

Tor: Internet privacy in the age of big surveillance

Roger Dingledine, The Tor Project



Tor Overview

Online anonymity: open source, open network

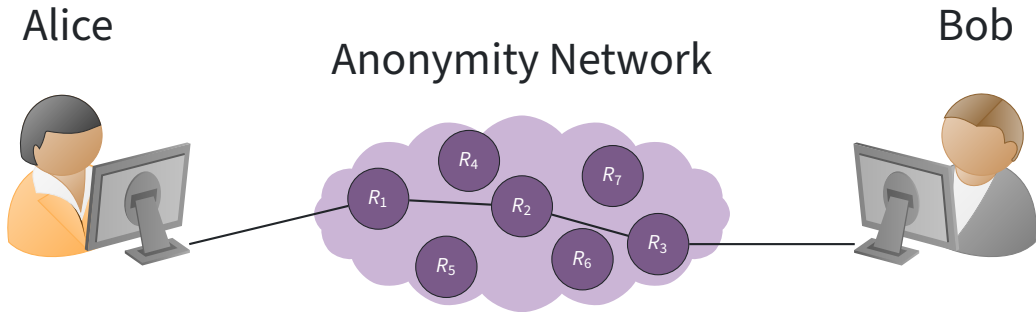
Community of devs, researchers, users, relay operators

US 501(c)(3) non-profit organization with 50ish staff

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

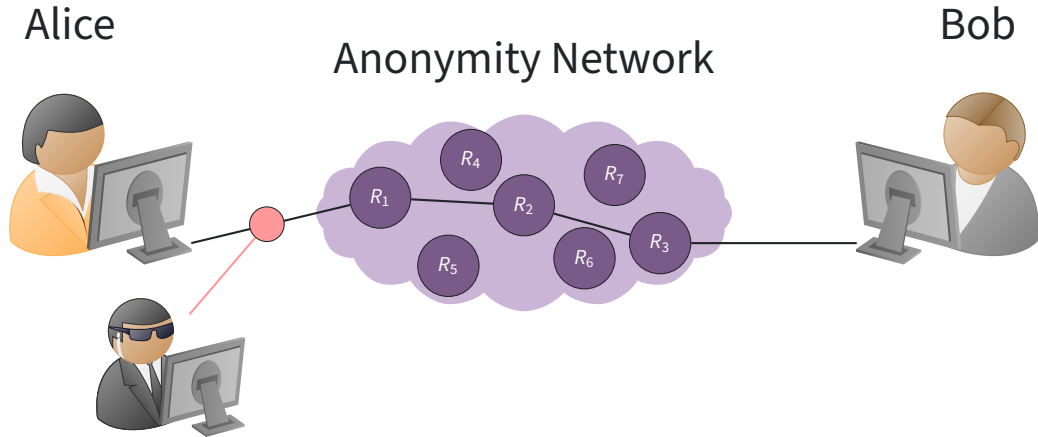
Part of larger ecosystems: internet freedom, free software, censorship resistance, anonymity research

Threat Model

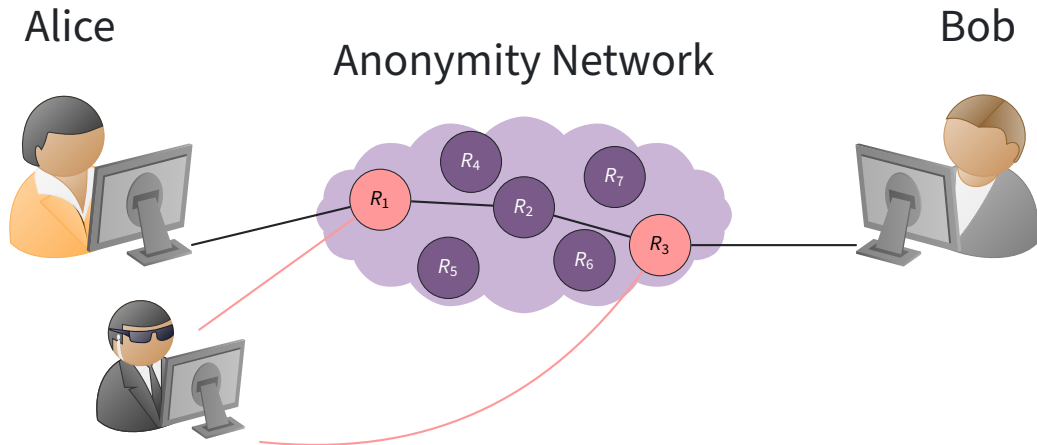


{What can the attacker do?}

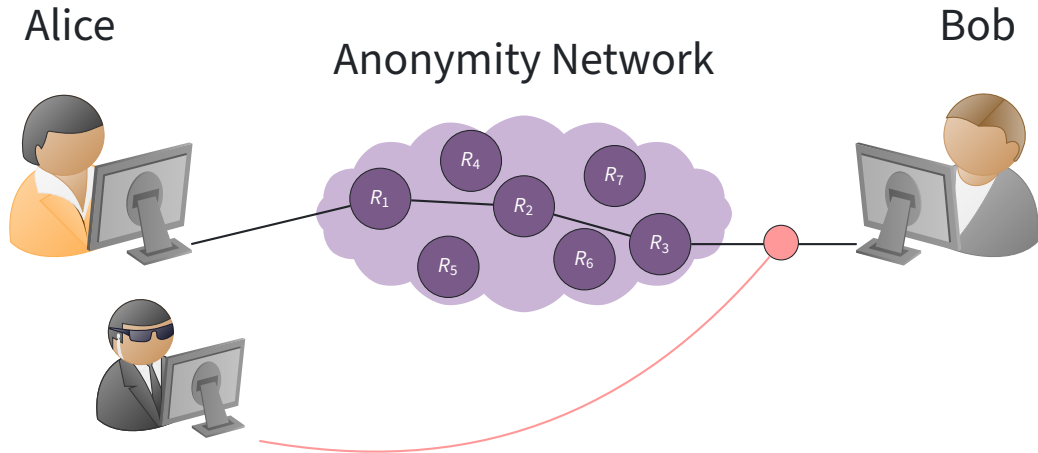
Threat Model



Threat Model



Threat Model

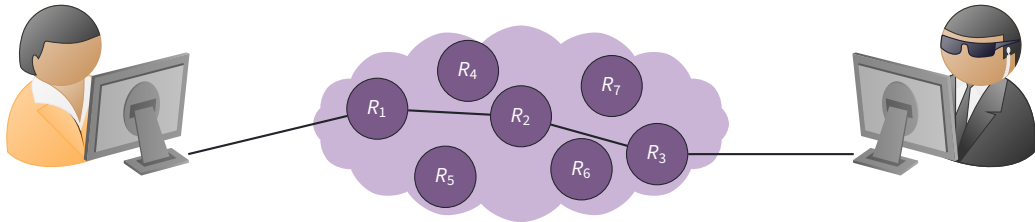


Threat Model

Alice

Anonymity Network

Bob



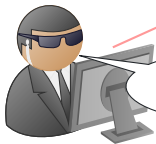
Anonymity isn't Encryption

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."

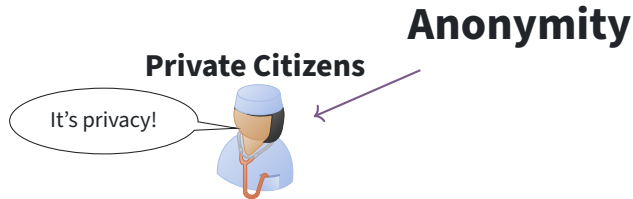
 **Ryan Mac**
BuzzFeed News Reporter

 **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](#)

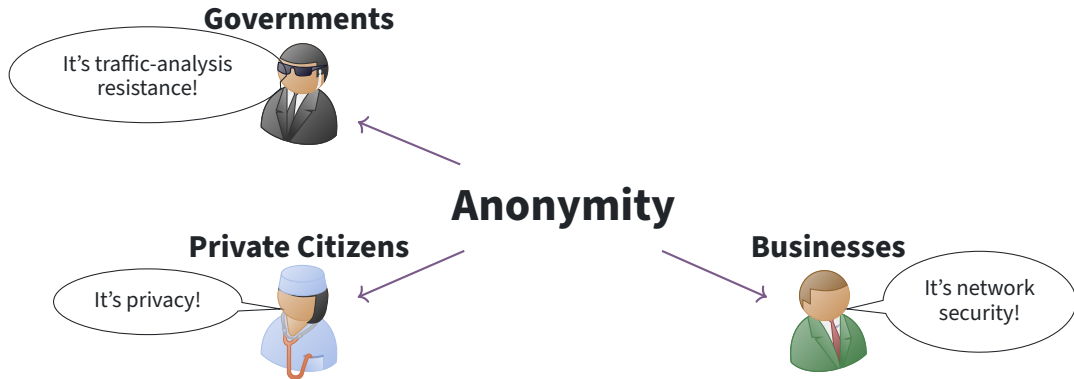
Anonymity is different for each use case



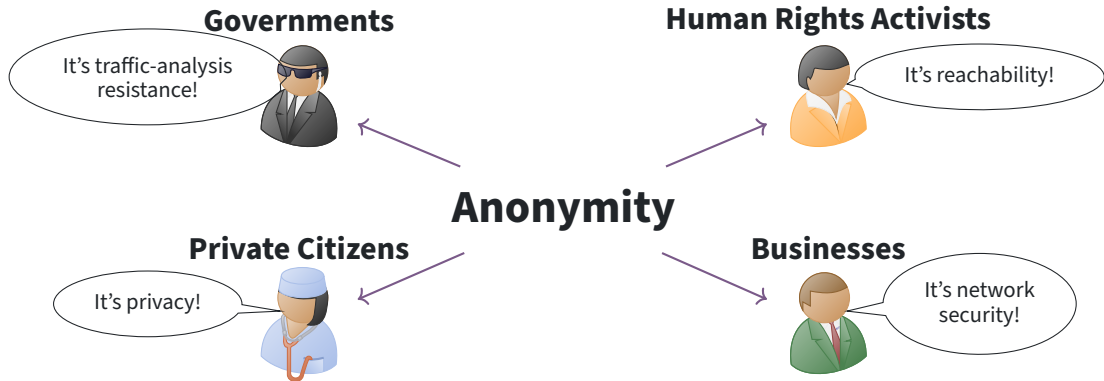
Anonymity is different for each use case



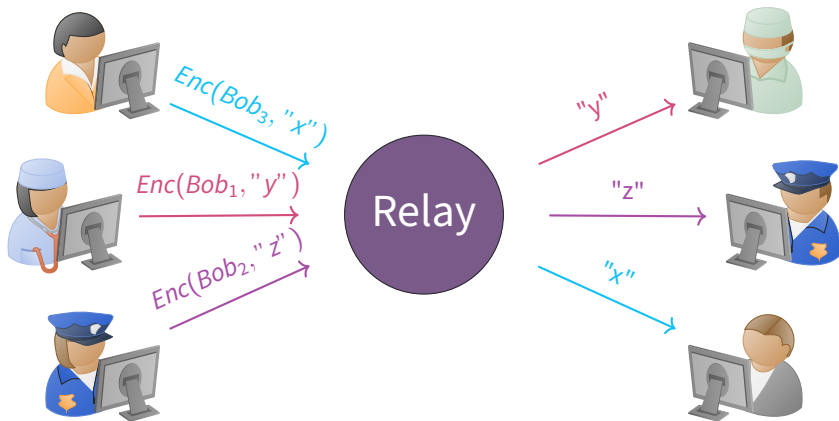
Anonymity is different for each use case



Anonymity is different for each use case

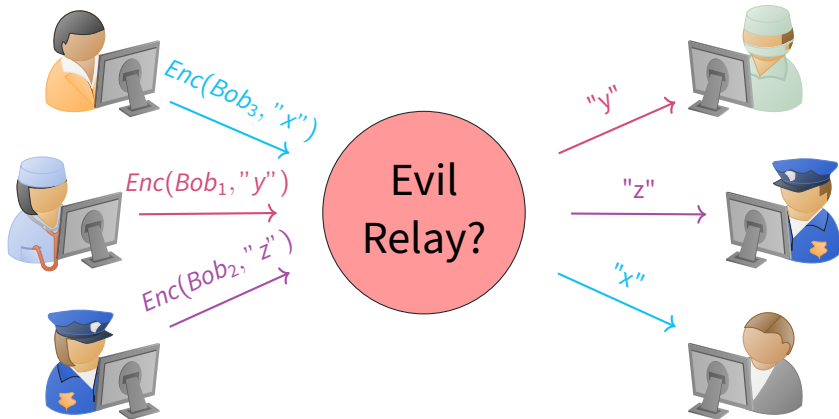


A Simple Design

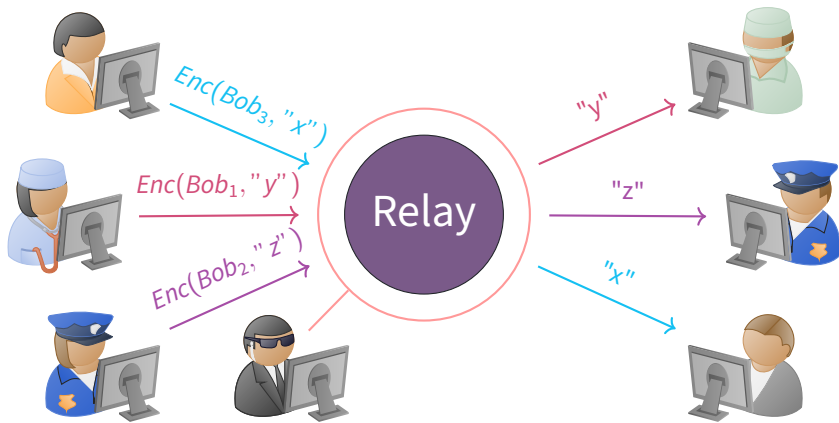


Equivalent to most commercial proxy/VPN providers.

A Simple Design

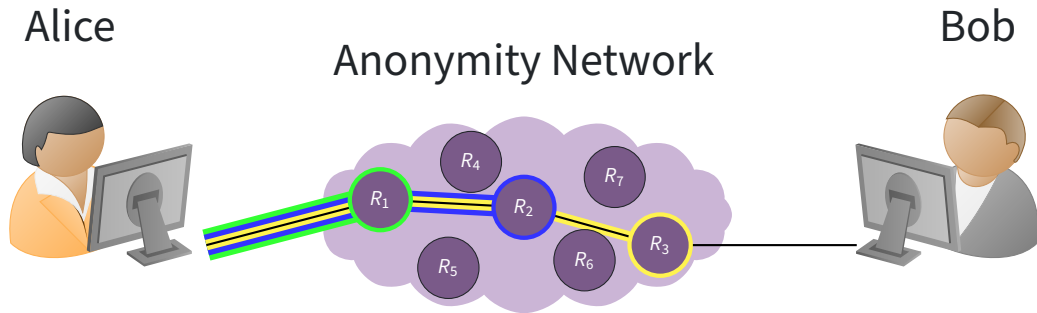


A Simple Design



Timing analysis lets an observer match up connections.

The Tor Design



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

I'm a political activist, part of a semi-criminalized minority.

In my younger years I entered the public debate openly, and as a result got harassed by government agencies. I later tried to obfuscate my identity, but I found that my government has surprisingly broad powers to track down dissidents.

Only by using anonymizing means, among which Tor is key, can I get my message out without having police come to "check my papers" in the middle of the night. **Tor allows me freedom to publish my message to the world without being personally persecuted for it.**

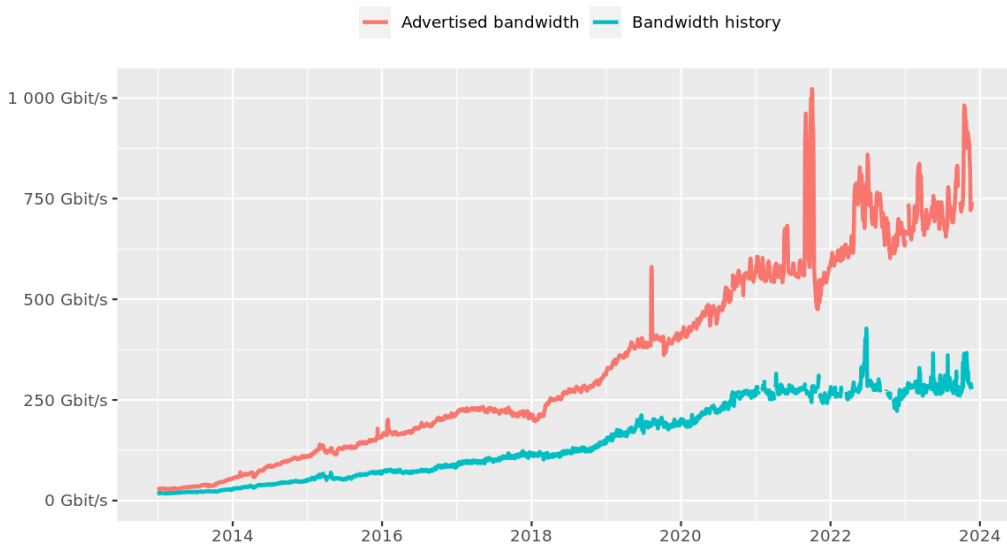
—Anonymous Tor User

I'm a doctor in a very political town. I have patients who work on legislation that can mean billions of dollars to major telecom, social media, and search concerns.

When I have to do research on diseases and treatment or look into aspects of my patients' histories, I am well aware that my search histories might be correlated to patient visits and leak information about their health, families, and personal lives. **I use Tor to do much of my research when I think there is a risk of correlating it to patient visits.**

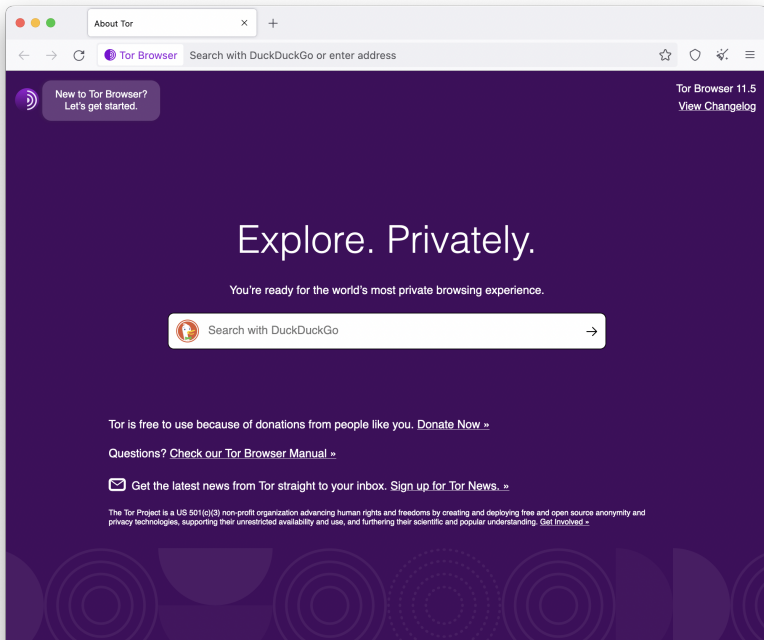
—Anonymous Tor User

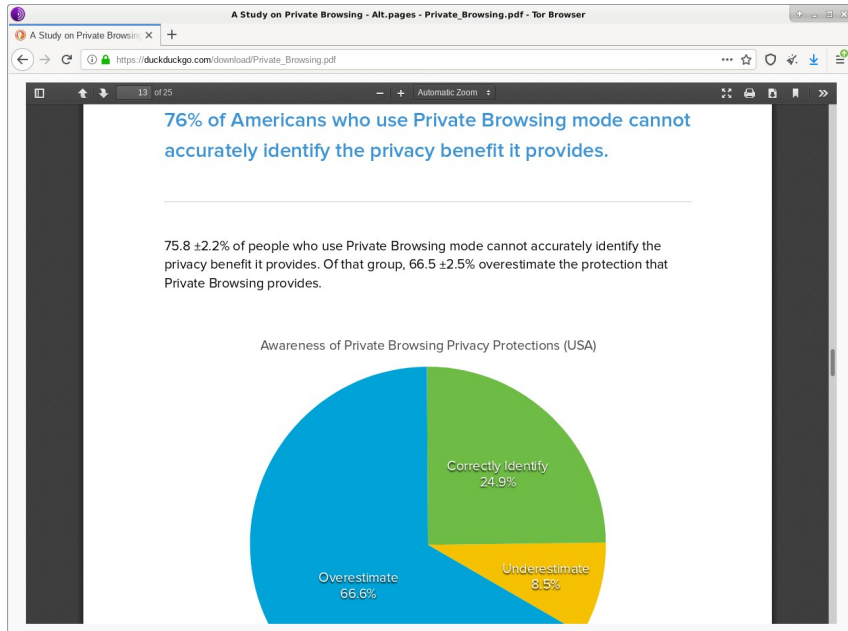
Total relay bandwidth

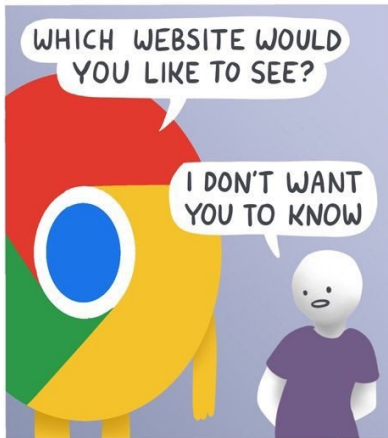


Tor's **safety** comes from **diversity**

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.







@SKELETON_CLAW



SKELETONCLAW.COM

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!



Technology is not neutral

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

Dual-use technology is inherently political!

يالله بالستر...!



تصفح بأمان!

غذارة هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.

تشكل شبكة الانترنت وسيلة للتواصل والمعرفة وخدمة تطبيقات حياتنا اليومية. وقد جلب الموقع الذي ترغب بخدماته محتويات مدمجة تحت "قائمة المحتويات المحظورة" حسب تصنيف "الهيئة التنظيمية لخدمة الانترنت" لدولة الإمارات العربية المتحدة.

إذا كنت تترك وتبحث عن محتوى مختلف، الرجاء، انقر هنا.

Surf Safely!

This website is not accessible in the UAE.

The Internet is a powerful medium for communication, sharing and serving our daily learning needs. However, the site you are trying to access contains content that is prohibited under the "Internet Access Management Regulatory Policy of the Telecommunications Regulatory Authority of the United Arab Emirates".

If you believe the website you are trying to access does not contain any such content, please [click here](#).

© 2009 communications.gov.ae

خطرا!



تصفح بأمان!

غذارة هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.

تشكل شبكة الانترنت وسيلة للتواصل والمعرفة وخدمة تطبيقات حياتنا اليومية. وقد جلب الموقع الذي ترغب بخدماته محتويات مدمجة تحت "قائمة المحتويات المحظورة" حسب تصنيف "الهيئة التنظيمية لخدمة الانترنت" لدولة الإمارات العربية المتحدة.

إذا كنت تترك وتبحث عن محتوى مختلف، الرجاء، انقر هنا.

Surf Safely!

This website is not accessible in the UAE.

The Internet is a powerful medium for communication, sharing and serving our daily learning needs. However, the site you are trying to access contains content that is prohibited under the "Internet Access Management Regulatory Policy of the Telecommunications Regulatory Authority of the United Arab Emirates".

If you believe the website you are trying to access does not contain any such content, please [click here](#).

هذا الموقع محظور

This site is blocked

الوصول إلى هذا الموقع غير مسموح به حالياً لأنه مصنف ضمن قوائم المحتويات المحظورة بموجب أحكام السياسة التنظيمية لإدارة النفاذ إلى الإنترنت في دولة الإمارات العربية المتحدة.

Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE's Internet Access Management Policy.

إذا كنت ترغب في إعادة النظر في تصنيف هذا الموقع، يرجى الفصل بطلبية استعراض للمحتويات.

If you would like the classification on this site to be reviewed, please fill in and submit the Feedback Form.

Access Denied

Your request was denied because of its content categorization: "Computers/Internet/Proxy Avoids"

http://torproject.org/

Dear User,

Sorry, the requested page is unavailable.

المطلوب غير متاح.

If you believe the requested page should not be blocked please [click here](#).

إذا كنت ترى أن هذه الصفحة ينبغي أن لا تكون محظورة، نرجو منك تقديم تعليق.

For more information about internet services in Saudi Arabia, please click here: [www.internet.gov.sa](#)

للمزيد من المعلومات عن الخدمات الإلكترونية في المملكة العربية السعودية، يرجى النقر هنا: [www.internet.gov.sa](#)

أف! oops

قد تم منع النفاذ إلى هذا الموقع

This site has been blocked

تم إيقاف عملية النفاذ إلى الموقع الذي تحاول زيارته نظرًا لاحتوائه على محتويات محظورة.

The web page you are trying to access has been blocked as the content contains prohibited material.

إذا كنت ترى أن هذه الصفحة ينبغي أن لا تكون محظورة، نرجو منك تقديم تعليق.

If you believe the requested page should not be blocked please [click here](#).

Access is prohibited

الموقع الذي تحاول زيارته محظور

Access to this website is prohibited

الموقع الذي تحاول زيارته محظور نظرًا لاحتوائه على محتويات محظورة.

The site is blocked according to the government filtering policy. If you find this page has been blocked in error, kindly fill out the form and we will investigate.

Thank You

Registered fields are required by

Full Name *

Email *

Blocked URL *

Comments

Submit

Sorry, the requested page is unavailable.

If you believe the requested page should not be blocked please [click here](#).

عذراً، الموقع المطلوب غير متاح.

إن كنت ترى أن هذه الصفحة ينبغي أن لا تكون محظورة، نرجو منك تقديم تعليق.

For more information about internet services in Saudi Arabia, please click here: [www.internet.gov.sa](#)

للمزيد من المعلومات عن الخدمات الإلكترونية في المملكة العربية السعودية، يرجى النقر هنا: [www.internet.gov.sa](#)

عزيزي العميل: تم حجب هذا الموقع بناءً على اللوائح والقوانين.

بأن هناك خطأ يرجى إرسال رسالة على البريد الإلكتروني unblock.kw@kw.zain.com مع ذكر عنوان الموقع الذي تم حجب.

Dear Customer: This site has been blocked according to the regulations and laws of the Kingdom of Bahrain.

Site Blocked

This web site has been blocked for violating regulations and laws of Kingdom of Bahrain.

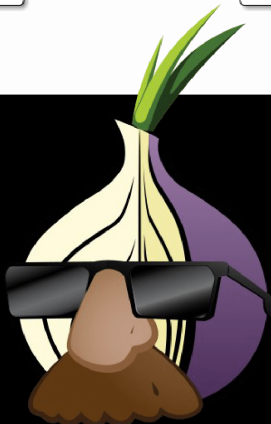
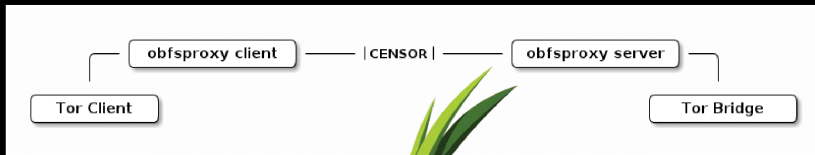
الموقع محظور

هذا الموقع محظور لأنه انتهك الأنظمة والقوانين في مملكة البحرين.

If you believe the requested page should not be blocked please [click here](#).

إذا كنت ترى أن هذه الصفحة ينبغي أن لا تكون محظورة، نرجو منك تقديم تعليق.

Pluggable transports



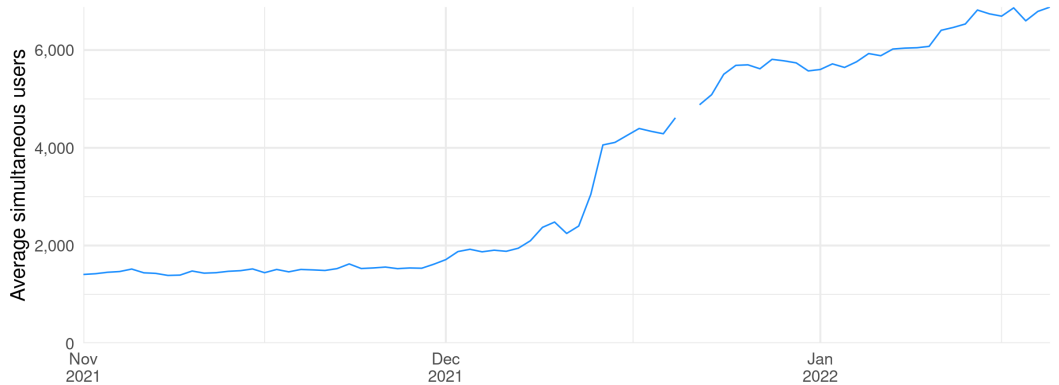
Snowflake pluggable transport

Snowflake makes your traffic look like a WebRTC (zoom, jitsi, skype, signal, etc) call, and those are allowed in many parts of the world.

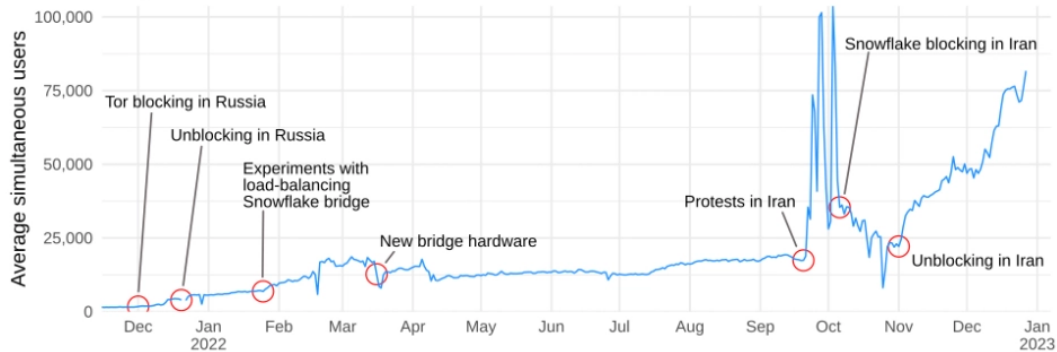
People can volunteer as Snowflake proxies simply by installing an extension in their browser.

The resulting volume and variety of volunteers gives us more options on how to distribute them to users.

Daily snowflake users



Daily Snowflake users in 2022



Arms races

Censorship arms race is bad

Surveillance arms race is worse

...and centralization of the internet makes it worse still

I CAN HAZ
FREEDOM?



Censorship implies surveillance

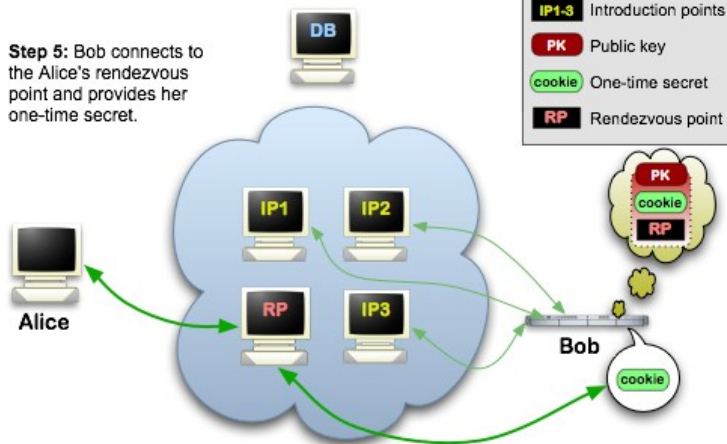
Recurring theme where western companies build the oppression tools

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

Tor Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.



Onion service properties

- Self authenticated
- End-to-end encrypted
- Built-in NAT punching
- Limit surface area
- No need to “exit” from Tor





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.

BBC Blogs - Technology & Creativity Blog - Leveraging the Tor Network to circumvent blocking of BBC News content - Tor Browser

BBC Blogs - Technology & Creativity Blog

https://www.bbc.co.uk/blogs/internet/entries/936e460a-03b3-41db-be96-a6f2f27934e6

BBC

Sign in

News

Sport

Reel

Worklife

Travel

Future

More

Search

Technology + Creativity Blog

Previous

Home

Next

Leveraging the Tor Network to circumvent blocking of BBC News content

Wednesday 30 October 2019, 8:18



Abdallah al-Salmi
Strategy Analyst, BBC News

Tagged with: [BBC News](#), [BBC World Service](#), [Media Distribution](#), [Public Service](#)

COMMENTS

The BBC World Service's news content [became available on the Tor Network last week](#) in a move that attracted wide media attention.

The decision to go ahead with setting this service up came at a time when BBC News is either blocked or restricted in several parts of the world.

For example, in Egypt, Iran and China, our audiences are finding it either impossible or difficult to access our content without the use of a circumvention tool, such as a VPN.

The Tor Network is an overlay network on the internet, which provides increased security and is resistant to blocking.

About this Blog



Staff from the BBC's online and technology teams talk about BBC Online, BBC iPlayer, BBC Red Button and the BBC's digital services. The blog is reactively moderated. Your host is Jonathan Murphy.

Follow [Technology & Creativity Blog](#) on Twitter

[Blog home](#)
[Explore all BBC blogs](#)

Blog Updates

Stay updated with the latest posts from the blog

41

Contact Sales: +1 (888) 274-3482



The Cloudflare Blog

Keep up to date with Cloudflare's latest news. Subscribe to the Blog.

Email Address

Subscribe

Product News

Speed & Reliability

Security

Serverless

Cloudflare Network

Developers

Deep Dive

Life @Cloudflare



Introducing the Cloudflare Onion Service

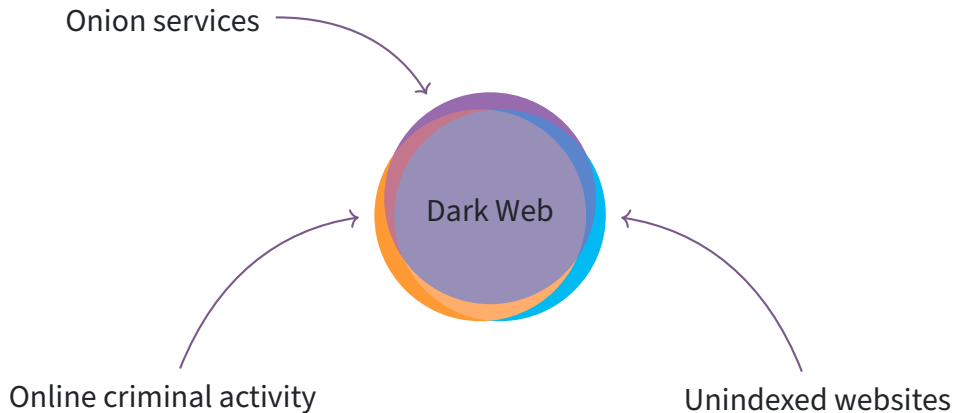
[Tweet](#)



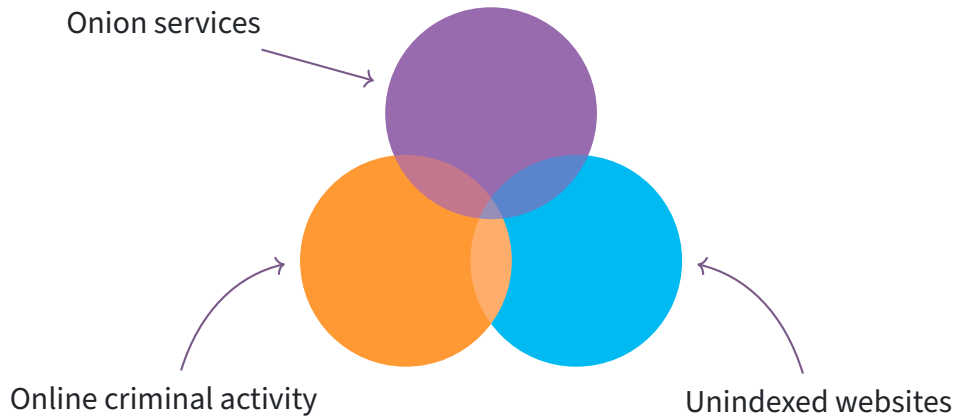
Mahrud Sayrafi

September 20, 2018 12:00PM

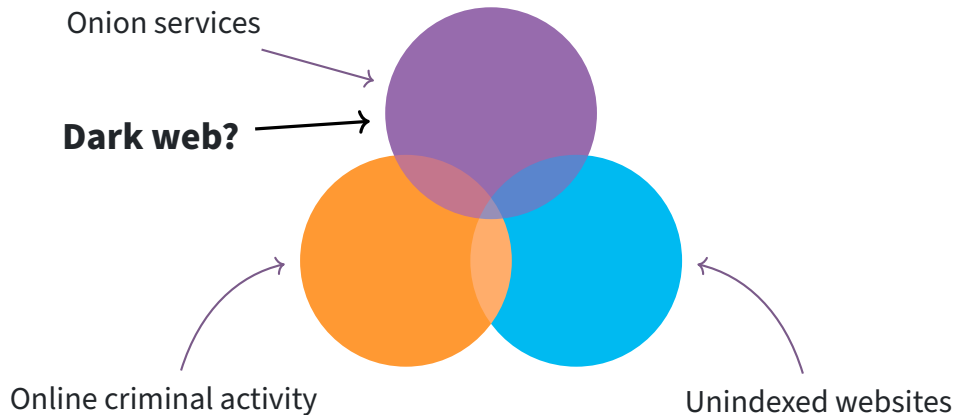




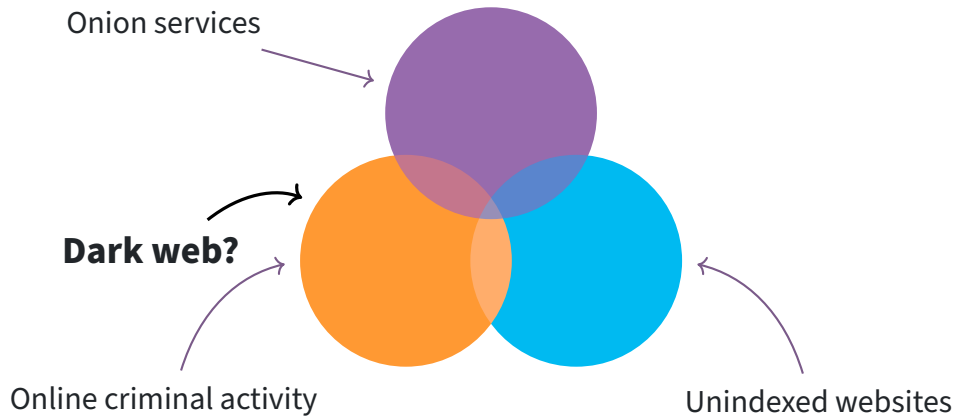
The "Dark Web" as popularly depicted



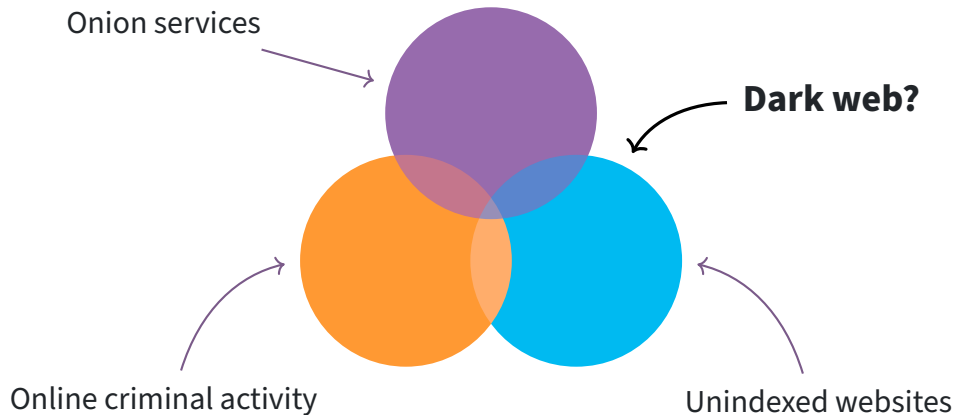
Closer to reality



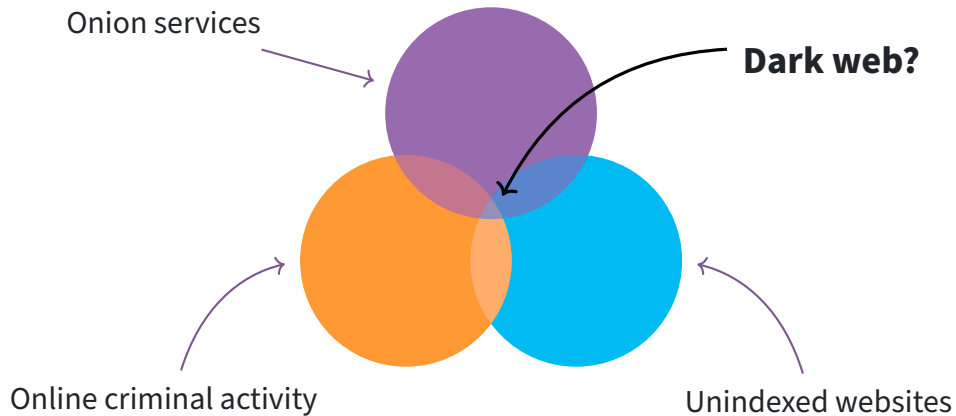
Closer to reality



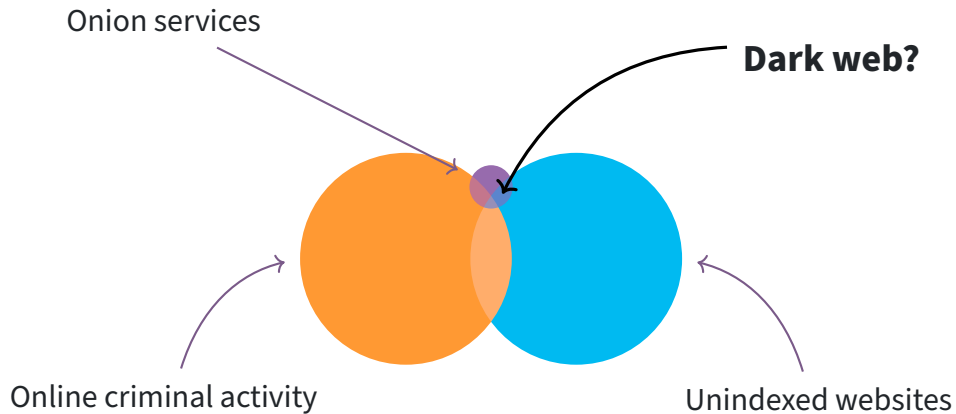
Closer to reality



Closer to reality

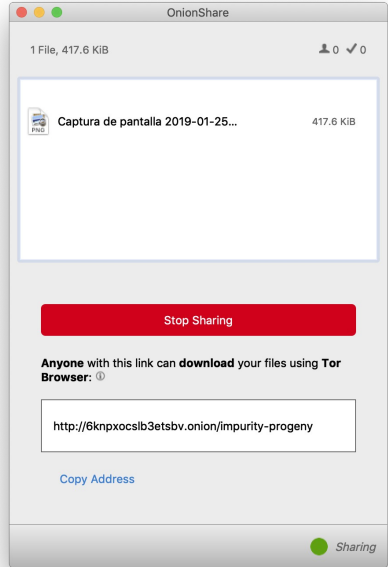
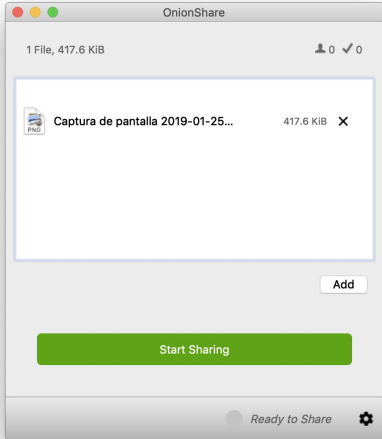


Closer to reality

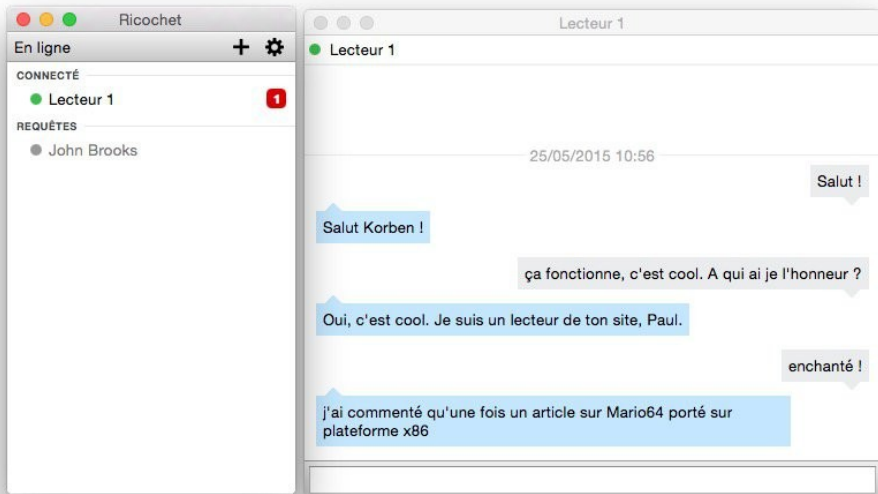


Scale also matters

OnionShare



Ricochet



Tor isn't foolproof

- Opsec mistakes
- Browser metadata fingerprints
- Browser exploits
- Traffic analysis



I WANT TO RUN A RELAY

YOU'LL NEED TO DO THE FOLLOWING

1

CHOOSE A RELAY

2

FIND ALLIES

3

GET A PRIZE

1

CHOOSE YOUR RELAY



Calls to action

Understand the risks of centralized architectures

Fight the slippery slope that is internet censorship

Participate in privacy / censorship research, e.g.

<https://petsymposium.org/>

<https://foci.community/>

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