“This is your last chance, kid. Honest people don't have anything to hide.”

Don’t they?
“But what if I decreed that from now on, every time you went to evacuate some solid waste, you'd have to do it in a glass room perched in the middle of Times Square, and you'd be buck naked?”

“[Privacy is] about your life belonging to you.”
The right to whisper.
keep prices low with Baby on the go

save with $27 in coupons

Expires September 5, 2009

Use our valuable coupons to save on everything Baby needs for mealtime, changing time and bath time—in no time.
How do we lose privacy?
https://duckduckgo.com/?q=nsa+spying
Chirp! Chirp! Chirp! Chirp! <³ LoL #funnybirdnoises wtf!?
John McAfee knows about metadata.
For example:

http://freegeoip.net/

IP: 207.38.152.228
Location: 40.7143, -74.006

IP: 166.84.7.99
IP: 207.38.152.228
Location: 40.7143, -74.006
Time: 25/Aug/2013:20:50:41 -0400

IP: 166.84.7.99
IP: 207.38.152.228
Location: 40.7143, -74.006
Time: 25/Aug/2013:20:50:41 -0400
Request: /blog/images/implied-facepalm.jpg

IP: 166.84.7.99
IP: 207.38.152.228
Location: 40.7143, -74.006
Time: 25/Aug/2013:20:50:41 -0400

Request: /blog/images/implied-facepalm.jpg
User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:23.0) Gecko/20100101 Firefox/23.0

IP: 166.84.7.99
IP: 207.38.152.228
Location: 40.7143, -74.006
Time: 25/Aug/2013:20:50:41 -0400

Request: /blog/images/implied-facepalm.jpg
User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:23.0) Gecko/20100101 Firefox/23.0


IP: 166.84.7.99
IP: 207.38.152.228
Location: 40.7143, -74.006
Time: 25/Aug/2013:20:50:41 -0400
Request: /blog/images/implied-facepalm.jpg
User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:23.0) Gecko/20100101 Firefox/23.0
IP: 166.84.7.99
Coooookies.
Like us on facebook for a chance to win a FREE Lunch.
Now What?!!
Cryptography may provide:

Cryptography *may* provide:

Confidentiality

Cryptography *may* provide:

Confidentiality

Integrity

Cryptography may provide:

Confidentiality
Integrity
Authenticity

Cryptography may provide:

Confidentiality
Integrity
Authenticity

Security is HARD.

What are we protecting?
Who are we protecting it from?
Who or what can defeat our solution?
What are we still leaking?
Can we do better?

http://youtu.be/NO0cvqT1tAE
Low hanging fruit first.
Default to HTTPS.
Default to HTTPS.

Many sites (Twitter, Facebook, Gmail, ...) already default to HTTPS.
Default to HTTPS.

Many sites (Twitter, Facebook, Gmail, ...) already default to HTTPS.

Dig in preferences for ‘Enable SSL by default’ or similar setting.
Default to HTTPS.

Many sites (Twitter, Facebook, Gmail, ...) already default to HTTPS.

Dig in preferences for ‘Enable SSL by default’ or similar setting.

Use the EFF’s ‘HTTPS-Everywhere’ browser plugin: https://www.eff.org/https-everywhere
Authentication

The identity of Twitter, Inc. at San Francisco, California US has been verified by VeriSign Class 3 Extended Validation SSL CA.

Certificate Information

Your connection to twitter.com is encrypted with 128-bit encryption.

The connection uses TLS 1.2.

The connection is encrypted using RC4_128, with SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism.

New to Twitter? Sign up

Full name
Email
Password

Sign up for Twitter

https://youtu.be/iQsKdtjwYI

@jschauma

Wednesday, September 4, 13
Integrity
Confidentiality
Authentication
Security is HARD.

What are we protecting?
Who are we protecting it from?
Who or what can defeat our solution?
What are we still leaking?
Can we do better?

https://youtu.be/NO0cvqT1tAE
HTTPS protects data in transit.

IP: 207.38.152.228
Location: 40.7143, -74.006
Time: 25/Aug/2013:20:50:41 -0400


User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:23.0) Gecko/20100101 Firefox/23.0

IP: 166.84.7.99
HTTPS protects data in transit.
Milestones in the History of Human Toilet Use

Toilet paper invented in Sui Dynasty China

AD 600

Sir John Harrington invents the flush toilet

1596

Thomas Crapper popularizes indoor plumbing

1860s

Twitter

2006

https://t.co/iOf6M1xSoO
“If you are not paying for it, you’re not the customer - you’re the product being sold.”
Where I come from...

<table>
<thead>
<tr>
<th>Preference Name</th>
<th>Status</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>network.http.sendRefererHeader</td>
<td>user set</td>
<td>integer</td>
<td>0</td>
</tr>
</tbody>
</table>

http://nullreferrer.com/

@jshauma

Wednesday, September 4, 13
Where I come from...

...is really none of your business.
Control your cookie consumption!

https://t.co/PHDdu91aDP
@jschauma

Private Browsing

Wednesday, September 4, 13
Private Browsing

- Always use private browsing mode
- Accept third-party cookies: Never
Private Browsing

https://www.eff.org/issues/do-not-track
Time: 25/Aug/2013:20:50:41 -0400
Location: 40.7143, -74.006
IP: 207.38.152.228
Block trackers:

https://www.abine.com/dntdetail.php
https://twitter.com/abine

https://www.ghostery.com/
https://twitter.com/ghostery
Top sites are covertly cramming cookies down users' throats

Two new studies show top sites let hundreds of different third parties track customers' online behavior -- and most violate common privacy standards
Top sites are covertly cramming cookies down users' throats

Two new studies show top sites let hundreds of different third parties track customers' online behavior -- and most violate common privacy standards

By Ted Samson | InfoWorld

Most Popular

- 11 things Microsoft is actually doing right
- 12 terrific new updates in VMware vSphere 5.5
- Why Microsoft .Net failed
- A first, jaundiced look at Windows 8.1 RTM
- Top 10 Amazon cloud challengers

Recent Posts

- A first, jaundiced look at Windows 8.1 RTM

https://t.co/DiMYreMHPX
Quis custodiet ipsos custodes?

Tracking helps the digital marketplace work better.

It just needs to be fully transparent so you can manage it effectively.

Try out the Evidon TrackerMap™ now.

https://t.co/SgLGkKUxtF
Chrome Settings

Privacy

- Use a web service to help resolve navigation errors
- Use a prediction service to help complete searches and URLs typed in the address bar
- Predict network actions to improve page load performance
- Enable phishing and malware protection

Web content

- Font size: Medium
- Page zoom: 100%

Network

@jschauma

https://t.co/vTufUSJUkO

Wednesday, September 4, 13
Quis custodiet ipsos custodes?

How does Phishing and Malware Protection work in Firefox?

Phishing and Malware Protection works by checking the sites that you visit against lists of reported phishing and malware sites. These lists are automatically downloaded and updated every 30 minutes or so when the Phishing and Malware Protection features are enabled.

[...]

Before blocking the site, Firefox will request a double-check to ensure that the reported site has not been removed from the list since your last update. In both cases, existing cookies you have from google.com, our list provider, may also be sent.
Panopticlick
How Unique — and Trackable — Is Your Browser?

Your browser fingerprint appears to be unique among the 3,334,454 tested so far.

https://panopticlick.eff.org/
Panopticlick
How Unique — and Trackable — Is Your Browser?

Your browser fingerprint appears to be unique among the 3,334,454 tested so far.

https://panopticlick.eff.org/
So... what are we still leaking?

IP: 207.38.152.228
Location: 40.7143, -74.006
Time: 25/Aug/2013:20:50:41 -0400

User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:23.0) Gecko/20100101 Firefox/23.0
Request: /blog/images/implied-facepalm.jpg
If you could just write down all of the phone numbers you’ve called in the last two years together with time, duration and location of the calls made, that’d be super.

It’s just metadata.
Client IP: 207.38.152.228
Provider: www.gmail.com

IP: 166.84.7.99
Client IP: 207.38.152.228
Provider: www.gmail.com

IP: 166.84.7.99
Provider: mail.yahoo.com

Wednesday, September 4, 13
Client IP: 207.38.152.228
Server: www.gmail.com

IP: 74.125.226.245

SSL

LOL “Upstream”

IP: 166.84.7.99

IP: 63.250.192.45

SSL
PGP

@GPGTools:  https://gpgtools.org/

@mailvelope:  http://www.mailvelope.com/

http://www.gnupg.org/
What are we still leaking?
What are we still leaking?
What are we still leaking?
From: jschauma@twitter.com
To: doctorow@craphound.com

IP: 207.38.152.228
Location: 40.7143, -74.006
Time: 25/Aug/2013:20:50:41 -0400

What are we still leaking?
Can we do better?

Wednesday, September 4, 13
IP: 207.38.152.228

@jschauma

connection encrypted

IP: 166.84.7.99

Wednesday, September 4, 13
Off The Record Messaging

end-to-end encryption
authentication
deniability
perfect forward secrecy

http://www.cypherpunks.ca/otr/
chat content encrypted

LOL
“Border” search

https://t.co/gSg4jcV8bs
§ 287 (a) (3) of the Immigration and Nationality Act, 66 Stat. 233, 8 U.S.C. § 1357(a)(3), which simply provides for warrantless searches of automobiles and other conveyances "within a reasonable distance from any external boundary of the United States"
Connections established via SSL to central server.
Connections established via SSL to central server.

chat content encrypted
IP: 207.38.152.228
Location: 40.7143, -74.006
Time: 25/Aug/2013:20:50:41 -0400

Connections established via SSL to central server.

chat content encrypted

IP: 166.84.7.99

LOL Metadata
No VPN.

Client IP: 207.38.152.228
Server: www.gmail.com

IP: 74.125.226.245

IP: 166.84.7.99
Location: 40.7143, -74.006
IP: 207.38.152.228
Location: 40.7143, -74.006
IP: 207.38.152.228

LOL NSL

IP: 205.251.192.55

Wednesday, September 4, 13
How Tor Works

Alice’s Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Understand your threat model!

@jschauma

https://xkcd.com/538/

Wednesday, September 4, 13
Understand your threat model!

A CRYPTO NERD'S IMAGINATION:
His laptop's encrypted. Let's build a million-dollar cluster to crack it.

WHAT WOULD ACTUALLY HAPPEN:
Blast! Our evil plan is foiled!

No good! It's 4096-bit RSA!

LOL NSL

LOL indeed.

https://xkcd.com/538/
Things you can do: Part I (Web)

Use services with strong privacy defaults.

https://prism-break.org/
Things you can do: Part I (Web)

DuckDuckGo
https://duckduckgo.com/

ixquick
https://ixquick.com/

YaCy*
http://www.yacy.net

http://donttrack.us/

@jschauma
Things you can do: Part I (Web)

enable HTTPS on services
use HTTPS-Everywhere

Delete Cookies
Enable DNT
Disable Referer
Set User Agent
Things you can do: Part II (Email)

Disable HTML.

Delete your email.

Use services with strong privacy defaults.

https://t.co/uorBWl4X5a
Things you can do: Part II (Email)

https://mykolab.com/

https://mail.riseup.net/

(Run your own mail server.)
Things you can do: Part II (Email)

Use PGP.

@GPGTools: https://gpgtools.org/

@mailvelope: http://www.mailvelope.com/

http://www.gnupg.org/
Things you can do: Part III (Chat)

Use OTR.

Don’t store logs.
Things you can do: Part III (Chat)

https://crypto.cat/

https://www.adium.im/

...

https://whispersystems.org/

https://guardianproject.info/apps/gibber/

@jschauma
Things you can do:
Part IV

Use a VPN.

Use Tor.

Wednesday, September 4, 13
Tumbling down the rabbit hole...
Tumbling down the rabbit hole...
Down the rabbit hole.

Tumbling down the rabbit hole...

Tails
https://tails.boum.org/

Least Authority
https://leastauthority.com/

Wednesday, September 4, 13
Tumbling down the rabbit hole...

@jschauma

Tails
https://tails.boum.org/

Least Authority
https://leastauthority.com/

Little Snitch
https://t.co/brvDYrO0ur
Hidden Services
https://t.co/f0LmP2vylJ

Tails
https://tails.boum.org/

Least Authority
https://leastauthority.com/

Little Snitch
https://t.co/brvDYr00Ur

Tumbling down the rabbit hole...
@jschauma

Tumbling down the rabbit hole...

Hidden Services
https://t.co/fOLmP2vylJ

Dark Web
http://www.thehiddenwiki.net/

Tails
https://tails.boum.org/

Least Authority
https://leastauthority.com/

Little Snitch
https://t.co/brvDYrQOuir

Wednesday, September 4, 13
Down the rabbit hole...

Hidden Services
https://t.co/fOLmP2vylJ

Dark Web
http://www.thehiddenwiki.net/

Tails
https://tails.boum.org/

Least Authority
https://leastauthority.com/

Little Snitch
https://t.co/brvDYo0ur
Oh, and one more thing...

http://www.netmeister.org/blog/opt-links.html
Oh, and one more thing...

https://supporters.eff.org/donate

"Nobody does more lasting good for the Internet with less. Every penny you donate makes change for the better."

— Cory Doctorow