# Anonymity, Usability, and Humans. Pick Two.

Andrew Lewman
andrew@torproject.org

16 May 2011

TorProject.org

# What are we talking about?

- Crash course on anonymous communications
- Quick overview of Tor
- Usability, Security, and Humans

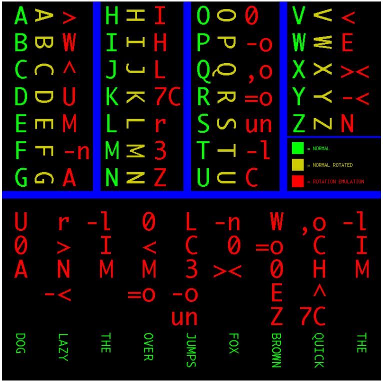
# The Tor Project, Inc.

501(c)(3) non-profit organization dedicated to the research and development of technologies for online anonymity and privacy

# What is anonymity?

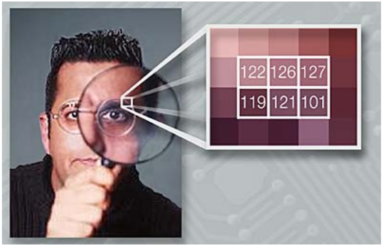
# Anonymity isn't cryptography

- Cryptography protects the contents in transit
- You still know who is talking to whom, how often, and how much data is sent.



# Anonymity isn't steganography

Attacker can tell Alice is talking to someone, how often, and how much data is sent.



# Anonymity isn't just wishful thinking...

- "You can't prove it was me!"

# Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"

# Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"

# Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"
- "Promise you won't tell"

# Anonymity isn't just wishful thinking...

- "You can't prove it was me!"
- "Promise you won't look"
- "Promise you won't remember"
- "Promise you won't tell"
- "I didn't write my name on it!"

# Anonymity isn’t just wishful thinking...

- ”You can’t prove it was me!”
- ”Promise you won’t look”
- ”Promise you won’t remember”
- ”Promise you won’t tell”
- ”I didn’t write my name on it!”
- ”Isn’t the Internet already anonymous?”

# ..since "weak" isn't anonymity.

- *"You can't prove it was me!"* Proof is a very **strong** word. Statistical analysis allows suspicion to become certainty.

# ..since "weak" isn't anonymity.

- *"Promise you won't look/remember/tell"* Will other parties have the abilities and incentives to keep these promises?

# ..since "weak" isn't anonymity.

- *"I didn't write my name on it!"* Not what we're talking about.

# ..since "weak" isn't anonymity.

- *"Isn't the Internet already anonymous?"* Nope!

# Anonymous communication

- People have to hide in a crowd of other people (”anonymity loves company”)
- The goal of the system is to make all users look as similar as possible, to give a bigger crowd
- Hide who is communicating with whom
- Layered encryption and random delays hide correlation between input traffic and output traffic

# Low-latency versus High-latency anonycomm systems

- Tor is not the first system; ZKS, mixmaster, single-hop proxies, Crowds, Java Anon Proxy.
- Low-latency systems are vulnerable to end-to-end correlation attacks.
- High-latency systems are more resistant to end-to-end correlation attacks, but by definition, less interactive.

# Low-latency systems are all the rage

- Interactive apps: web, instant messaging, VOIP, ssh, X11, cifs/nfs, video streaming (millions of users)
- Multi-hour delays: email, nntp, blog posting? (tens of thousands of users?)

# Low-latency systems are all the rage

- And if anonymity loves company...

# What is Tor?

- online anonymity software and network

# What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)

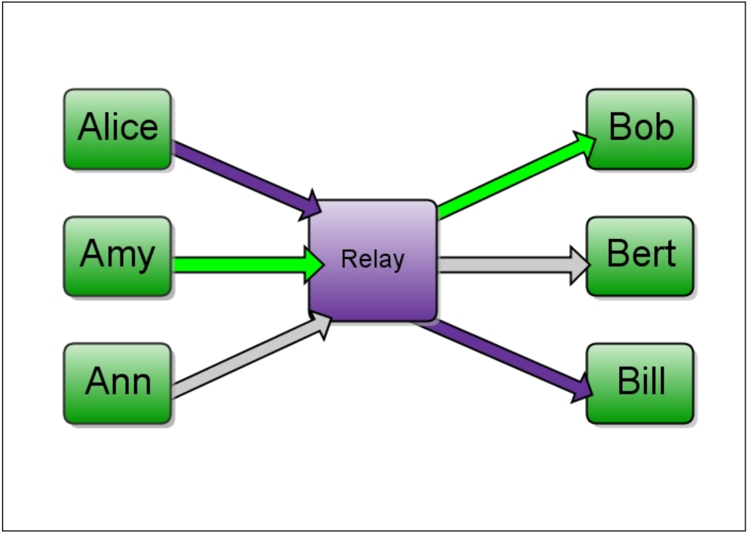
# What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech

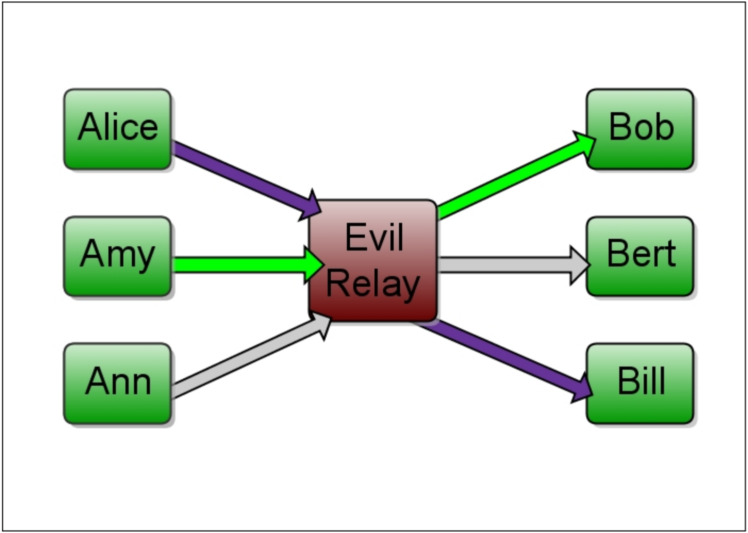
# What is Tor?

- online anonymity software and network
- open source, freely available (3-clause BSD license)
- active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech
- increasingly diverse toolset:
  Tor, Torbutton, Tor Browser Bundle, TAILS Anonymous Operating System, Tor Weather, Tor auto-responder, Secure Updater, Orbot, Torora, Tor Check, Arm, Nymble, Tor Control, Tor Wall, TorVM

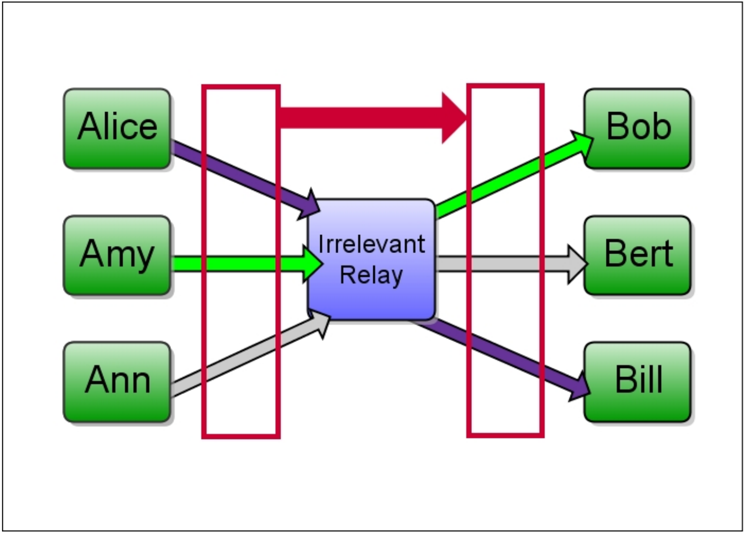
# How is Tor different from other systems?



# How is Tor different from other systems?



# How is Tor different from other systems?

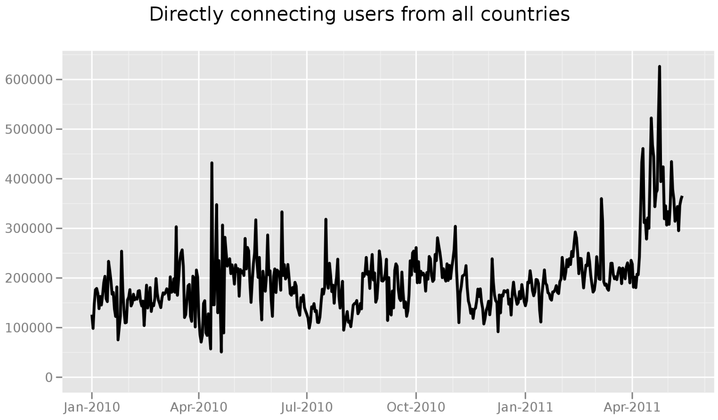


# Who uses Tor?

- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims

# estimated 300k to 800k daily users

# How many people use Tor daily?

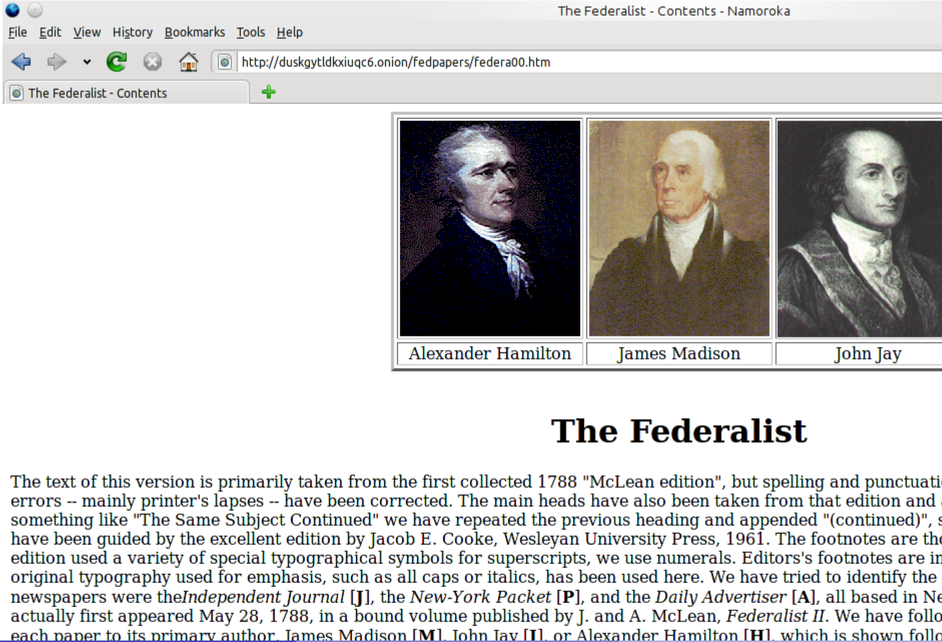


The Tor Project - https://metrics.torproject.org/

# Online and Offline change happens

# ...spring is in the air...

# Tor hidden services


The Federalist - Contents - Namoroka
File Edit View History Bookmarks Tools Help
http://duskgytldkxiuqc6.onion/fedpapers/federa00.htm
The Federalist - Contents
Alexander Hamilton
James Madison
John Jay

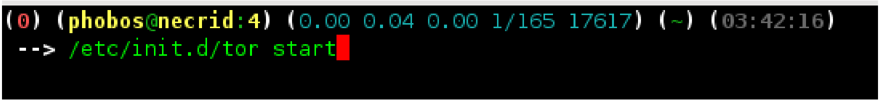
## The Federalist

The text of this version is primarily taken from the first collected 1788 "McLean edition", but spelling and punctuati errors -- mainly printer's lapses -- have been corrected. The main heads have also been taken from that edition and something like "The Same Subject Continued" we have repeated the previous heading and appended "(continued)", s have been guided by the excellent edition by Jacob E. Cooke, Wesleyan University Press, 1961. The footnotes are th edition used a variety of special typographical symbols for superscripts, we use numerals. Editors's footnotes are in original typography used for emphasis, such as all caps or italics, has been used here. We have tried to identify the newspapers were the*Independent Journal* **[J]**, the *New-York Packet* **[P]**, and the *Daily Advertiser* **[A]**, all based in Ne actually first appeared May 28, 1788, in a bound volume published by J. and A. McLean, *Federalist II*. We have follo each paper to its primary author, James Madison **[M]**, John Jay **[J]**, or Alexander Hamilton **[H]**, which is shown follo

# Anonymity, Usability, and Humans

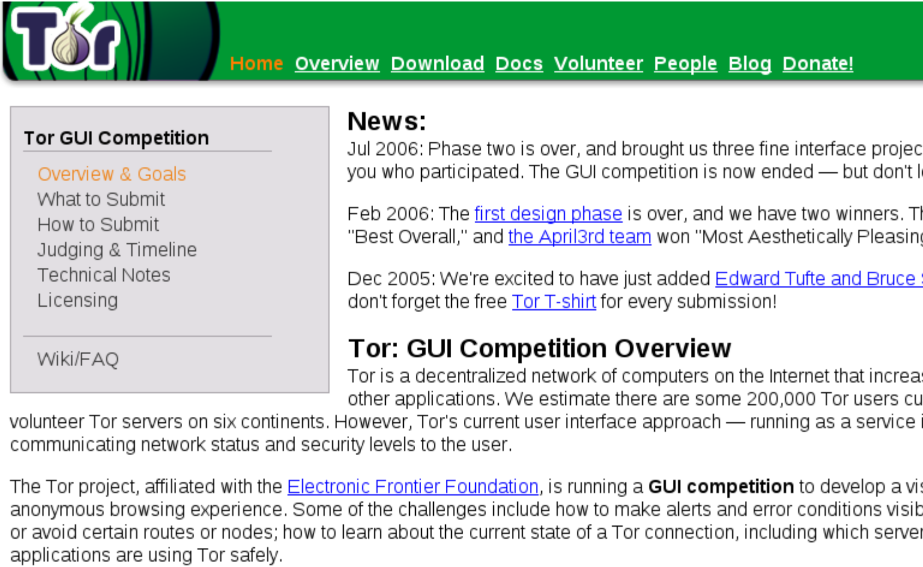
- Allow the user to fully configure Tor rather than manually searching for and opening text files.
- Let users learn about the current state of their Tor connection, and configure or find out whether any of their applications are using it.
- Make alerts and error conditions visible to the user.
- Run on Windows, Linux, and OS X, on a normal consumer-level machine.

# First iteration: command line



```
(0) (phobos@necrid:4) (0.00 0.04 0.00 1/165 17617) (~) (03:42:16)
 --> /etc/init.d/tor start
```

# Second iteration: GUI controller contest



**Tor GUI Competition**

- Overview & Goals
- What to Submit
- How to Submit
- Judging & Timeline
- Technical Notes
- Licensing

Wiki/FAQ

## News:

Jul 2006: Phase two is over, and brought us three fine interface projec
you who participated. The GUI competition is now ended — but don't l

Feb 2006: The first design phase is over, and we have two winners. Th
"Best Overall," and the April3rd team won "Most Aesthetically Pleasin

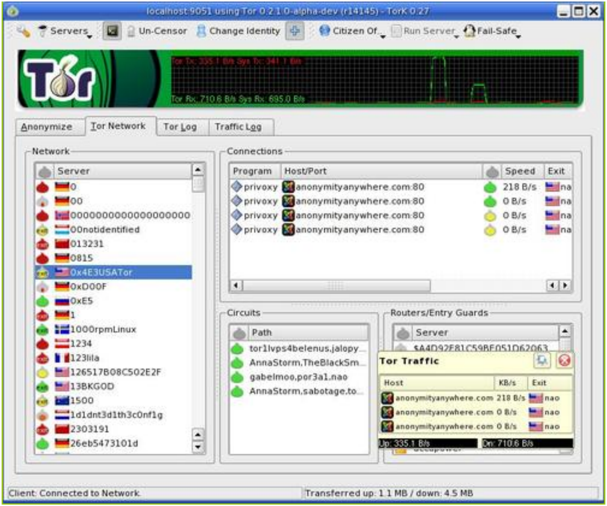
Dec 2005: We're excited to have just added Edward Tufte and Bruce S
don't forget the free Tor T-shirt for every submission!

## Tor: GUI Competition Overview

Tor is a decentralized network of computers on the Internet that increa
other applications. We estimate there are some 200,000 Tor users cu
volunteer Tor servers on six continents. However, Tor's current user interface approach — running as a service i
communicating network status and security levels to the user.

The Tor project, affiliated with the Electronic Frontier Foundation, is running a **GUI competition** to develop a vis
anonymous browsing experience. Some of the challenges include how to make alerts and error conditions visib
or avoid certain routes or nodes; how to learn about the current state of a Tor connection, including which server
applications are using Tor safely.

# TorK



localhost:9051 using Tor 0.2.1.0-alpha-dev (r14145) - TorK 0.27

Network

| Server |
|---|
| 0 |
| 00 |
| 0000000000000000000 |
| 00notidentified |
| 013231 |
| 0815 |
| 0x4E3USATor |
| 0xD00F |
| 0xE5 |
| 1 |
| 1000rpmLinux |
| 1234 |
| 123lila |
| 126517B08C502E2F |
| 13BKGOD |
| 1500 |
| 1d1dnt3d1th3c0nf1g |
| 2303191 |
| 26eb5473101d |

Connections

| Program | Host/Port | Speed | Exit |
|---|---|---|---|
| privoxy | anonymityanywhere.com:80 | 218 B/s | na |
| privoxy | anonymityanywhere.com:80 | 0 B/s | na |
| privoxy | anonymityanywhere.com:80 | 0 B/s | na |
| privoxy | anonymityanywhere.com:80 | 0 B/s | na |

Circuits

| Path |
|---|
| tor1lvps4belenus,jalopy... |
| AnnaStorm,TheBlackSm... |
| gabelmoo,por3a1,nao |
| AnnaStorm,sabotage,to... |

Routers/Entry Guards

| Server |
|---|
| $A4D92E81C59BE051D62063 |

Tor Traffic

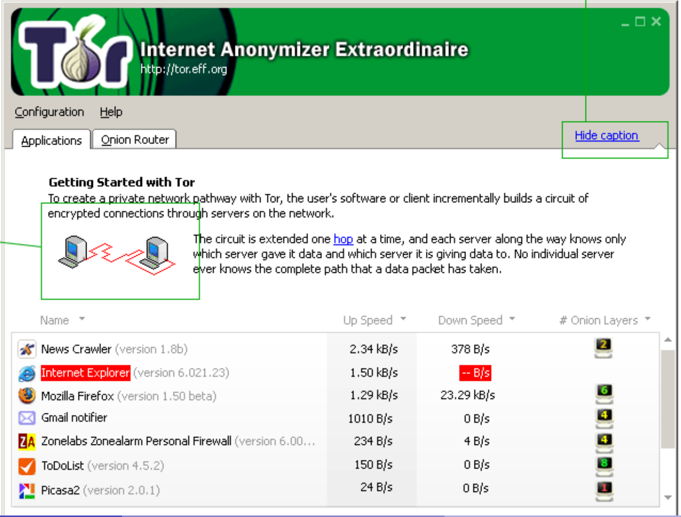
| Host | KB/s | Exit |
|---|---|---|
| anonymityanywhere.com | 218 B/s | nao |
| anonymityanywhere.com | 0 B/s | nao |
| anonymityanywhere.com | 0 B/s | nao |

Up: 335.1 B/s Dn: 710.6 B/s

Client: Connected to Network. Transferred up: 1.1 MB / down: 4.5 MB

# April3rd

This is the default view when user opens the Tor Control Panel for the first time. The text in the caption is used to explain how to get started with Tor. Once the user chooses to hide the caption text, this setting is remembered when Tor Control Panel is accessed again.



**Getting Started with Tor**

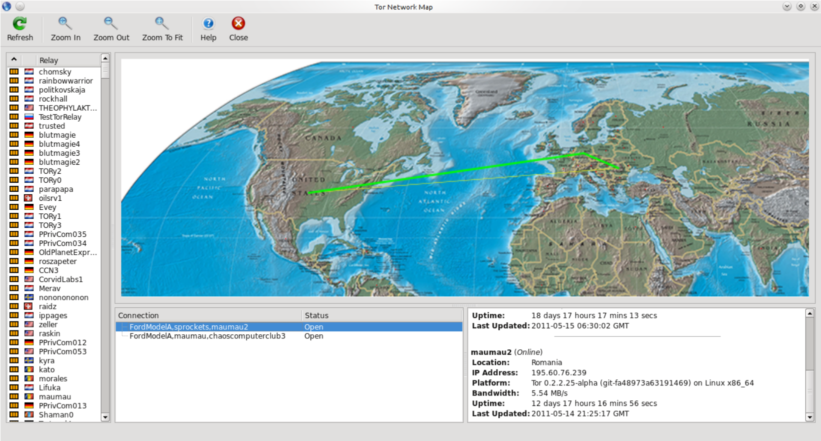
To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through servers on the network.

The circuit is extended one hop at a time, and each server along the way knows only which server gave it data and which server it is giving data to. No individual server ever knows the complete path that a data packet has taken.

| Name | Up Speed | Down Speed | # Onion Layers |
|---|---|---|---|
| News Crawler (version 1.8b) | 2.34 kB/s | 378 B/s | 2 |
| Internet Explorer (version 6.021.23) | 1.50 kB/s | -- B/s | |
| Mozilla Firefox (version 1.50 beta) | 1.29 kB/s | 23.29 kB/s | 6 |
| Gmail notifier | 1010 B/s | 0 B/s | 4 |
| Zonelabs Zonealarm Personal Firewall (version 6.00... | 234 B/s | 4 B/s | 4 |
| ToDoList (version 4.5.2) | 150 B/s | 0 B/s | 8 |
| Picasa2 (version 2.0.1) | 24 B/s | 0 B/s | 1 |

Caption-help includes diagrams and links to further help topics.

# Vidalia



Relay
chomsky
rainbowwarrior
politkovskaja
rockhall
THEOPHYLAKT...
TestTorRelay
trusted
blutmagie
blutmagie4
blutmagie3
blutmagie2
TORy2
TORy0
parapapa
oilsrv1
Evey
TORy1
TORy3
PPrivCom035
PPrivCom034
OldPlanetExpr...
roszapeter
CCN3
CorvidLabs1
Merav
nononononon
raidz
ippages
zeller
raskin
PPrivCom012
PPrivCom053
kyra
kato
morales
Lifuka
maumau
PPrivCom013
Shaman0

| Connection | Status |
|---|---|
| FordModelA,sprockets,maumau2 | Open |
| FordModelA,maumau,chaoscomputerclub3 | Open |

**Uptime:** 18 days 17 hours 17 mins 13 secs
**Last Updated:** 2011-05-15 06:30:02 GMT

**maumau2** *(Online)*
**Location:** Romania
**IP Address:** 195.60.76.239
**Platform:** Tor 0.2.2.25-alpha (git-fa48973a63191469) on Linux x86_64
**Bandwidth:** 5.54 MB/s
**Uptime:** 12 days 17 hours 16 mins 56 secs
**Last Updated:** 2011-05-14 21:25:17 GMT

# Time for a demo

Demonstration of Tor Browser Bundle

# Experience so far

- Our web site is confusing to users and not technical enough for researchers.

# Experience so far

- Our web site is confusing to users and not technical enough for researchers.
- Concepts of anonymity and its threats escape most users.
  "I want my Youtube!" "I use tor to organize on facebook."

# Experience so far

- Our web site is confusing to users and not technical enough for researchers.
- Concepts of anonymity and its threats escape most users.
  "I want my Youtube!" "I use tor to organize on facebook."
- Cultural differences and their expectations of software, usability, anonymity, privacy, and what tor provides.

# Experience so far

- Our web site is confusing to users and not technical enough for researchers.
- Concepts of anonymity and its threats escape most users.
  "I want my Youtube!" "I use tor to organize on facebook."
- Cultural differences and their expectations of software, usability, anonymity, privacy, and what tor provides.
- Software leaks data all over the place. Stopping these leaks leads to unexpected user experiences.

# Experience so far

- Our web site is confusing to users and not technical enough for researchers.
- Concepts of anonymity and its threats escape most users.
  "I want my Youtube!" "I use tor to organize on facebook."
- Cultural differences and their expectations of software, usability, anonymity, privacy, and what tor provides.
- Software leaks data all over the place. Stopping these leaks leads to unexpected user experiences.
- Five years since we last dabbled in Usability.

# Next steps

Visit `https://www.torproject.org/` for more information, links, and ideas.

# Copyright

- who uses tor? `http://www.flickr.com/photos/mattw/2336507468/siz`, Matt Westervelt, CC-BY-SA.
- 500k, `http://www.flickr.com/photos/lukaskracic/334850378/sizes/l/`, Luka Skracic, used with permission.
- spring is in the air, Paco Pomet, http://pacopomet.wordpress.com/