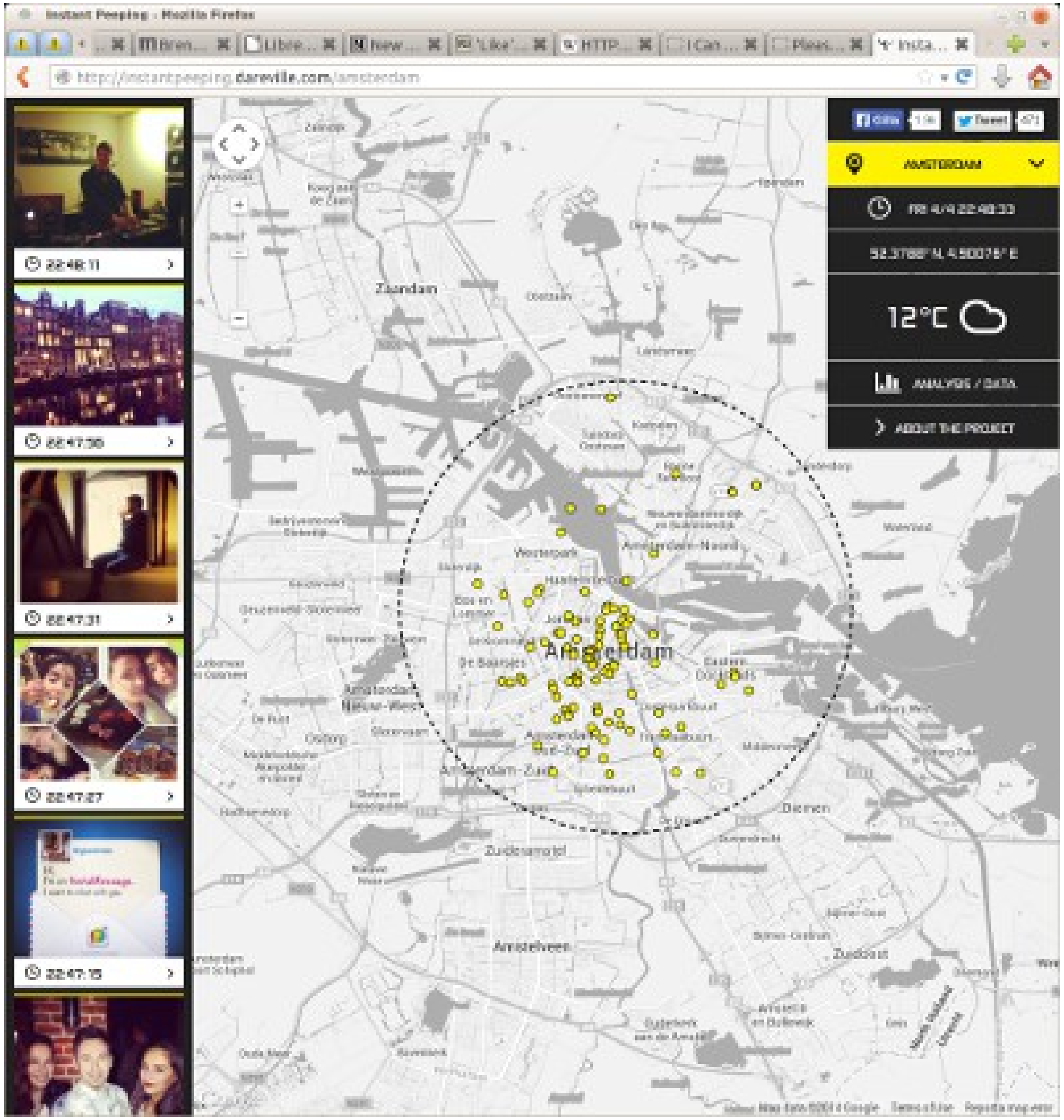
Background



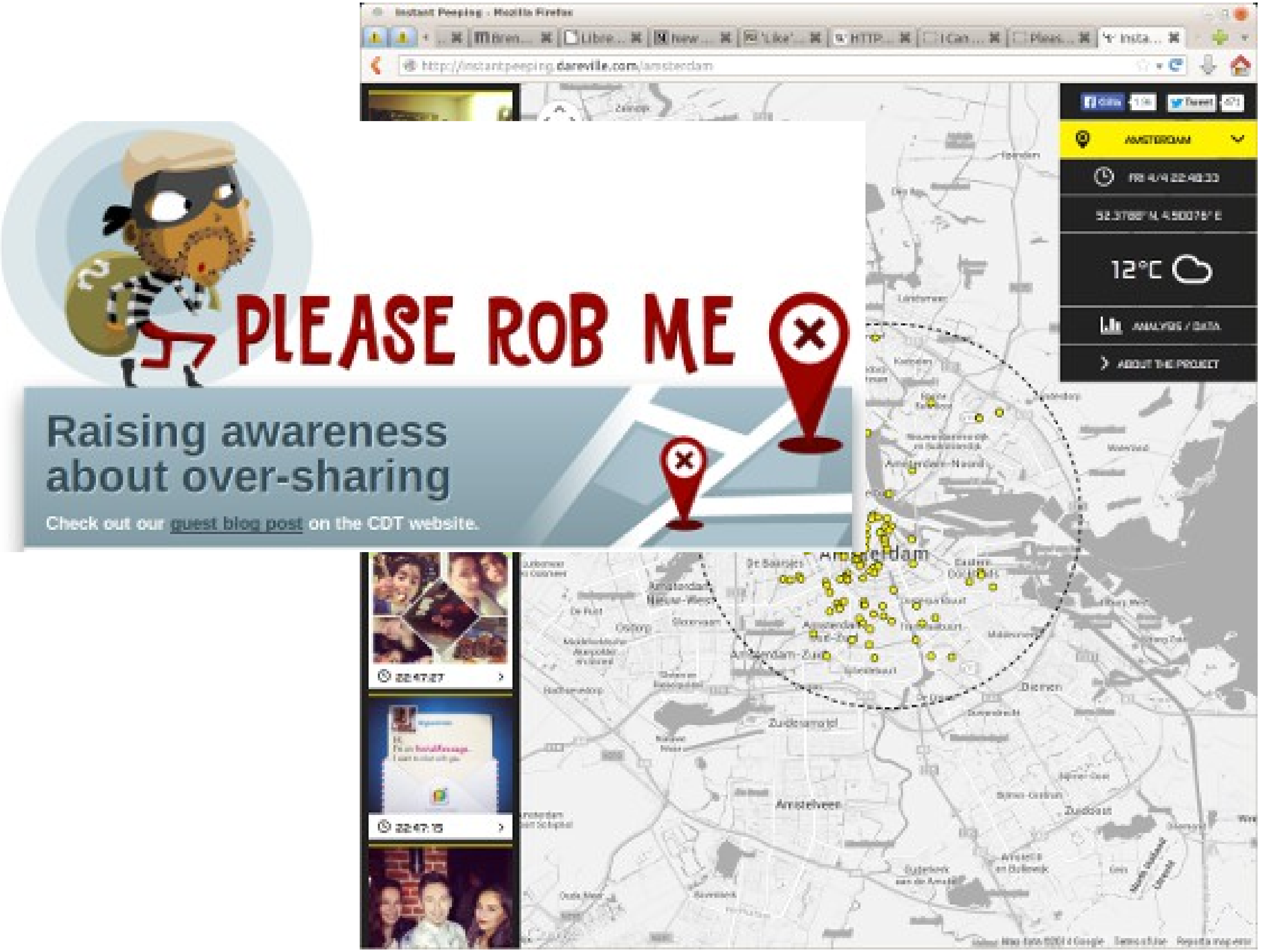
- Former IPA student (TU/e)
- PhD thesis on Fair Sharing and Vote Privacy
- Interests:
  - vote privacy
  - healthcare privacy, e-health
  - auction verifiability & privacy
  - privacy
  - …
  - practical security

We suck at privacy

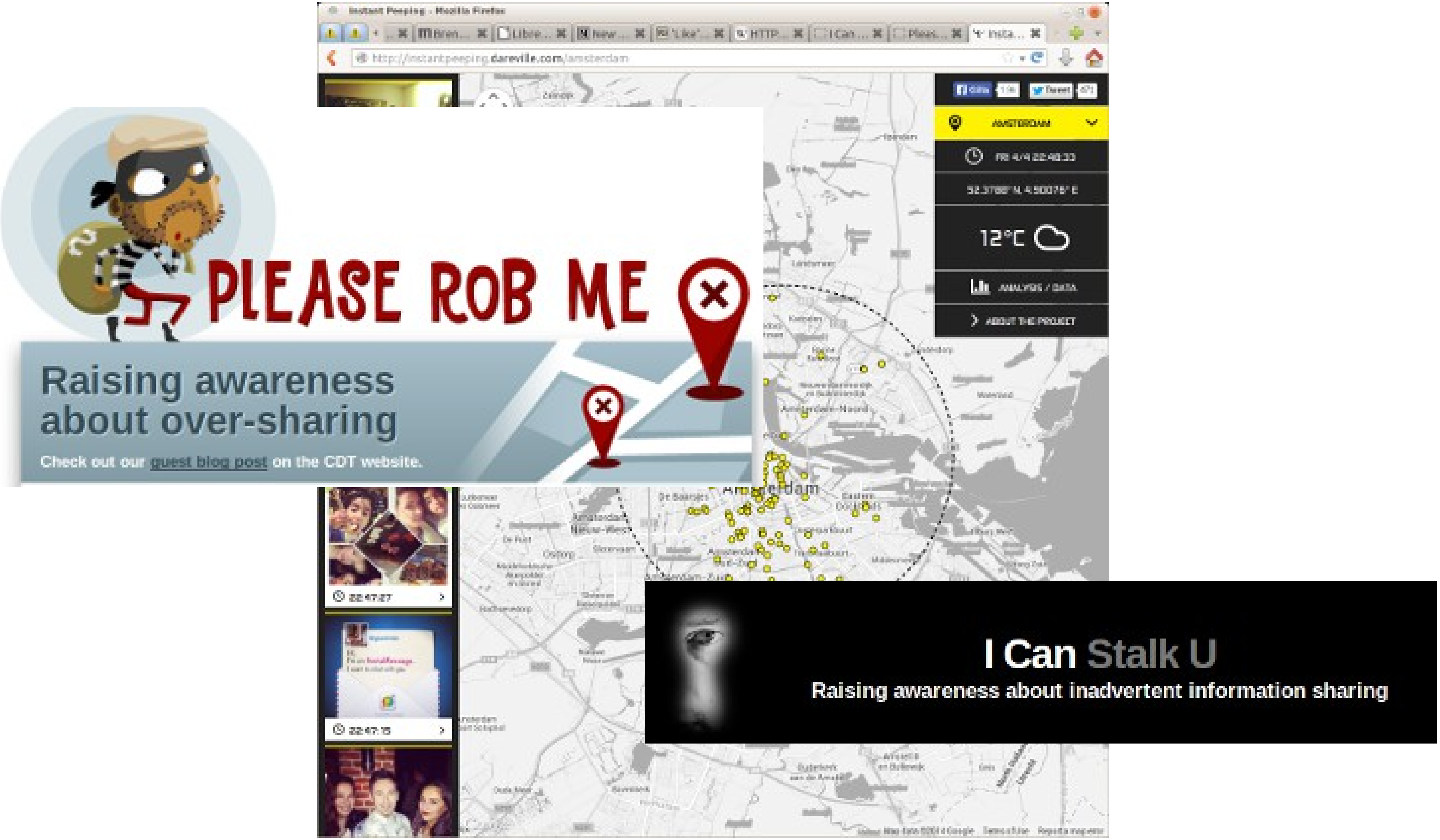
We suck at privacy



We suck at privacy


PLEASE ROB ME
Raising awareness about over-sharing
Check out our guest blog post on the CDT website.
Instant Peeping - Mozilla Firefox
http://instantpeeping.dareville.com/amsterdam
AMSTERDAM
FRI 4/4 22:48:33
52.3788° N, 4.90078° E
12°C
ANALYSIS / DATA
ABOUT THE PROJECT
22:47:27
22:47:15
Amsterdam
Amstelveen
Diemen
Zuidoost

We suck at privacy



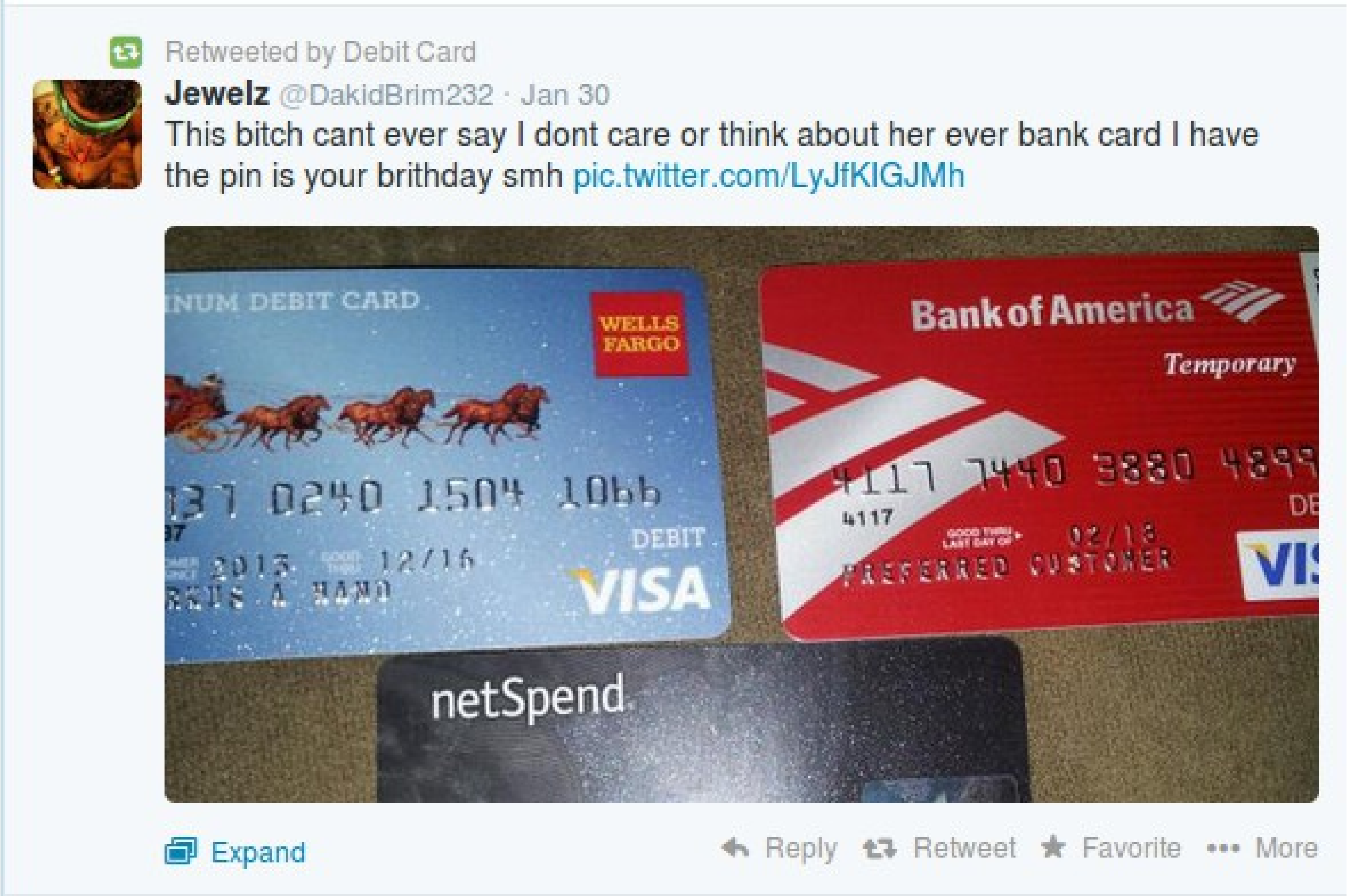
Raising awareness about over-sharing

Check out our guest blog post on the CDT website.

I Can Stalk U

Raising awareness about inadvertent information sharing

We **really** suck at privacy

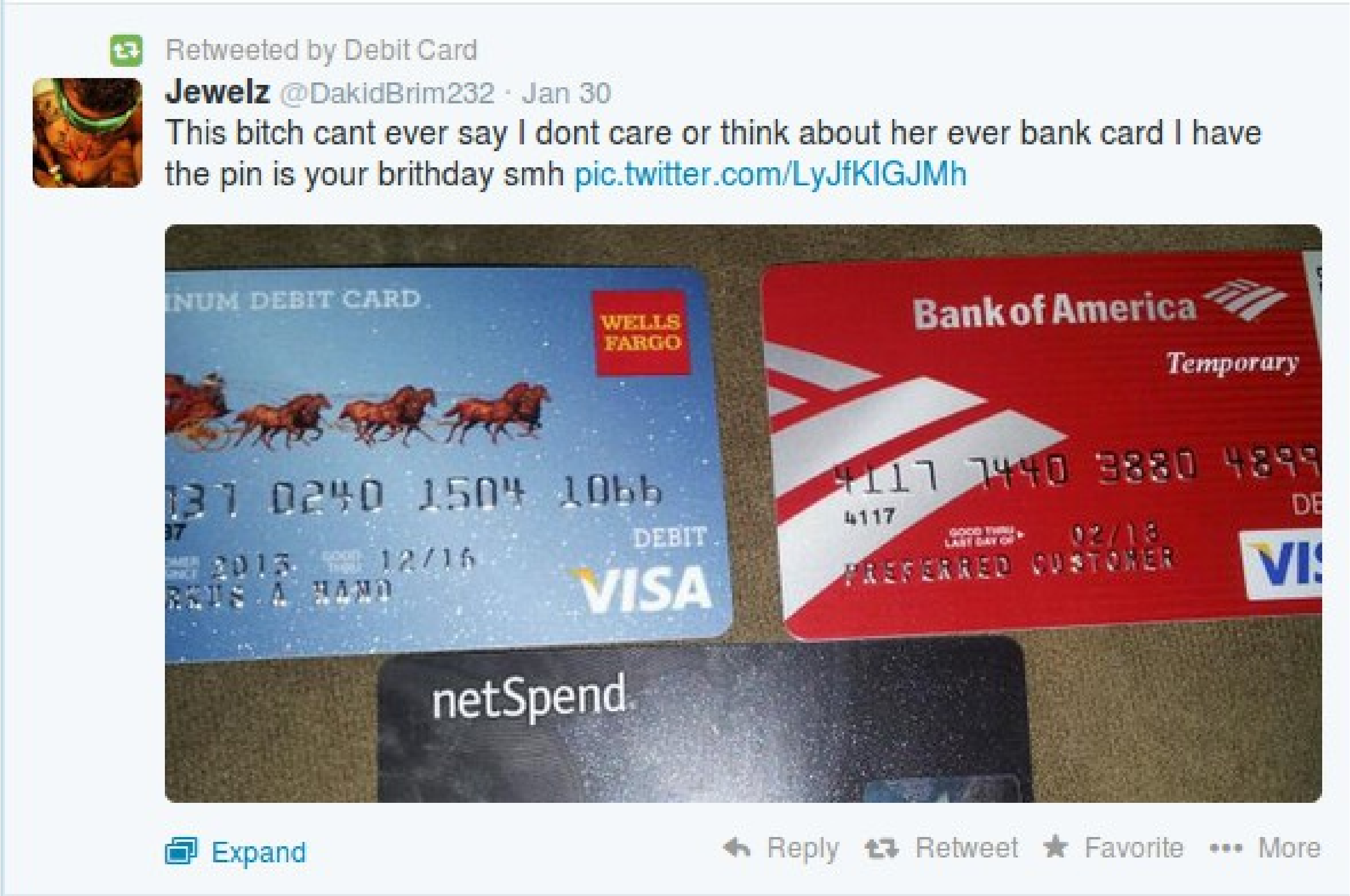


Retweeted by Debit Card

Jewelz @DakidBrim232 · Jan 30

This bitch cant ever say I dont care or think about her ever bank card I have the pin is your brithday smh pic.twitter.com/LyJfKIGJMh

We **really** suck at privacy



Retweeted by Debit Card

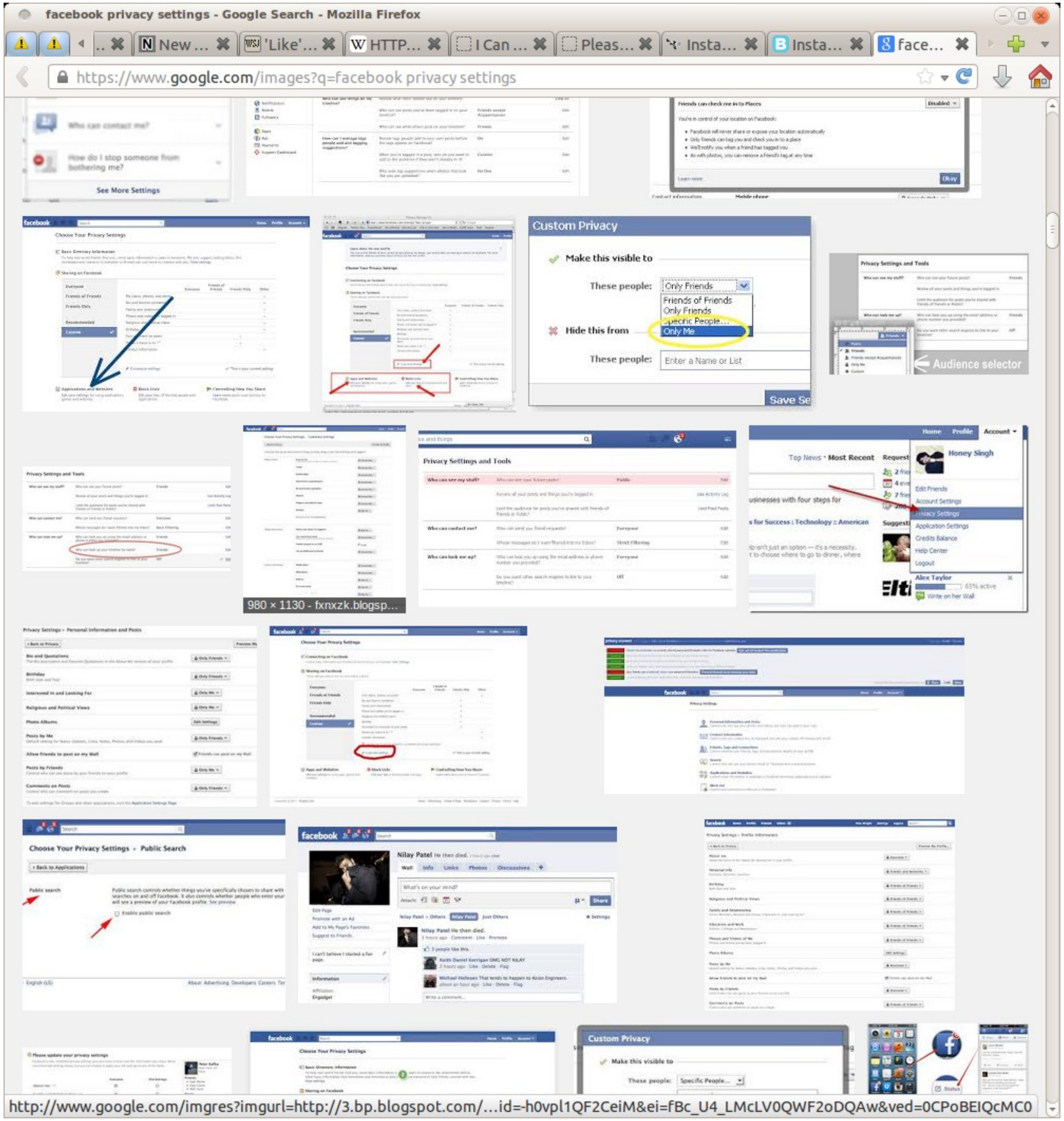
Jewelz @DakidBrim232 · Jan 30

This bitch cant ever say I dont care or think about her ever bank card I have the pin is your brithday smh pic.twitter.com/LyJfKIGJMh

Note: account number can suffice for withdrawal

Privacy is hard

Privacy is hard

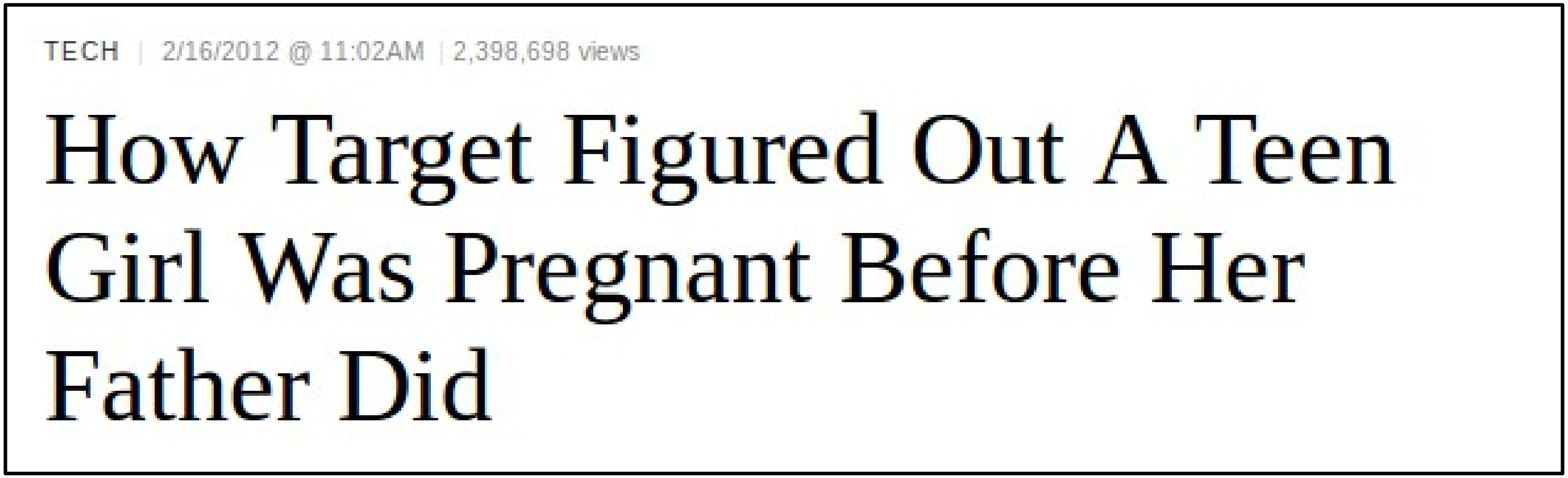

facebook privacy settings - Google Search - Mozilla Firefox
New ...
'Like'...
HTTP...
I Can ...
Pleas...
Insta...
Insta...
face...
https://www.google.com/images?q=facebook privacy settings
Custom Privacy
Make this visible to
These people: Only Friends
Friends of Friends
Only Friends
Specific People...
Only Me
Hide this from
These people: Enter a Name or List
Save Se
Audience selector
980 × 1130 - fxnxzk.blogsp...
Privacy Settings and Tools
Choose Your Privacy Settings › Public Search
See More Settings
http://www.google.com/imgres?imgurl=http://3.bp.blogspot.com/...id=-h0vpl1QF2CeiM&ei=fBc_U4_LMcLV0QWF2oDQAw&ved=0CPoBEIQcMC0

Privacy is **really** hard

“Another thing which is just an observation, when I was working on the ***blocking of the social plugins****, I always used the 👣 website to test my implementation. Today* ***Facebook suggested*** *me on my phone the* ***group of*** *👣.”*

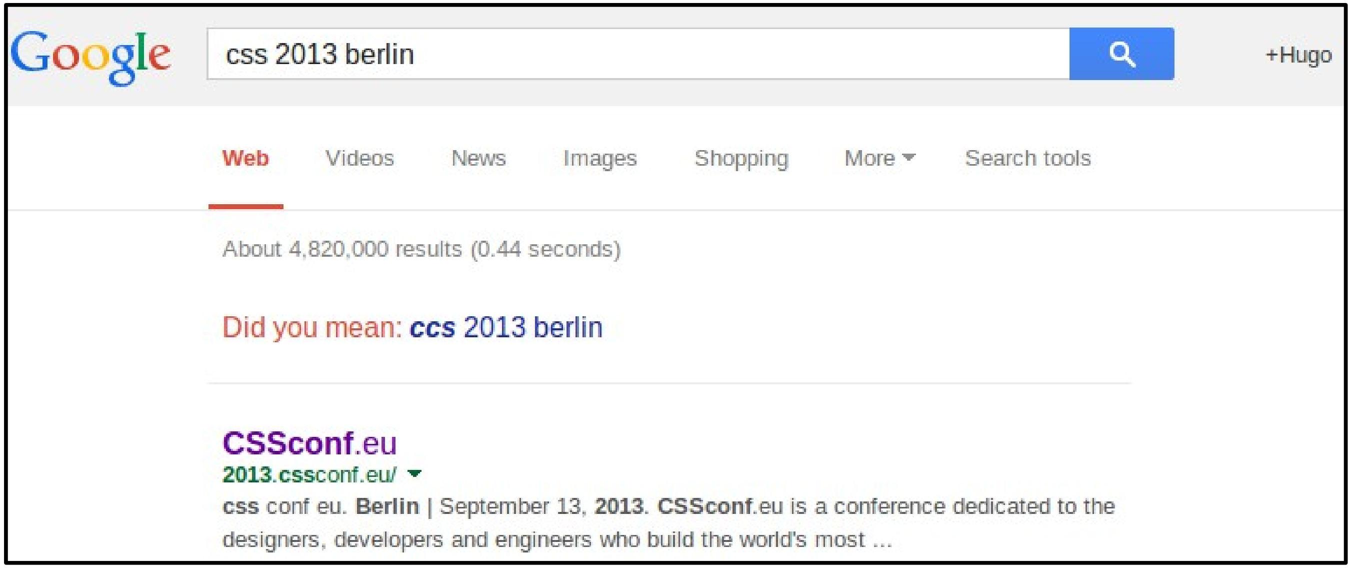
– an anonymous UL Bachelor student

Privacy is **really really** hard



TECH | 2/16/2012 @ 11:02AM | 2,398,698 views

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did



css 2013 berlin

About 4,820,000 results (0.44 seconds)

Did you mean: ***ccs*** 2013 berlin

CSSconf.eu
2013.cssconf.eu/

css conf eu. **Berlin** | September 13, **2013**. **CSSconf**.eu is a conference dedicated to the designers, developers and engineers who build the world's most ...

?

Wait, what **is** privacy?

Wait, what **is** privacy?

Good question!

Wait, what **is** privacy?

Good question!

- Privacy is wrt. someone

Wait, what **is** privacy?

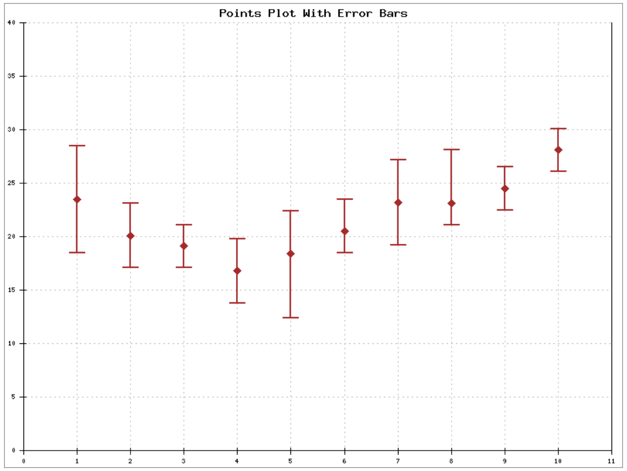
Good question!

- Privacy is wrt. someone
- Two sides:
  - (in)distinguishability

Wait, what **is** privacy?

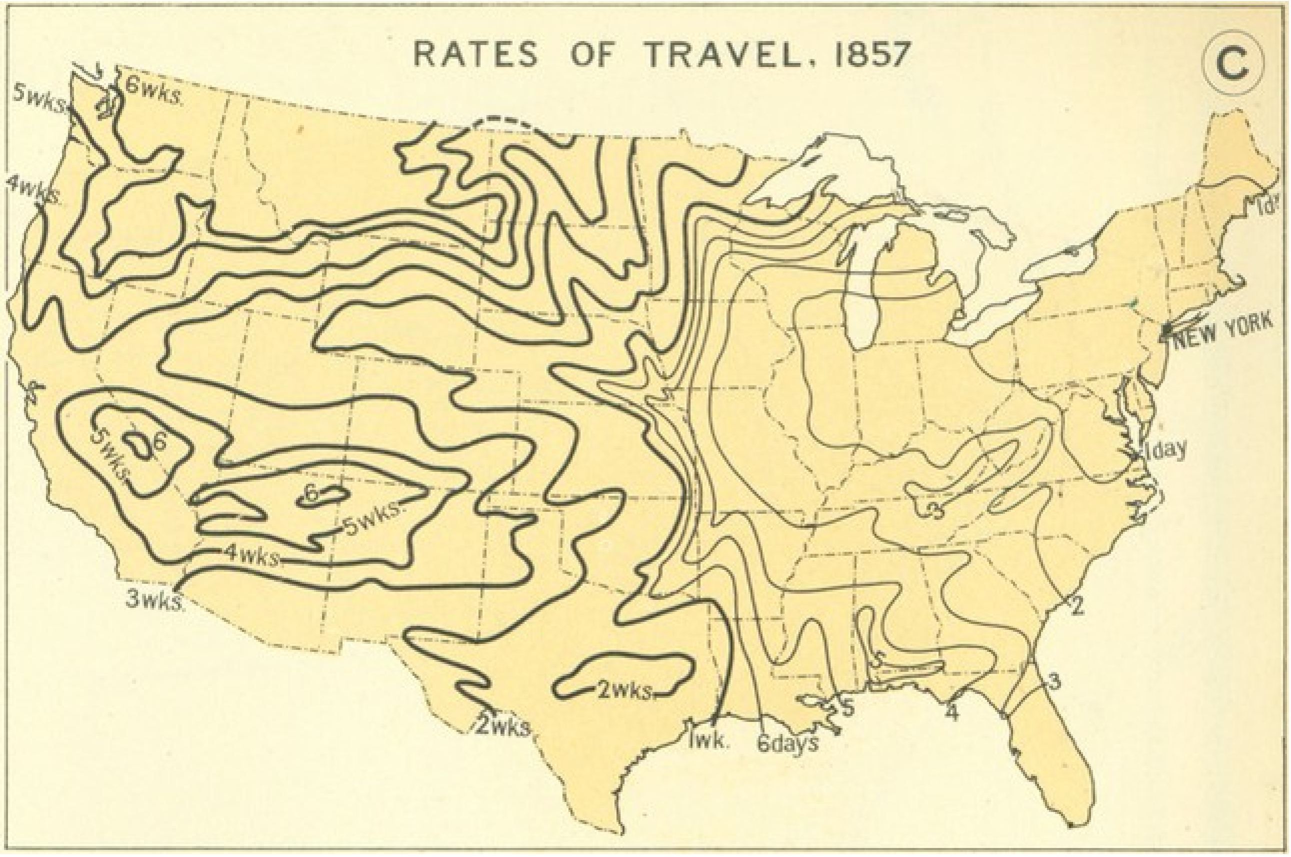
Good question!

- Privacy is wrt. someone
- Two sides:
  - (in)distinguishability
  - (un)certainty

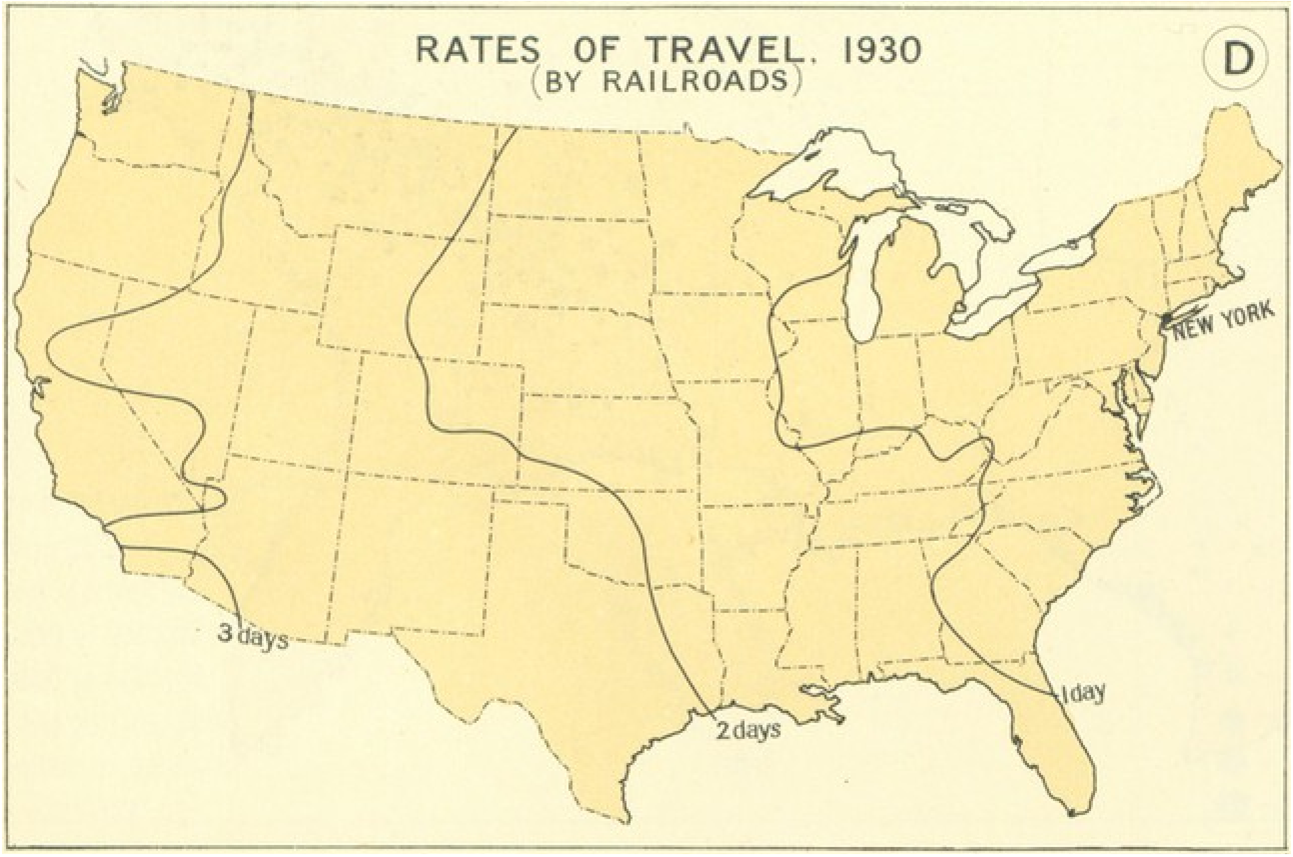


Did privacy become harder?

Did privacy become harder?



Did privacy become harder?



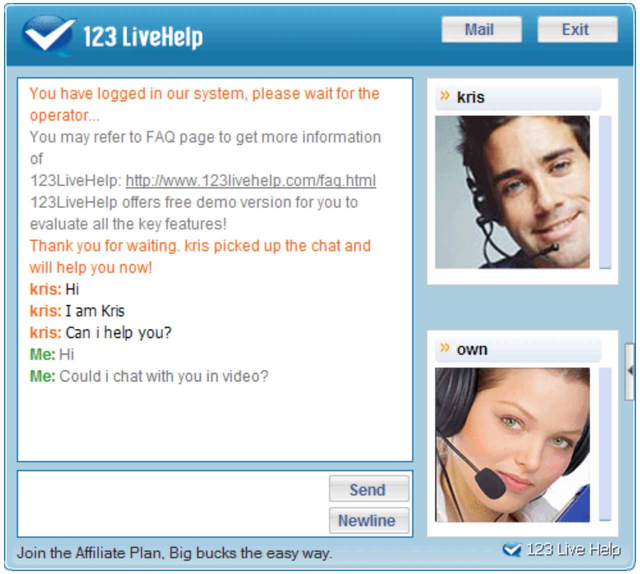
Did privacy become harder?

© Facebook

In a nutshell

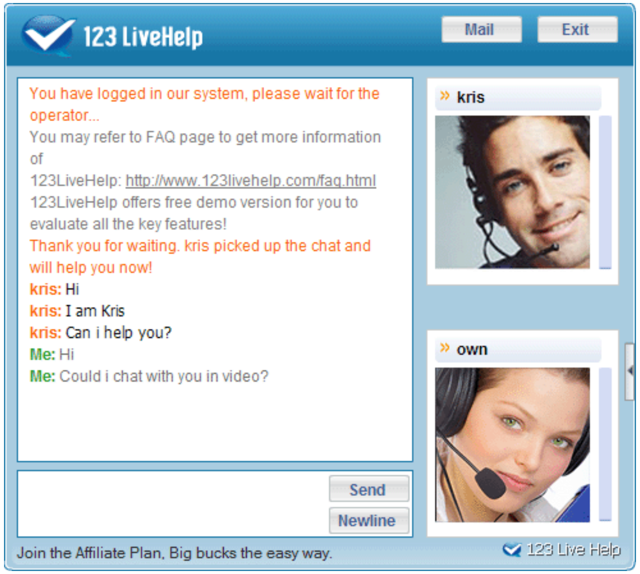
In a nutshell

In a nutshell



You have logged in our system, please wait for the operator...
You may refer to FAQ page to get more information of 123LiveHelp: http://www.123livehelp.com/faq.html
123LiveHelp offers free demo version for you to evaluate all the key features!
Thank you for waiting. kris picked up the chat and will help you now!
kris: Hi
kris: I am Kris
kris: Can i help you?
Me: Hi
Me: Could i chat with you in video?

In a nutshell



You have logged in our system, please wait for the operator...
You may refer to FAQ page to get more information of 123LiveHelp: http://www.123livehelp.com/faq.html
123LiveHelp offers free demo version for you to evaluate all the key features!
Thank you for waiting. kris picked up the chat and will help you now!
kris: Hi
kris: I am Kris
kris: Can i help you?
Me: Hi
Me: Could i chat with you in video?

Join the Affiliate Plan, Big bucks the easy way.

≈

Online privacy challenges

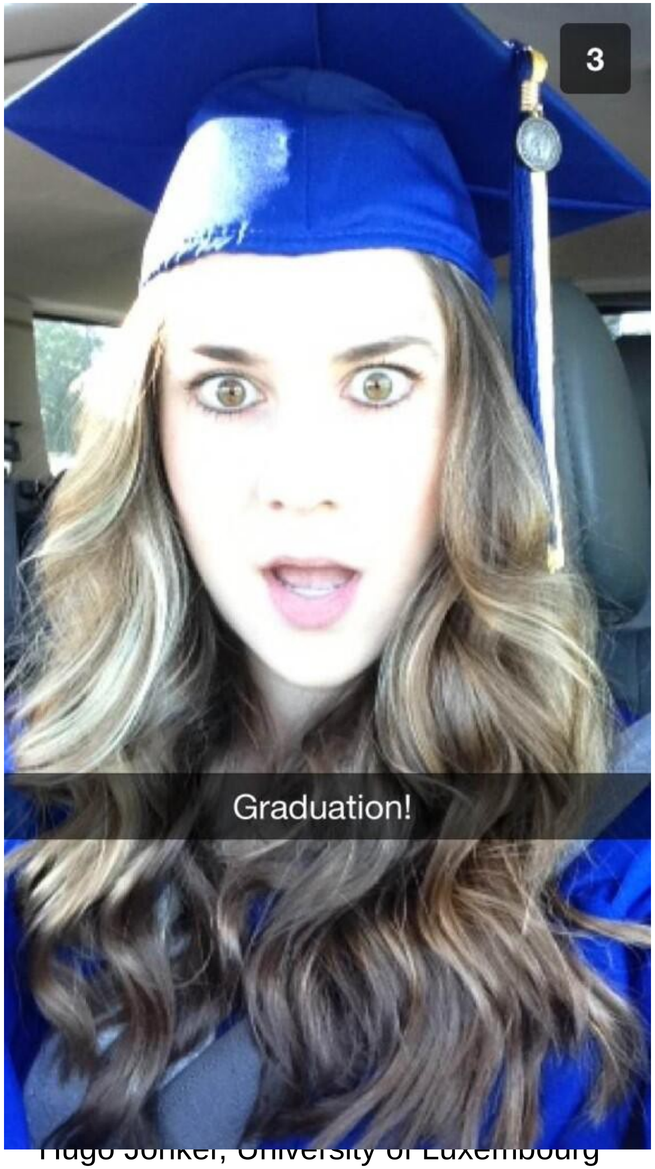
1. How to share with limits,

2. How to limit web tracking.

Sharing with limits

a case study of SnapChat

SnapChat



Graduation!

Failures of SnapChat (in 2012)

- Photos renamed, not fully removed
  a version still accessible via USB

- Photos not encrypted
  i.e. **always** accessible via USB

- ...

Beyond SnapChat

Beyond SnapChat

Obvious fixes:

Beyond SnapChat

Obvious fixes:

- really delete photos; encrypt photos

Beyond SnapChat

Obvious fixes:

- really delete photos; encrypt photos

Example applications:

Beyond SnapChat

Obvious fixes:

- really delete photos; encrypt photos

Example applications:

- selfies

Beyond SnapChat

Obvious fixes:

- really delete photos; encrypt photos

Example applications:

- selfies
- office white board photos

Beyond SnapChat

Obvious fixes:

- really delete photos; encrypt photos

Example applications:

- selfies
- office white board photos

How to control access?

Beyond SnapChat

Obvious fixes:

- really delete photos; encrypt photos

Example applications:

- selfies
- office white board photos

How to control access?

- context → privacy

Context implies privacy?

“In the office”

- Office wifi / AP
- Augmented location
  - Cell phone network
  - GPS

“work context”

- Shared: not accessible outside office
- Pic-taking device: only after passwd/unlock

Limit web tracking

Outline

- How the web works
- Tracking/fingerprinting outline
- Related work
- Thwarting ubiquitous tracking

How the web works (abstractly)

- Client-server communication:
  Server needs to know client address

- Layered structure
  - TCP/IP stack (OSI 1-6)
  - HTTP (OSI 7)
  - Browser + plugins: HTML + CSS / Java / Flash / …
  - JavaScript

HTTP

```
$ telnet facebook.com 80
HEAD /unsupportedbrowser HTTP/1.1
Host: www.facebook.com

HTTP/1.1 301 Moved Permanently
Cache-Control: private, no-cache, no-store, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Fri, 04 Apr 2014 22:37:48 GMT
Expires: Sat, 01 Jan 2000 00:00:00 GMT
Location: https://www.facebook.com/unsupportedbrowser
P3P: CP="Facebook does not have a P3P policy. Learn why here: http://fb.me/p3p"
Pragma: no-cache
Set-Cookie: datr=PDQ_UxyV3GBjiWmyk27HthOf; expires=Sun, 03-Apr-2016 22:37:48 GMT; path=/; domain=.facebook.com; httponly
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 0
X-FB-Debug: bJwsyEWZ2vw1AOhRFNOe9jSRe8+DrsC8ZMXbC6jwmpc=
Connection: keep-alive
Content-Length: 0
```

HTTP headers

Server		**Client**
• Set-cookie	↔	• Cookie
• E-tag	↔	• If-non-match
		• Referer
		• User-agent
		• Accept, Accept-*
		• DNT
		• ...

Cookies

- **Hack to add state**
- Last received cookie sent back to server

- validity:
  - Time: set by server (session, 1 yr, …)
  - Paths: set by server (path=/, path=/~user/, ...)
- can be “secure” and/or “httponly”

Why tracking?

- Find site errors / problems
- Count visitors, not pageviews
- Detect suspicious logins
- Targeted advertising

- Goal: track **a user**

How to track

- Client-side
  - Cookies
  - Evercookies/zombiecookies/...
  - History exploit
  - Active fingerprinting
- Server-side only
  - Passive fingerprinting
  - Web bugs

Zombiecookies

- Standard HTTP cookies
- Storing cookies in and reading out web history
- Storing cookies in HTTP ETags
- Internet Explorer (<9) userData storage
- HTML5 Session Storage
- HTML5 Local Storage
- HTML5 Global Storage
- HTML5 Database Storage via SQLite
- Storing cookies in RGB values of auto-generated, force-cached PNGs using HTML5 Canvas tag to read pixels (cookies) back out
- Local Shared Objects (Flash cookies)
- Silverlight Isolated Storage
- Cookie syncing scripts that function as a cache cookie and respawn the MUID cookie
- Caching in HTTP authentication
- …

Why fingerprinting?

- Cookies/zombiecookies/...: client-side storage.
- Fingerprinting:
  - Passive: infer info from server side.
  - Active: gather info from client side on-the-fly.
- Actually in use?
  - [S&P13, CCS13]: some, but not much... yet.

Related work

Privacy plugins

ABP
No
cript

...

Share this buttons [Roos11]

Share this buttons [Roos11]

- Buttons everywhere

Share this buttons [Roos11]

- Buttons everywhere
- JS code loaded from social network
  - Request will send cookie
  - Response can set / update cookie

Share this buttons [Roos11]

- Buttons everywhere
- JS code loaded from social network
  - Request will send cookie
  - Response can set / update cookie
- Facebook can track people not on FB

Share this buttons [Roos11]

- Buttons everywhere

- JS code loaded from social network
  - Request will send cookie
  - Response can set / update cookie

- Facebook can track people not on FB
- Google is worse (AdSense, Analytics)

Panopticlick [PETS10]

Panopticlick [PETS10]

- Effectiveness of fingerprinting

Panopticlick [PETS10]

- Effectiveness of fingerprinting
- Results:
  - 90% of desktop browsers **unique**
  - No JS → better results
  - Mobile → less plugins → better results

Panopticlick [PETS10]

- Effectiveness of fingerprinting
- Results:
  - 90% of desktop browsers **unique**
  - No JS → better results
  - Mobile → less plugins → better results
- Fingerprints change...

Panopticlick [PETS10]

- Effectiveness of fingerprinting
- Results:
  - 90% of desktop browsers **unique**
  - No JS → better results
  - Mobile → less plugins → better results
- Fingerprints change...
- ...predecessor found in 65% (99.1% correct)

Panopticlick [PETS10]

- Effectiveness of fingerprinting
- Results:
  - 90% of desktop browsers **unique**
  - No JS → better results
  - Mobile → less plugins → better results
- Fingerprints change...
- ...predecessor found in 65% (99.1% correct)
- Revealing: order of fonts, order of plugins

Panopticlick [PETS10]

- Effectiveness of fingerprinting
- Results:
  - 90% of desktop browsers **unique**
  - No JS → better results
  - Mobile → less plugins → better results
- Fingerprints change...
- ...predecessor found in 65% (99.1% correct)
- Revealing: order of fonts, order of plugins
- Defensive paradox

Panopticlick (2)

Test	Entropy (bits)
user-agent header	10.00
plugins	15.40
fontlist	13.90
screen resolution	4.83
supercookie test	2.12
http accept headers	6.09
timezone	3.04
cookies enabled?	0.35

Panopticlick (2)

Test	Entropy (bits)	
user-agent header	10.00	←
plugins	15.40	←
fontlist	13.90	←
screen resolution	4.83	
supercookie test	2.12	
http accept headers	6.09	
timezone	3.04	
cookies enabled?	0.35	

Panopticlick (2)

Test	Entropy (bits)	
user-agent header	10.00	←
plugins	15.40	←
fontlist	13.90	←
screen resolution	4.83	
supercookie test	2.12	
http accept headers	6.09	
timezone	3.04	
cookies enabled?	0.35	

Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.30729)

More ways to fingerprint

More ways to fingerprint

[W2SP11] – fingerprinting JavaScript implementations
Hooray for the speedwars!

More ways to fingerprint

[W2SP11] – fingerprinting JavaScript implementations
Hooray for the speedwars!

[W2SP12] – fingerprinting HTML5 font rendering
All Arials are equal... except most aren't.

More ways to fingerprint

[W2SP11] – fingerprinting JavaScript implementations
Hooray for the speedwars!

[W2SP12] – fingerprinting HTML5 font rendering
All Arials are equal... except most aren't.

[W2SP13] – fingerprinting JS engine errors.
“Foutje, bedankt.”

More ways to fingerprint

[W2SP11] – fingerprinting JavaScript implementations
Hooray for the speedwars!

[W2SP12] – fingerprinting HTML5 font rendering
All Arials are equal... except most aren't.

[W2SP13] – fingerprinting JS engine errors.
“Foutje, bedankt.”

Clock skew can be passively detected, proxies don't help.

Fighting fingerprinting

Fighting fingerprinting

- DNT header?
  Ignored or used to improve tracking.

Fighting fingerprinting

- DNT header?
  Ignored or used to improve tracking.
- FireGloves:
  - Randomise typical fingerprint attributes
  - Thwart font detection.

Fighting fingerprinting

- DNT header?
  Ignored or used to improve tracking.
- FireGloves:
  - Randomise typical fingerprint attributes
  - Thwart font detection.
  - [CCS13]: there are more ways to skin a font.

Fighting fingerprinting

- DNT header?
  Ignored or used to improve tracking.
- FireGloves:
  - Randomise typical fingerprint attributes
  - Thwart font detection.
  - [CCS13]: there are more ways to skin a font.
- Tor Browser?
  - Our best bet so far...
  - … but not perfect (eg. [CCS13])

Fighting fingerprinting

- DNT header?
  Ignored or used to improve tracking.
- FireGloves:
  - Randomise typical fingerprint attributes
  - Thwart font detection.
  - [CCS13]: there are more ways to skin a font.
- Tor Browser?
  - Our best bet so far...
  - … but not perfect (eg. [CCS13])
- Again: defensive paradox.

Defensive paradox [S&P13]

Defensive paradox [S&P13]

- Change user-agent!
  … consistent with plugins?

Defensive paradox [S&P13]

- Change user-agent!
… consistent with plugins?
- Use NoScript!
… check popular websites' JS

Defensive paradox [S&P13]

- Change user-agent!
  … consistent with plugins?
- Use NoScript!
  … check popular websites' JS

The defense can be detected … which makes you more unique.

Abstract view on tracking

Abstract view on tracking

- Tracking goal: linking two usersessions

Abstract view on tracking

- Tracking goal: linking two usersessions
- Tracker operates on OSI layer 7 (or above)

Abstract view on tracking

- Tracking goal: linking two usersessions
- Tracker operates on OSI layer 7 (or above)
- User interacts with layer 7 (or above)

Abstract view on tracking

- Tracking goal: linking two usersessions
- Tracker operates on OSI layer 7 (or above)
- User interacts with layer 7 (or above)
- Info from lower layers is passed upwards

Abstract view on tracking

- Tracking goal: linking two usersessions
- Tracker operates on OSI layer 7 (or above)
- User interacts with layer 7 (or above)
- Info from lower layers is passed upwards

i_u = (OSI_1, OSI_2, …, OSI_7, Java, flash, JS,...)

Decomposition functions

- cookie(i_u) = get-cookie(i_u.OSI$_7$)
- username(i_u) = $\begin{cases} \text{user(session(}i_u\text{))} & \text{if is\_logged\_in(}i_u\text{)} \\ \textit{empty} & \text{otherwise} \end{cases}$
- ipaddr(i_u) = get-remote-addr(i_u.OSI7)
- etc.

Linking interactions

Linking interactions

Consider interactions i_{u1} , i_{u2}

Linking interactions

Consider interactions i_{u1} , i_{u2}

- Same for FaceBook iff $i_{u1} \approx_{fb} i_{u2}$

Linking interactions

Consider interactions i_{u1} , i_{u2}

- Same for FaceBook iff $i_{u1} \approx_{fb} i_{u2}$
- Same for Google iff $i_{u1} \approx_{goog} i_{u2}$

Linking interactions

Consider interactions i_{u1} , i_{u2}

- Same for FaceBook iff $i_{u1} \approx_{fb} i_{u2}$
- Same for Google iff $i_{u1} \approx_{goog} i_{u2}$

- How is $\approx_x$ defined, for any x?

Linking interactions

Consider interactions i_{u1} , i_{u2}

- Same for FaceBook iff $i_{u1} \approx_{fb} i_{u2}$
- Same for Google iff $i_{u1} \approx_{goog} i_{u2}$

- How is $\approx_x$ defined, for any x?
- How can we ensure $\not\approx_x$?

$i_{u1} \approx_x i_{u2}$?

- $\text{username}_x(i_{u1}) = \text{username}_x(i_{u2})$ $\lor$
- $\text{cookie}_x(i_{u1}) = \text{cookie}_x(i_{u2})$ $\lor$
- … $\lor$
- $\text{fingerprint}(i_{u1}) = \text{fingerprint}(i_{u2})$ $\lor$
- $\text{match}(\text{fingerprint}(i_{u1}), \text{fingerprint}(i_{u2})) > 85\%$ $\lor$
- $i_{u1} \in \text{clickhistory}(i_{u2})$ (e.g., logging in)

$i_{u1} \not\approx_{x} i_{u2}$?

- $\text{username}_x(i_{u1}) \neq \text{username}_x(i_{u2})$, $\wedge$
- $\text{cookie}_x(i_{u1}) \neq \text{cookie}_x(i_{u2})$ $\wedge$
- … $\wedge$

- $\text{match}(\text{fingerprint}(i_{u1}), \text{fingerprint}(i_{u2})) < 12\%$

$i_{u1} \not\approx_{x} i_{u2}$?

- $\text{username}_x(i_{u1}) \neq \text{username}_x(i_{u2})$, $\wedge$
- $\text{cookie}_x(i_{u1}) \neq \text{cookie}_x(i_{u2})$ $\wedge$
- … $\wedge$

- $\text{match}(\text{fingerprint}(i_{u1}), \text{fingerprint}(i_{u2})) < 12\%$

Preventing matching ≠ ensuring non-matching!

Solution approach

Solution approach

- Cannot prevent linking when logged in

Solution approach

- Cannot prevent linking when logged in
- IP address revealed → strong link
  proxies don't help...

Solution approach

- Cannot prevent linking when logged in
- IP address revealed → strong link
  proxies don't help...

Concept:

Solution approach

- Cannot prevent linking when logged in
- IP address revealed → strong link
  proxies don't help...

Concept:

- Each website gets unique interaction

Solution approach

- Cannot prevent linking when logged in
- IP address revealed → strong link
  proxies don't help...

Concept:

- Each website gets unique interaction
- Thwart identification for 3rd party sites

Take-home message

Take-home message

- Online privacy is hard...

Take-home message

- Online privacy is hard...
- ...and therefore an interesting research area

Take-home message

- Online privacy is hard...
- ...and therefore an interesting research area

Take-home message

- Online privacy is hard...
- ...and therefore an interesting research area

- IPA-days can be more than fun [FSEN07,FI08]
- Good targets for your security papers:
  CCS, CSF, S&P, NDSS, ESORICS,Usenix Security.
- Security papers need a security analysis.

Thank you for your attention!

References (1)

[PETS10] P. Eckersley. **How unique is your web browser?** In *Proc. 10Th Privacy Enhancing Technologies Symposium (PETS'10)*, LNCS 6205, pp. 1-18. Springer, 2010.

[CCS13] G. Acar, M. Juarez, N. Nikiforakis, C. Diaz, S. Gürses, F. Piessens, B. Preneel. **FPDetective: dusting the web for fingerprinters**. In *Proc. 20Th Conference on Computer & Communications Security (CCS'13),* pp. 1129-1140. ACM.

[W2SP11] K. Mowery, D. Bogenreif, S. Yilek, H. Shacham. **Fingerprinting information in JavaScript implementations**. In *Proc. 2nd Web 2.0 Security and Privacy (W2SP'11)*.

[W2SP12] K. Mowery, H. Shacham. **Pixel Perfect: Fingerprinting Canvas in HTML5**. In *Proc. 3rd Web 2.0 Security and Privacy (W2SP'12)*.

[W2SP13] M. Mulazzani, P. Reschl, M. Huber, M. Leithner, S. Schrittwieser, E. Weippl. **Fast and reliable browser identification with Javascript engine fingerprinting**. In *Proc. 3rd Web 2.0 Security and Privacy (W2SP'13)*.

References (2)

[FSEN07] M. Torabi Dashti, S. Krishnan Nair, H.L. Jonker. **Nuovo DRM Paradiso: Towards a Verified Fair DRM Scheme.** In *Proc. 1st International Symposium on Fundamentals of Software Engineering (FSEN’07)*, Springer-Verlag, LNCS 4767, pp. 33-48, 2007.

[FI08] M. Torabi Dashti, S. Krishnan Nair, H. Jonker. **Nuovo DRM Paradiso: Designing a Secure, Verified, Fair Exchange DRM Scheme.** *Fundamenta Informaticae*, 89(4):393–417, 2008.

[Roos11] A. Roosendaal. **Facebook Tracks and Traces Everyone: Like This!**. Tilburg Law School Research Paper No. 03/2011.

[S&P13] N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens,G. Vigna. **Cookieless monster: Exploring the ecosystem of web-based device fingerprinting.** In *Proc. 34th Symposium on Security and Privacy (SP'13)*, pp. 541-555. IEEE, 2013.