



Congratulations!
This browser is configured to use Tor.
You are now free to browse the Internet anonymously.
[Test Tor Network Settings](#)

Search securely with [Disconnect.me](#) 

What Next?
Tor is NOT all you need to browse anonymously!
You may need to change some of your browsing
habits to ensure your identity stays safe.
[Tips On Staying Anonymous »](#)

You Can Help!
There are many ways you can help make the Tor
Network faster and stronger:
• [Run a Tor Relay Node »](#)
• [Volunteer Your Services »](#)
• [Make a Donation »](#)

Anonymity Online for Everyone

What is missing for zero-effort privacy on the Internet?

Dominik Herrmann
Universität Siegen

Ephraim Zimmer,
Jens Lindemann and
Hannes Federrath
Universität Hamburg

Slides: <http://dhgo.to/inetsec15slides>

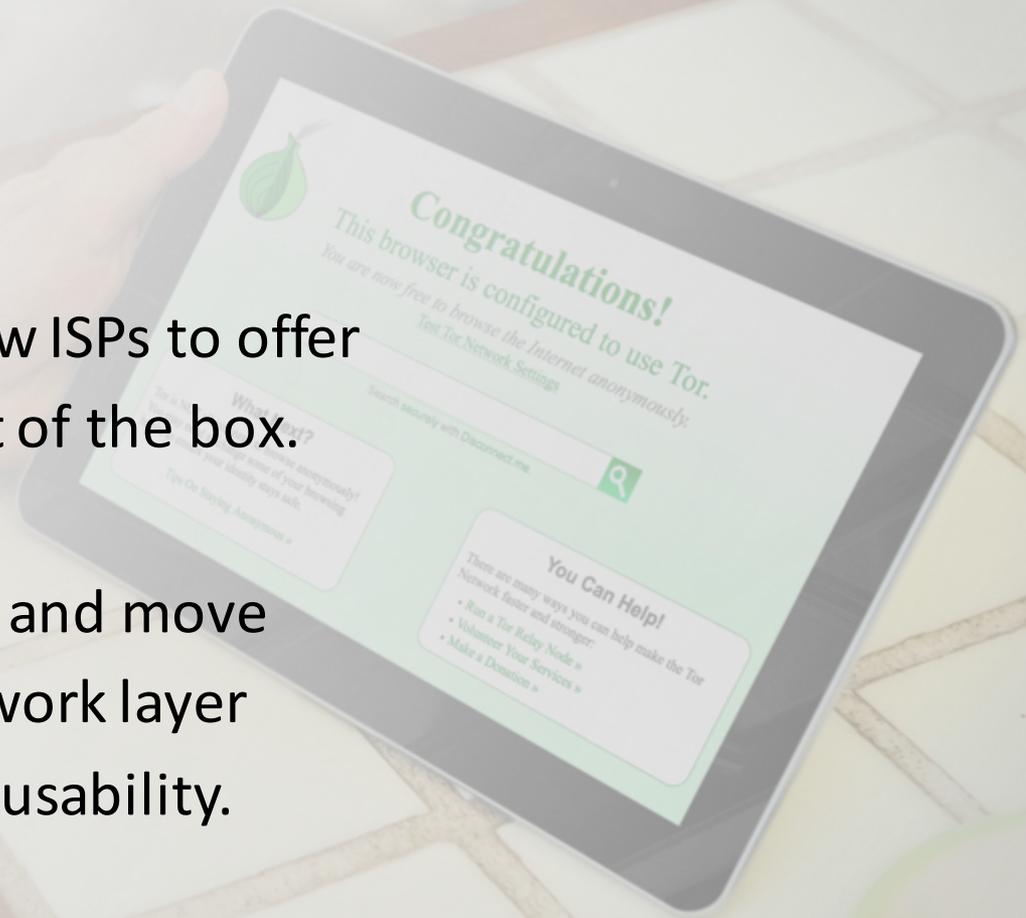


Anonymity Online for Everyone

What is missing for zero-effort privacy on the Internet?

Technical solutions that allow ISPs to offer a decent level of privacy out of the box.

How? Relax attacker model and move anonymization into the network layer for better performance and usability.



Anonymity Online for Everyone

What is missing for zero-effort privacy on the Internet?

Technical solutions that allow ISPs to offer a decent level of privacy out of the box.

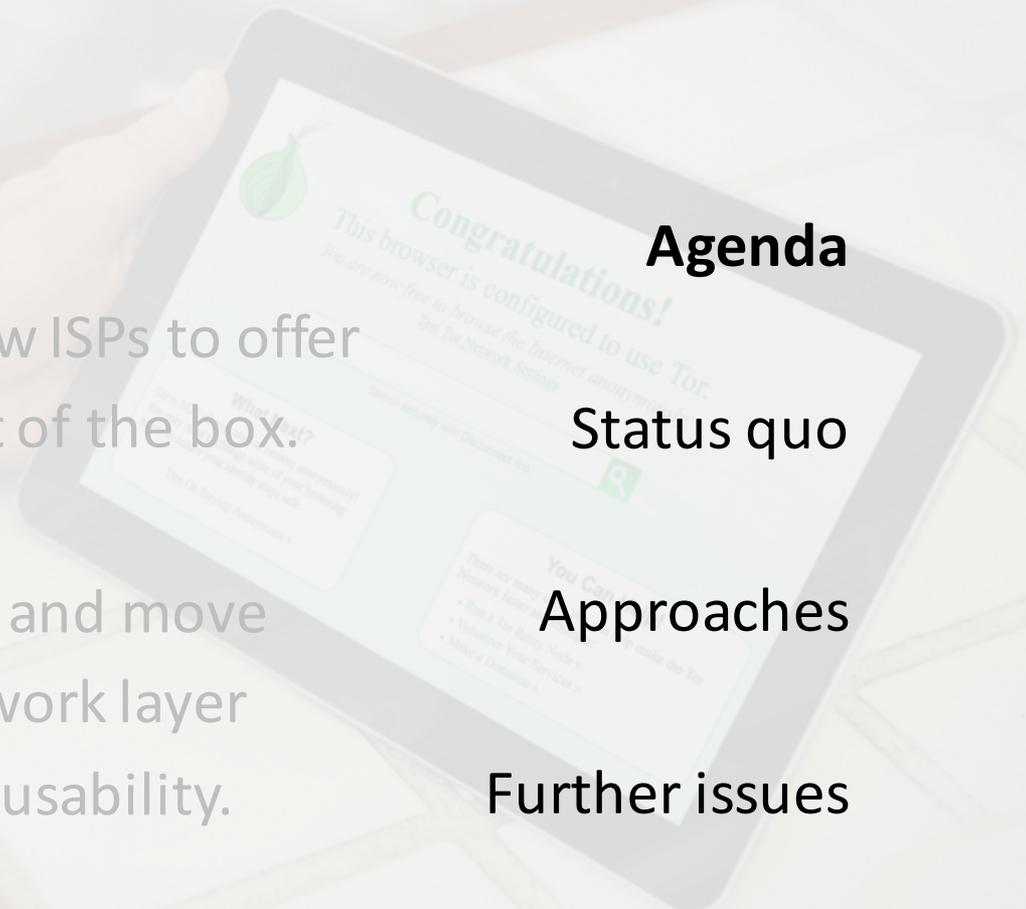
How? Relax attacker model and move anonymization into the network layer for better performance and usability.

Agenda

Status quo

Approaches

Further issues



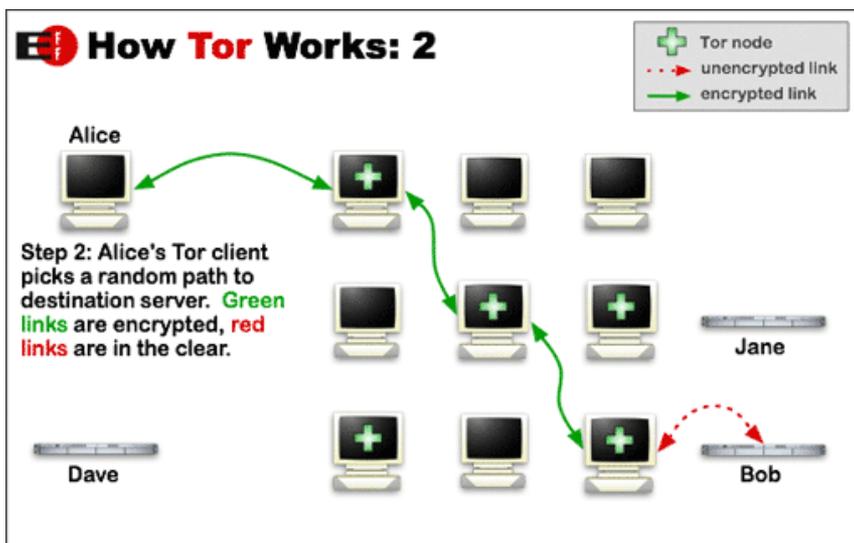
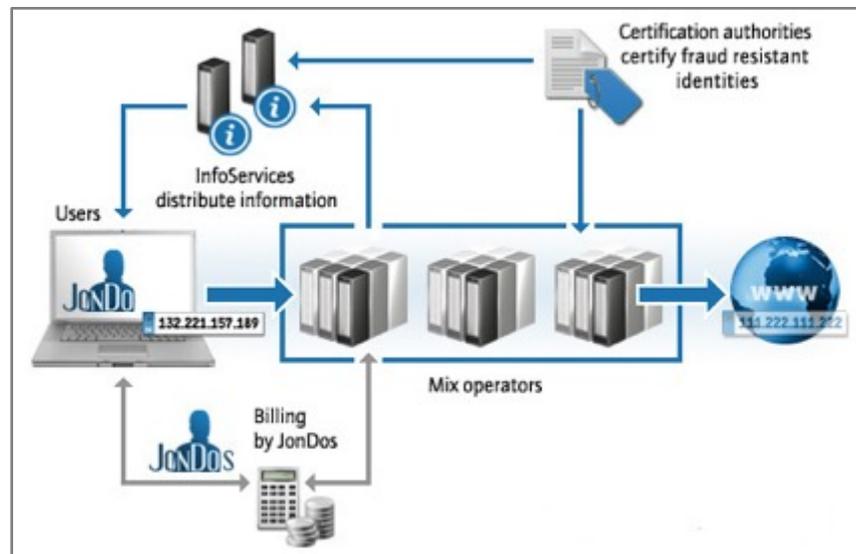
Self-defense tools offering relationship anonymity via onion routing and web mixes have been available for >10 years.

Relationship anonymity:

Observers cannot determine what services a user accesses.

Sender anonymity:

Destinations do not learn source IP address of user.

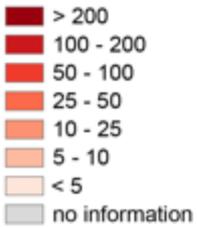


mainly an issue on IP layer
but also on application layer

However, self-defense tools are not used by “normal” citizens.

The anonymous Internet

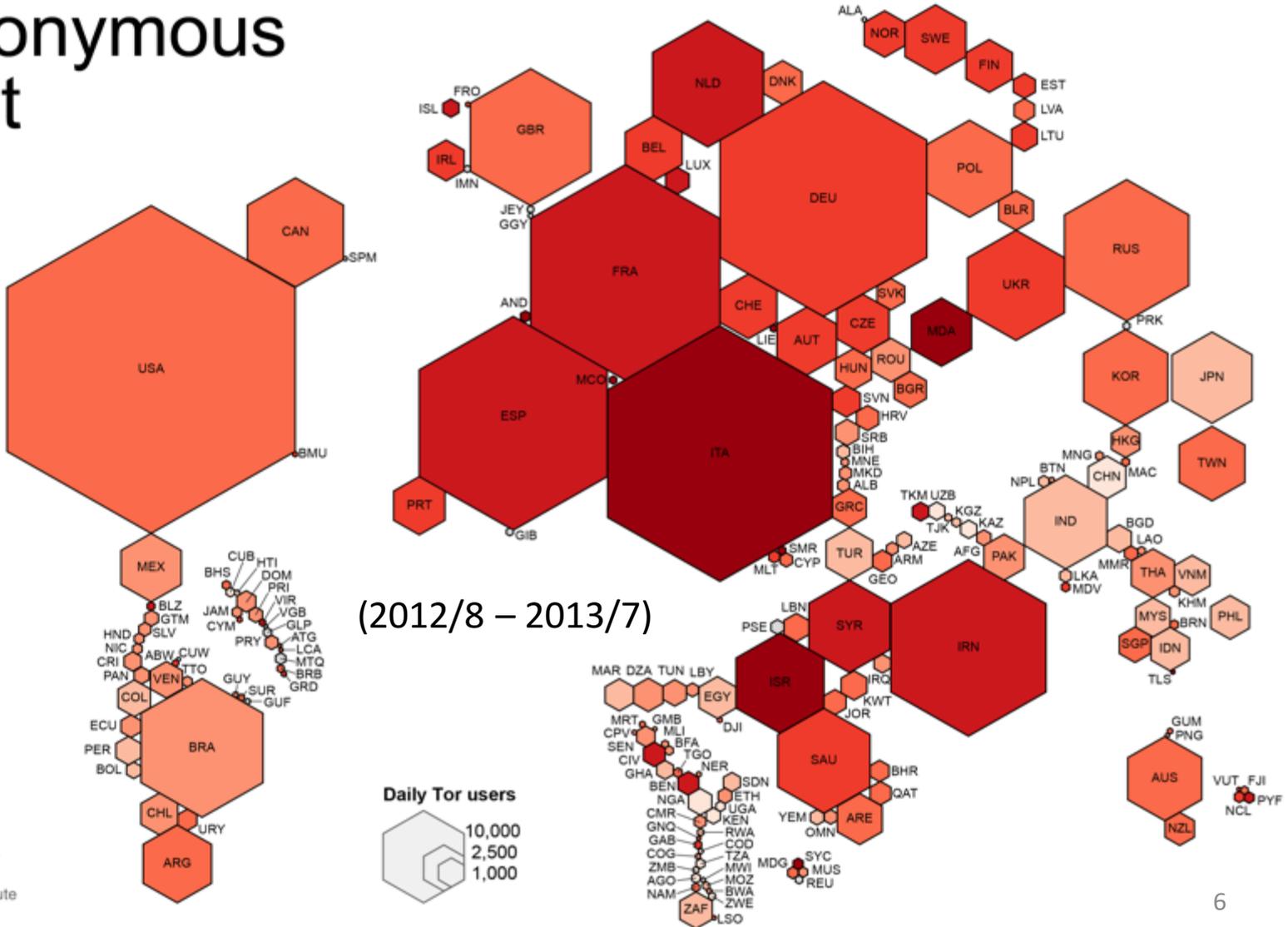
Daily Tor users per 100,000 Internet users



Average number of Tor users per day calculated between August 2012 and July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

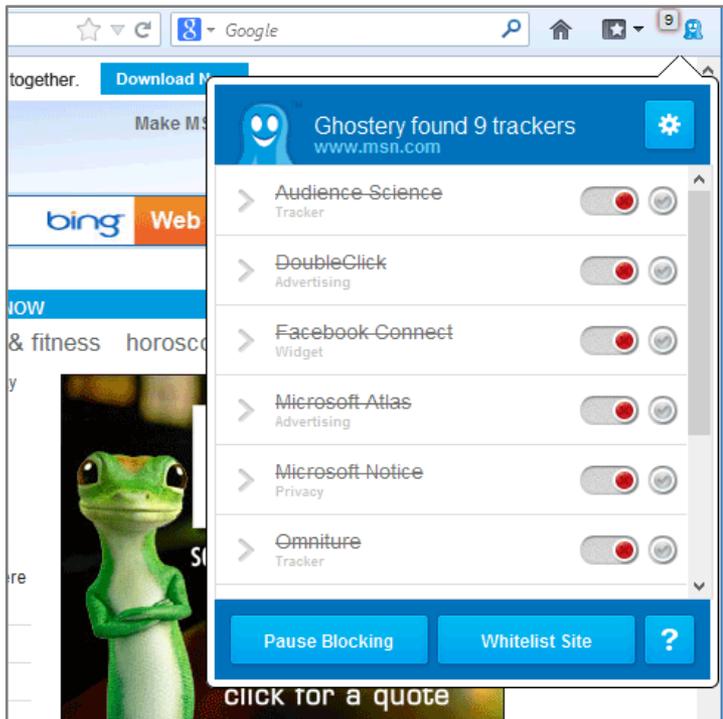
by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk



Popular browser plug-ins target a less complex privacy problem, but this may be sufficient for some users.

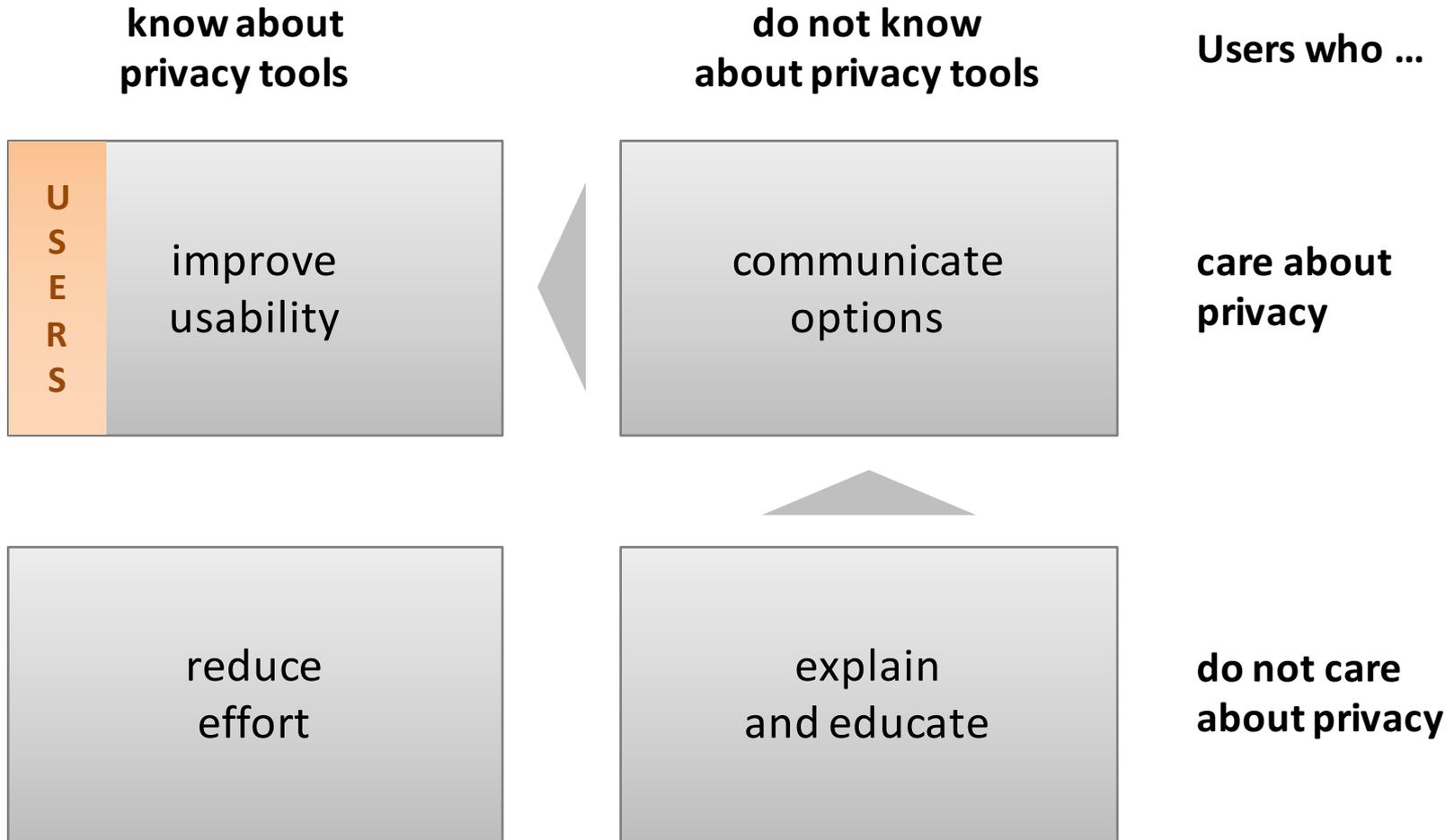
Unlinkability:

Destinations and their partners cannot track activities of a user.

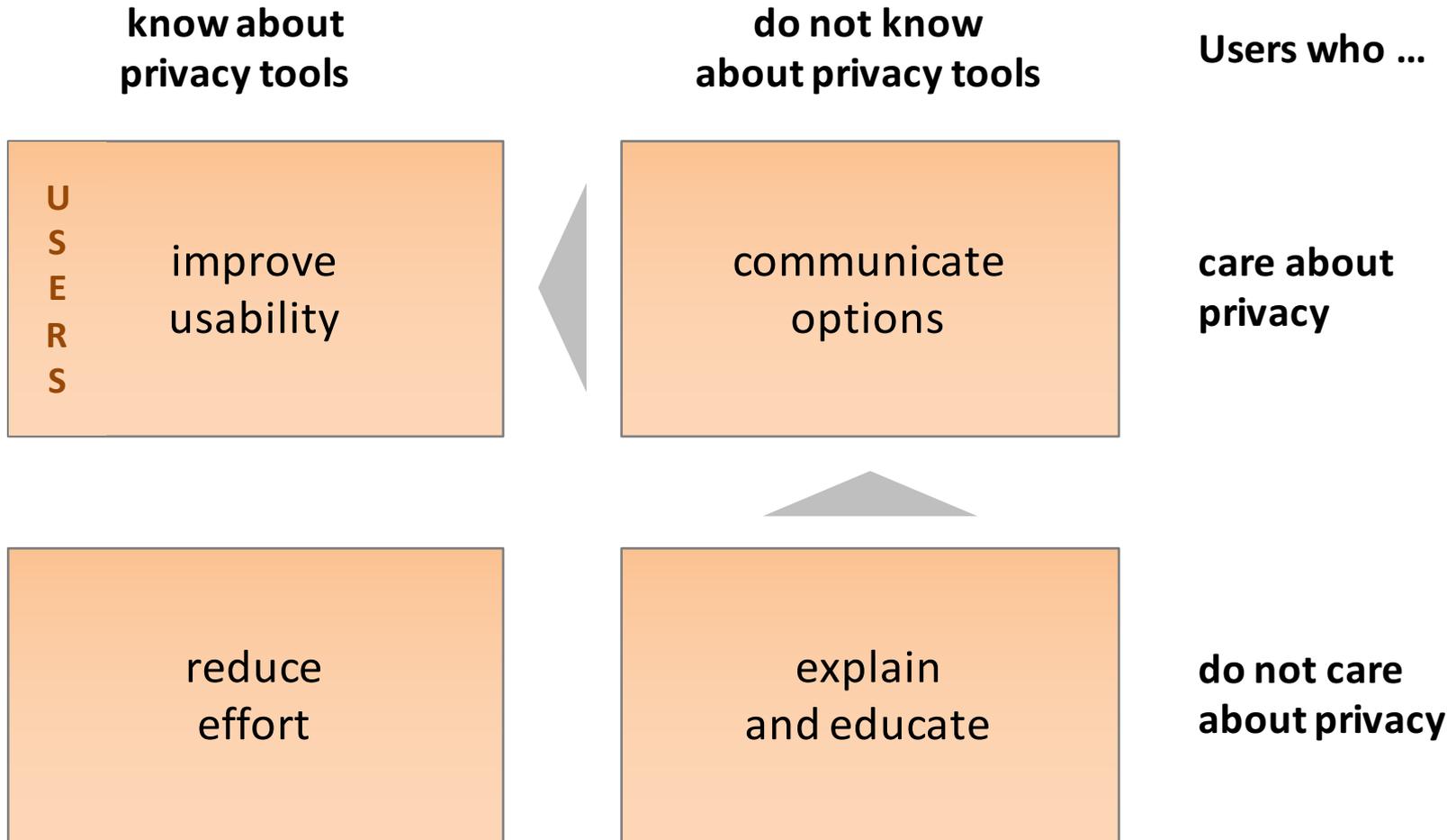


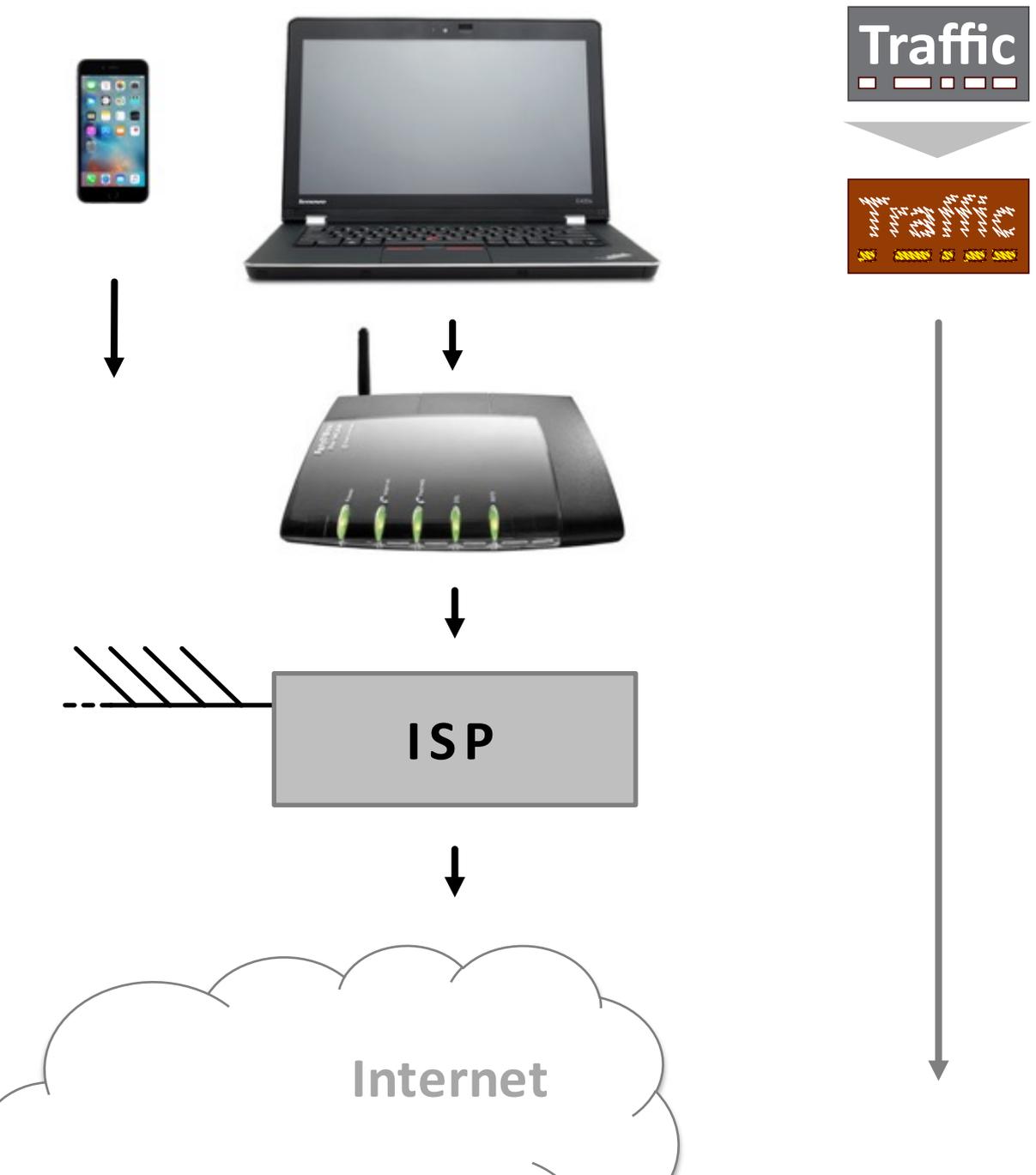
mainly happens on application layer
but also possible on IP layer

Why isn't everyone using Tor et al.? What can we do to increase their adoption?

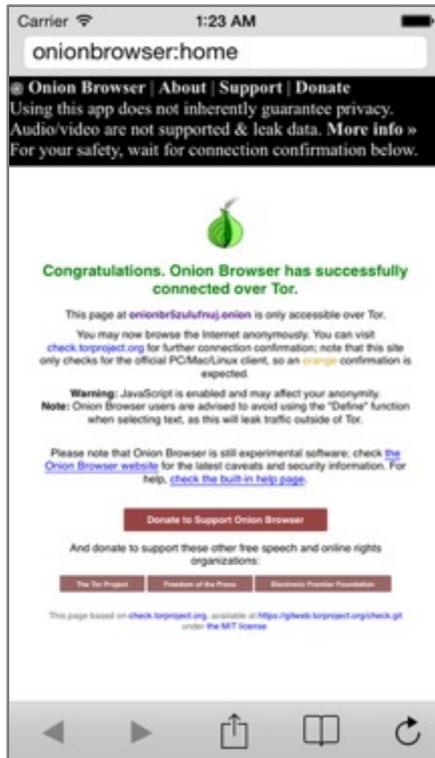


Why isn't everyone using Tor et al.? What can we do to increase their adoption?





Users are going mobile. Anonymous Internet access and tracking protection are difficult to realize on smartphones due to limitations of the OS.



OnionBrowser for iOS
limited to special browser



Orbot for Android
offers local proxy/VPN,
(requires rooted device)

Status quo

Approaches

Further issues

Privacy-enabled home routers appear to be *the* solution – or are they just yet another workaround?

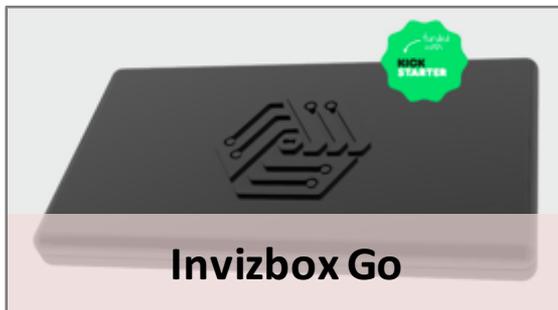


Anonabox

\$82,643 @ indiegogo



Price: \$49,00



Invizbox Go

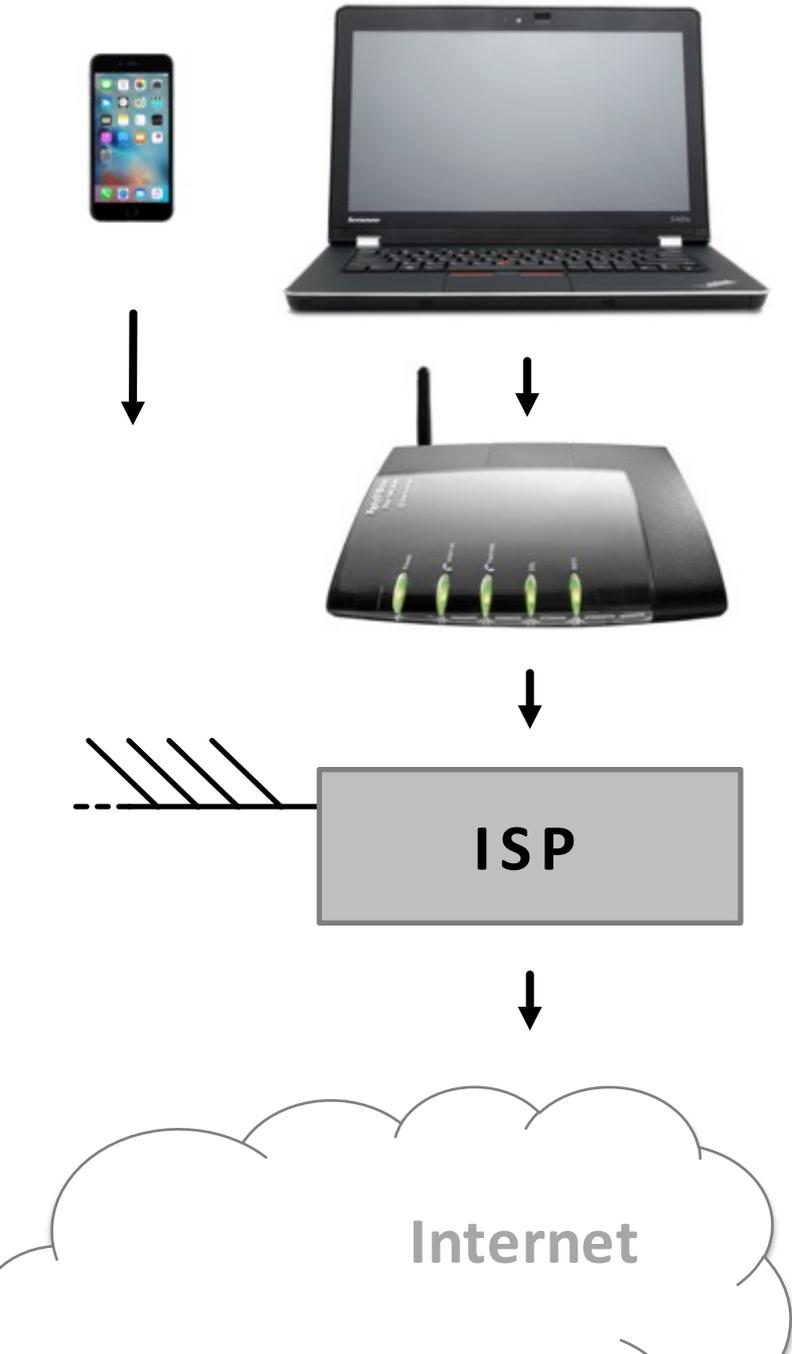
\$20,960 @ indiegogo
101,420 € @ kickstarter



eBLOCKER

\$81,000 @ indiegogo

Anonymizing routers do improve usability, but they have inherent limitations.



Ideally, works with any device out of the box

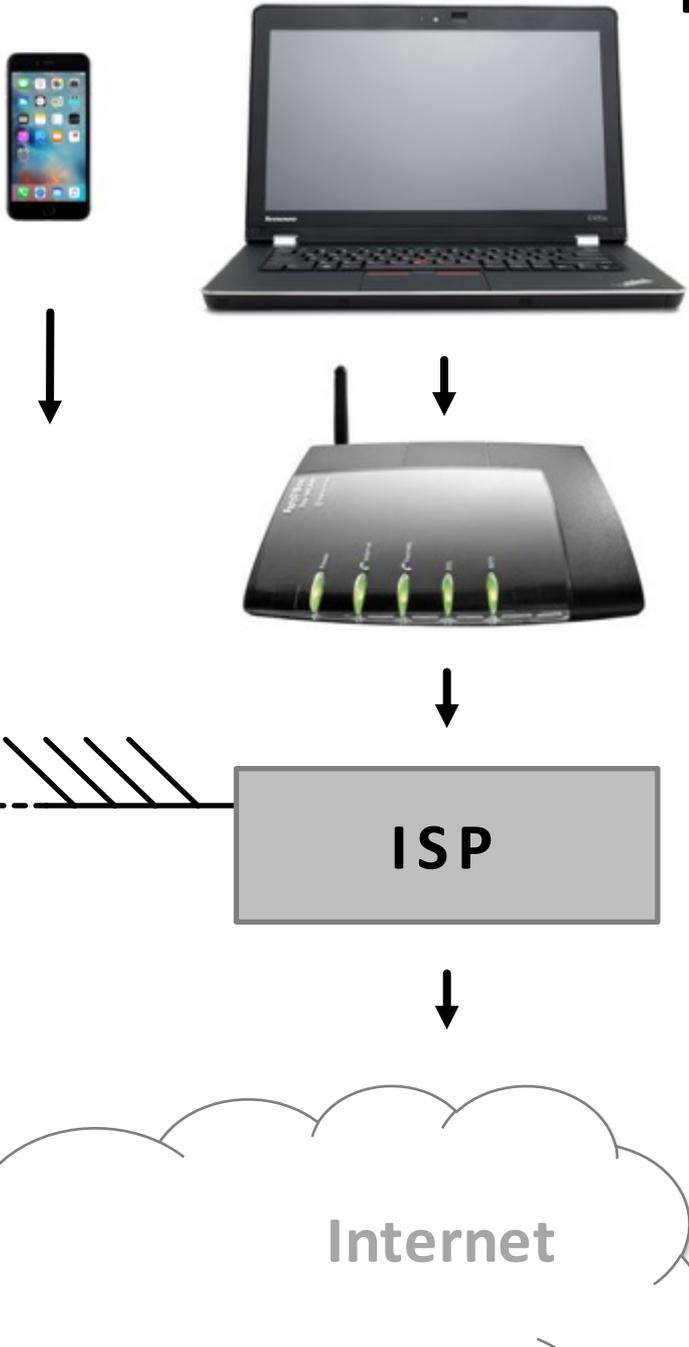
Unavailable on the road

Proxying all traffic (UDP!)

Layer 7 filtering (TLS!)



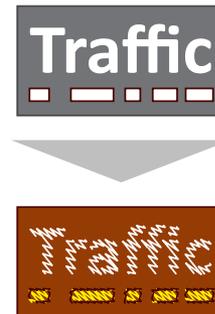
Delegating anonymization to the ISP reduces effort for users (again, limitations apply).



Less effort for users:

No special router needed

Works on the road



Have to trust ISP

Proxying all traffic (UDP!)

Layer 7 filtering (TLS!) 

Users will only accept privacy-enabled Internet, if there is no noticeable difference in performance and price. What are our options?

Reduce overhead of
anonymous routing



tailor anonymization
to individual applications

understand interference
between overlay und underlay

move anonymization
into network layer

cf. LAP, Dovetail, HORNET

Consider other approaches
to achieve privacy



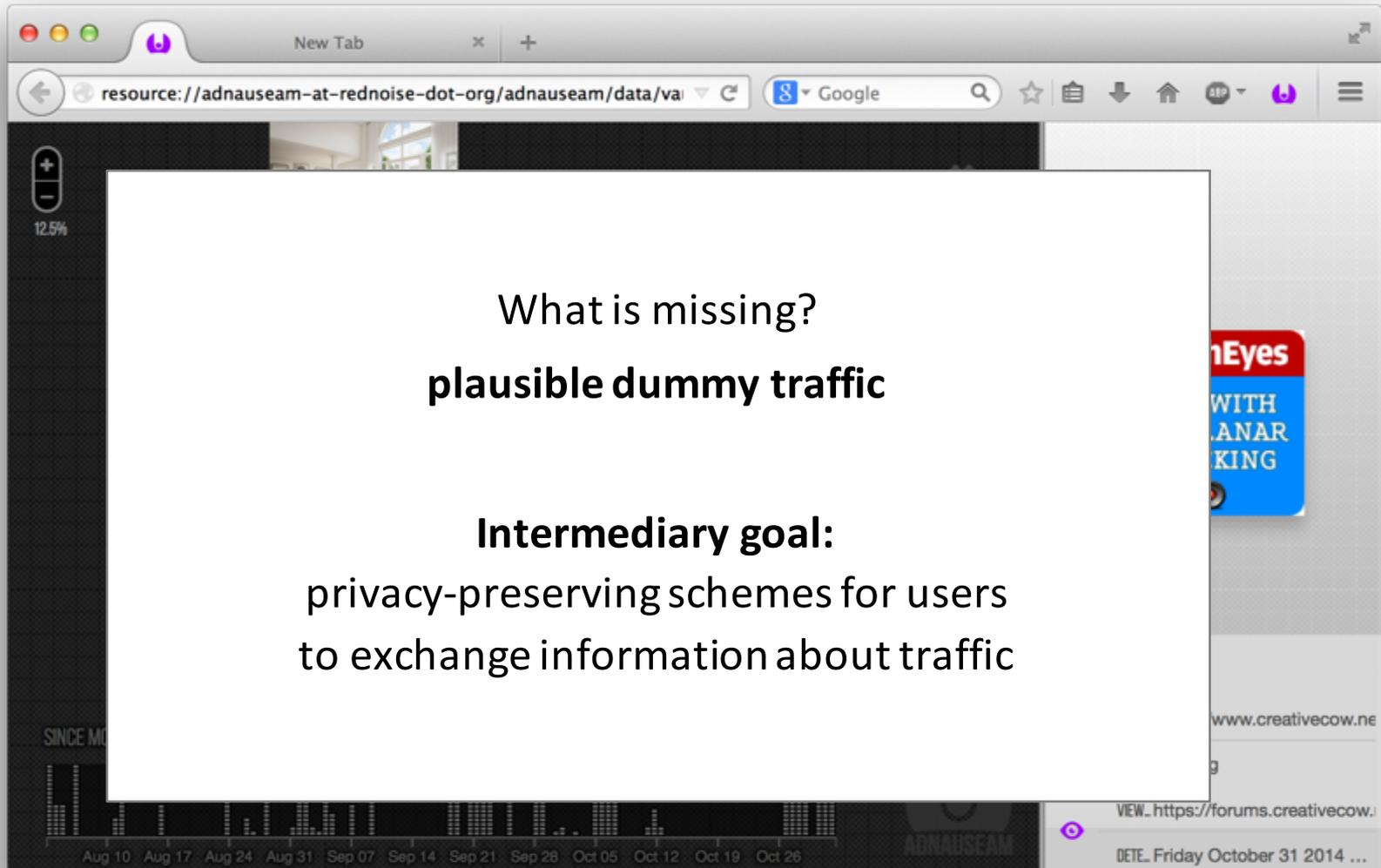
obfuscation
via dummy traffic

unlinkable IP addresses
to prevent tracking

cf. Raghawan et al. and
Herrmann et al.

Obfuscation with dummy traffic is an interesting solution – but a controversial approach.

cf. AdNauseam and TrackMeNot



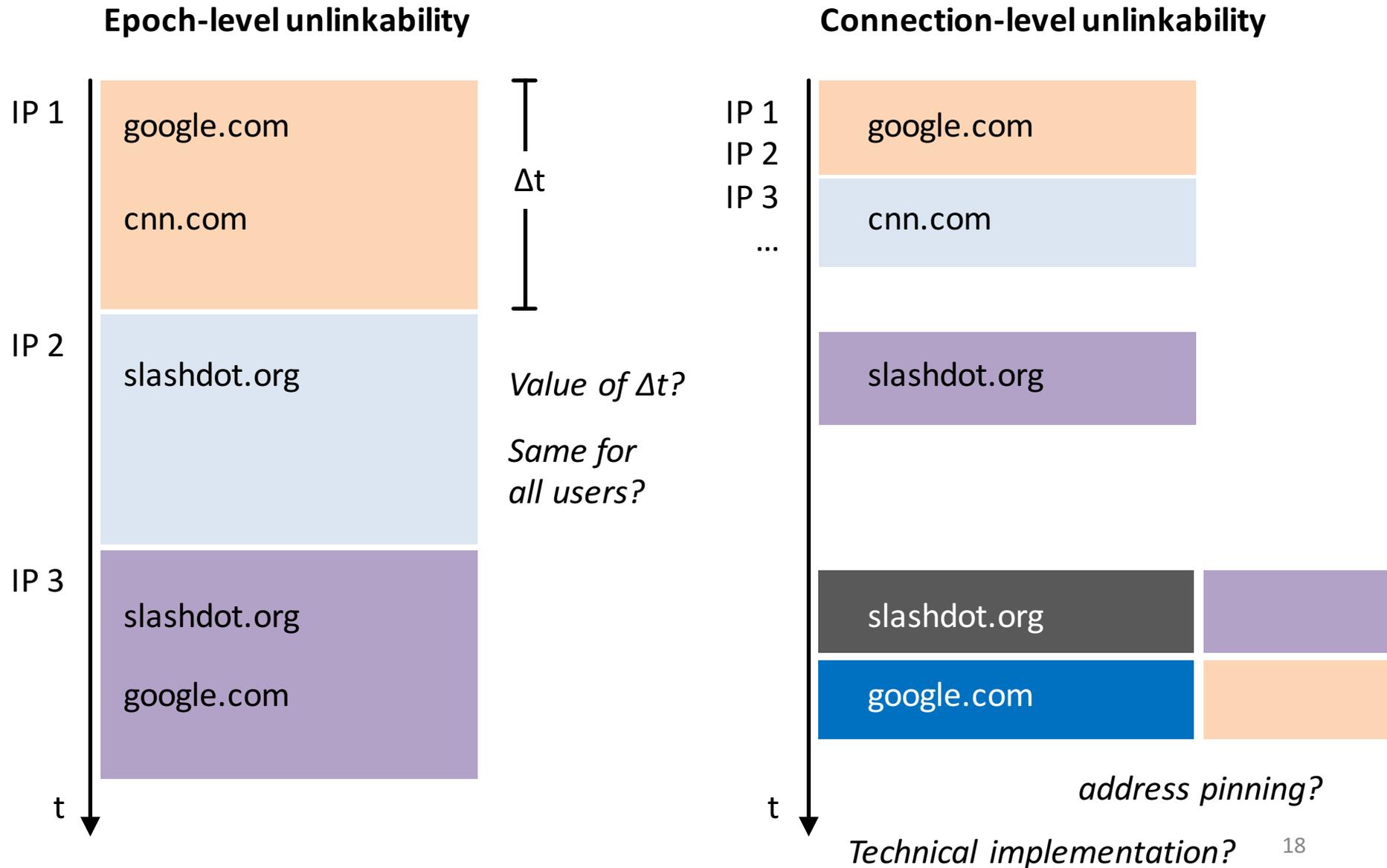
The image shows a screenshot of a web browser window. The address bar contains the URL `resource://adnauseam-at-rednoise-dot-org/adnauseam/data/va`. The browser's search bar shows "Google". The main content area displays a slide with the following text:

What is missing?
plausible dummy traffic

Intermediary goal:
privacy-preserving schemes for users
to exchange information about traffic

The slide is overlaid on a background that appears to be a data visualization or dashboard. On the right side, there is a red and blue advertisement for "Eyes WITH ANAR KING". At the bottom of the browser window, there is a timeline with dates from August 10 to October 26, and a "VIEW" link for a forum post on creativecow.net.

If sender anonymity is not necessary and unlinkability of actions is sufficient, we suggest that ISPs should improve IP address assignment.



Status quo

Approaches

Further issues

Apart from anonymizing IP addresses, there are at least three further issues to be considered.

Application
layer filtering

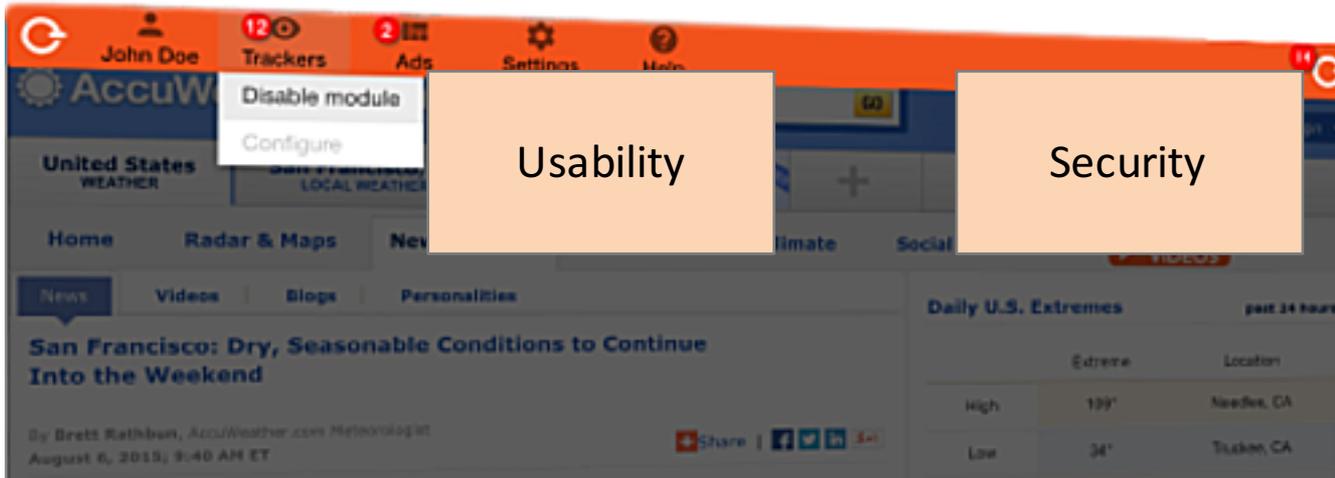
Unclear effectiveness of parsing JavaScript
Make TLS interception acceptable via whitelisting

Data
retention

Ensure ISP can abide the law and does not misuse its power
Devise efficient storage techniques

Verifiability
of operation

Zero-effort privacy means users will not notice, if their router or ISP fail to anonymize their traffic properly. How to verify correct operation?



Inject a toolbar into websites?



Router status indicator?

Anonymity Online for Everyone

Users either apathetic or
in state of analysis paralysis

Complement self-defense tools
for power users with decent level
of privacy out of the box for all users

Relaxing attacker model and moving
anonymization into network layer
interesting areas for future work

