

Lessons from the Tor community

Roger Dingledine

March 4, 2023

The Tor Project



Tor Overview

Online anonymity: open source, open network

Community of devs, researchers, users, relay operators

US 501(c)(3) non-profit organization with 30ish staff

Estimated 2,000,000 to 8,000,000 daily users

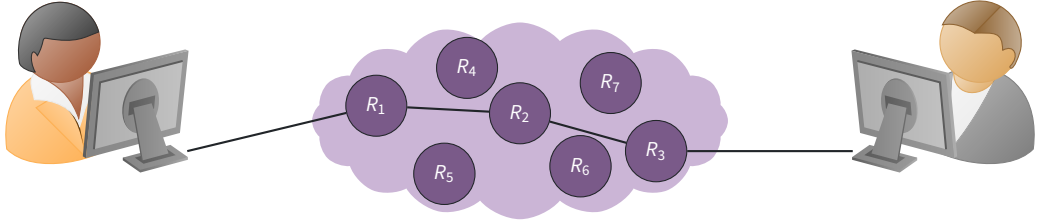
Part of larger ecosystems: internet freedom, free software, censorship resistance, anonymity research

Threat Model

Alice

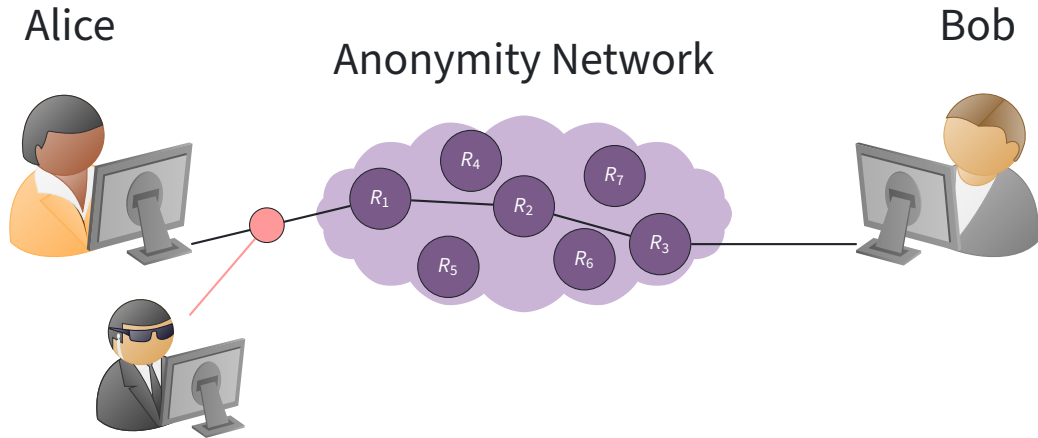
Anonymity Network

Bob

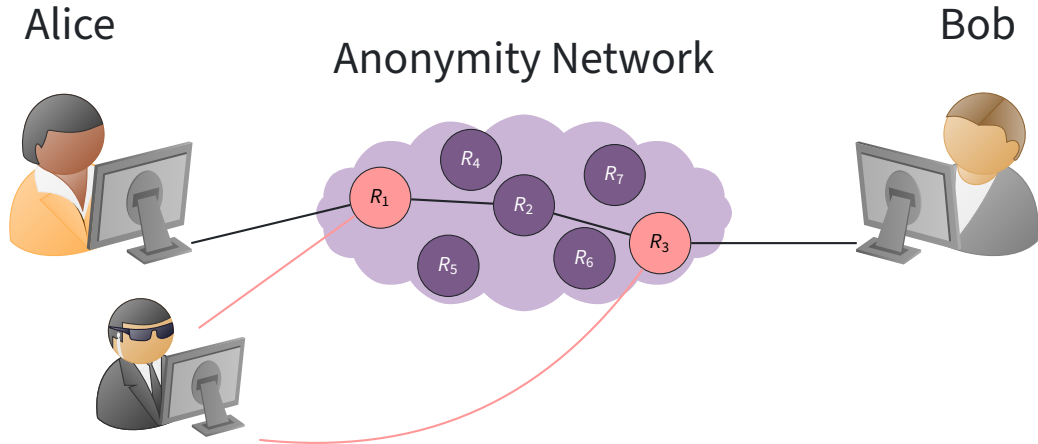


{What can the attacker do?}

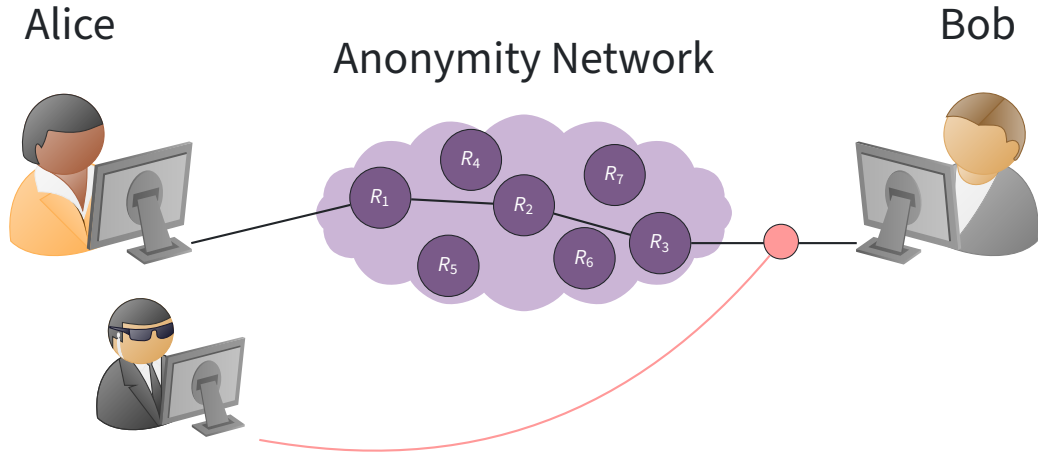
Threat Model



Threat Model



Threat Model

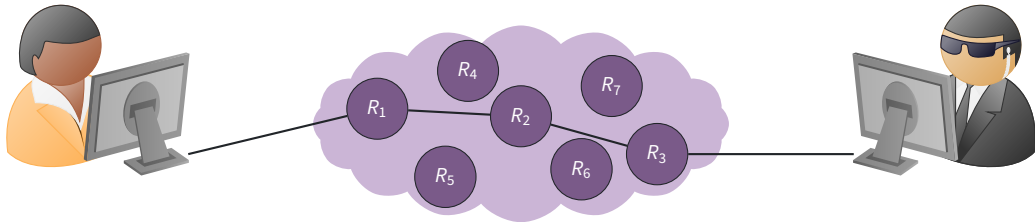


Threat Model

Alice

Anonymity Network

Bob



Anonymity isn't Encryption

Alice

Bob



...RG9uJ3QgdXNlIGJhc2U2NCBmb3IgZW5jcnlwdGlvbi4...



Gibberish!

Encryption just protects contents.

Communications Metadata



"We Kill People Based on Metadata."

—Michael Hayden, former director, NSA.

Attorney General Bill Barr Will Ask Zuckerberg To Halt Plans For End-To-End Encryption Across Facebook's Apps - Tor Browser

Attorney General Bill Barr W × +

https://www.buzzfeednews.com/article/ryanmac/bill-barr-facebook-letter-halt-encryption 110%

TECH

Attorney General Bill Barr Will Ask Zuckerberg To Halt Plans For End-To-End Encryption Across Facebook's Apps

"We are writing to request that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety."

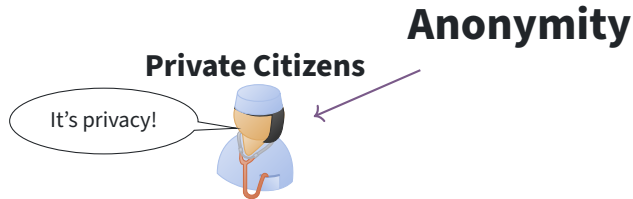
 **Ryan Mac**
BuzzFeed News Reporter

 **Joseph Bernstein**
BuzzFeed News Reporter

Last updated on October 3, 2019, at 3:28 p.m. ET
Posted on October 3, 2019, at 1:36 p.m. ET

 [Tweet](#)  [Share](#)  [Copy](#)

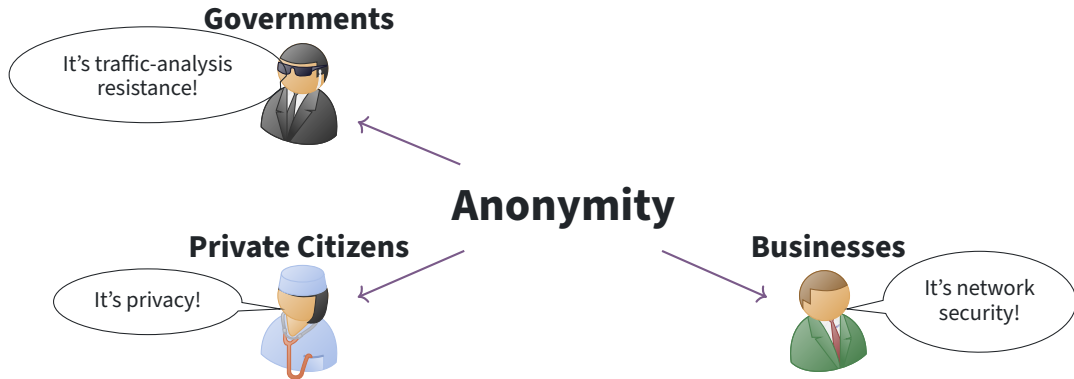
Anonymity is different for each use case



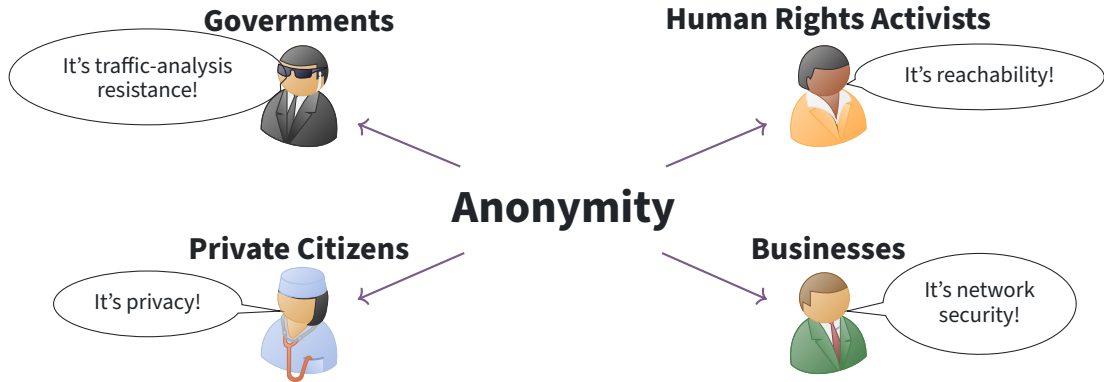
Anonymity is different for each use case



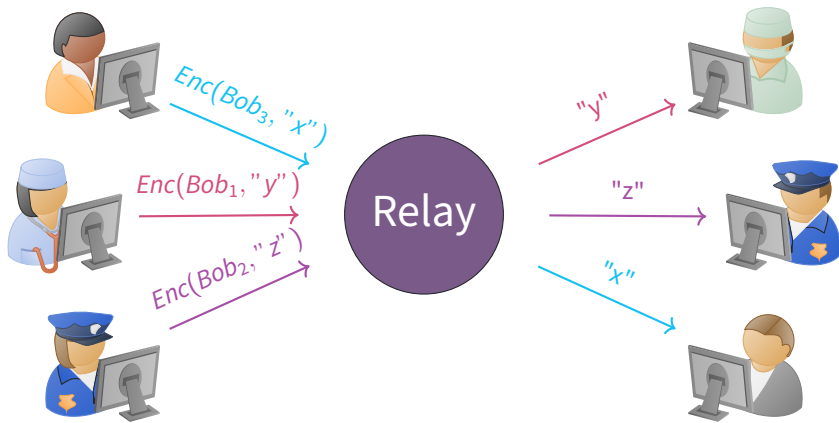
Anonymity is different for each use case



Anonymity is different for each use case

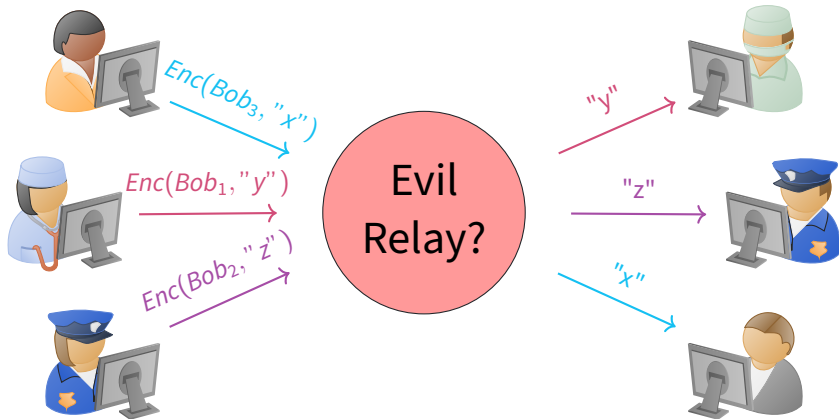


A Simple Design

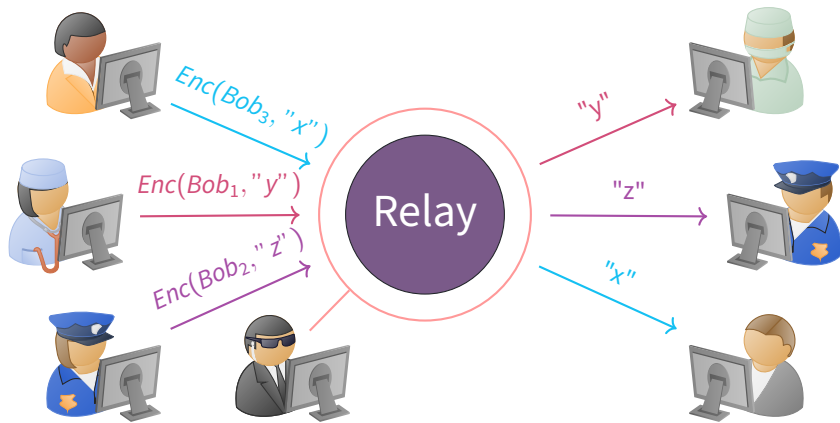


Equivalent to most commercial proxy/VPN providers.

A Simple Design

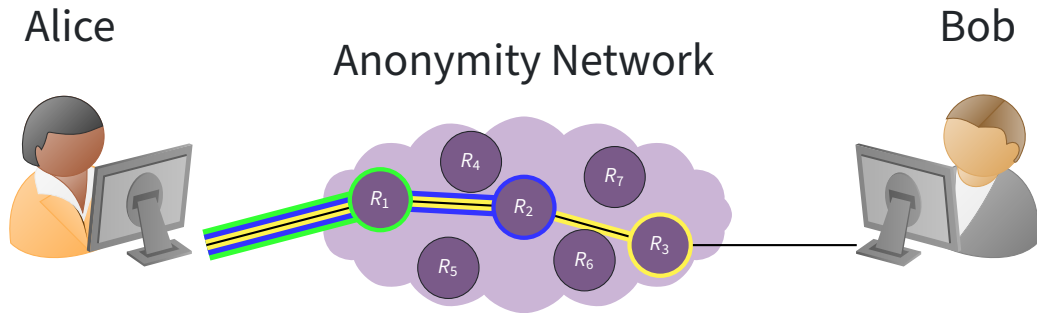


A Simple Design



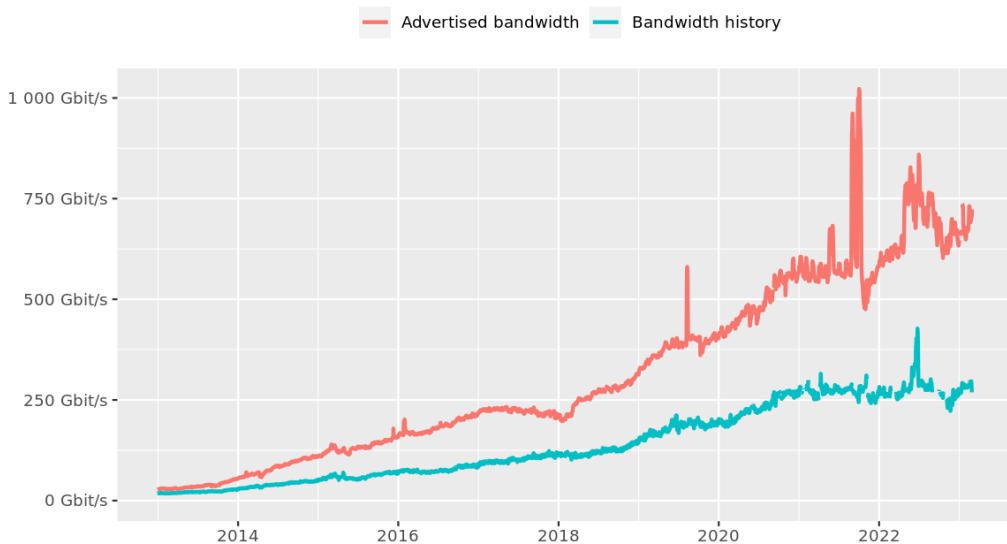
Timing analysis lets an observer match up connections.

The Tor Design



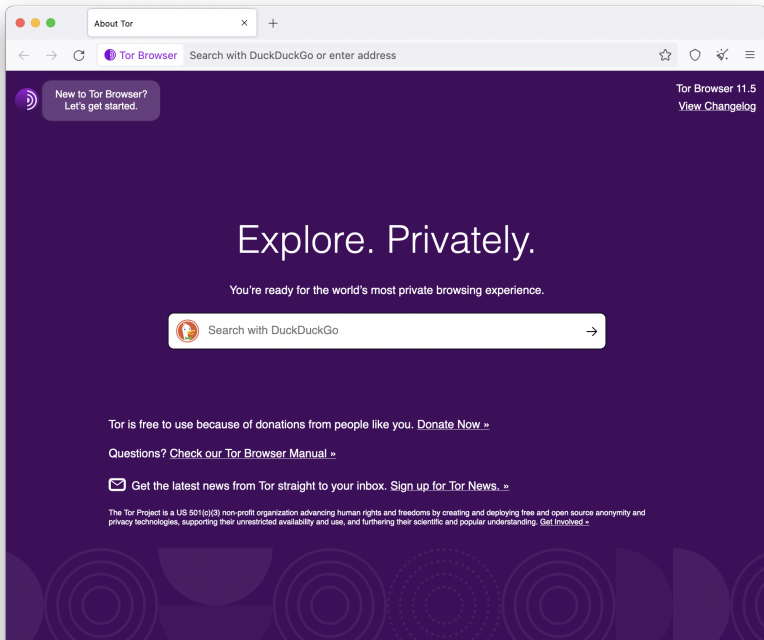
Multiple relays so no single relay can link Alice to Bob.

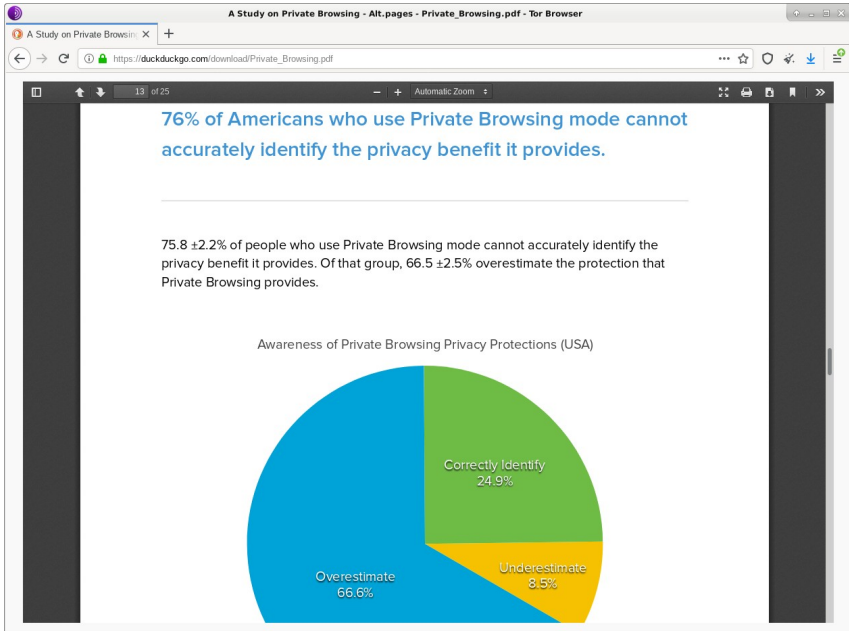
Total relay bandwidth



Tor's **safety** comes from **diversity**

1. Diversity of relays. The more relays we have and the more diverse they are, the fewer attackers are in a position to do traffic confirmation. Research problem: How do we measure diversity over time?
2. Diversity of users and reasons to use it. 50000 users in Iran means almost all of them are normal citizens.





Transparency for Tor is key

- Open source / free software
- Public design documents and specifications
- Publicly identified developers

Transparency for Tor is key

- Open source / free software
- Public design documents and specifications
- Publicly identified developers
- Not a contradiction: privacy is about choice!

Growing your community | sustainability

Volunteer ecosystem, commons vs capitalism

Individual sustainability, keeping motivated long term

Funding tied into sustainability too: reproduce capitalism? get govt funding? charge per user?



Telnet Is Not A Crime: Unconvincing Prosecution Screenshot Leaked in Ola Bini Case

BY [DANNY O'BRIEN](#) | AUGUST 23, 2019



ESPAÑOL

Since EFF [visited Ecuador three weeks ago](#), the investigation into open source developer Ola Bini has proceeded as we described then: drawn out, with little evidence of wrong-doing, but potentially compromised by acts of political theater outside the bounds of due process and a fair trial.

Technology is not neutral

Power imbalances are central to Tor: it's more useful to vulnerable people than those who already have power.

Technology is inherently political!

But that doesn't mean we need to like or endorse or talk about all of our users. 'Absolute free speech' vs 'framing and community-building' vs 'how the system works technically'.

The crypto wars

We should take as many lessons as we can from the https win.

If you hear that NSA stores encrypted traffic for longer, what do you do?

“Jurisdictional arbitrage”, MLATs, CLOUD act



1 Million People use Facebook over Tor



FACEBOOK OVER TOR · FRIDAY, APRIL 22, 2016

People who choose to communicate over Tor do so for a variety of reasons related to privacy, security and safety. As we've [written previously](#) it's important to us to provide methods for people to use our services securely – particularly if they lack reliable methods to do so.

Censorship implies surveillance

Recurring theme where western companies build the oppression tools

Censorship becoming more widespread in the west (e.g. RT.com in europe)

Iran's "halal internet" dreams, Russia heading there too over-there-istan

Center of privacy research

Thriving interaction with research community

Attacking Tor is challenging so it's where the academics go

And we help mentor grad students, clarify and highlight research questions, review papers, etc

Calls to action

Understand the risks of centralized architectures

Fight the slippery slope that is internet censorship

Participate in privacy research, e.g.

<https://petsymposium.org/>

Volunteer as a relay, a bridge, or a snowflake!

<https://donate.torproject.org/>