

SSH Tunnels, VPNs, Proxies, and Tor

Chris Bailey, 2/18/17

What are they?

Methods of redirecting and securing network traffic

Work differently

Different use cases

Different threat models

Why use them?

Avoiding censorship

Anonymity*

Privacy*

Security*

*In theory, if you use them correctly and your adversary has limited resources

Proxies

Sit between you and your destination, relaying traffic

Your destination sees the proxy's IP, not yours



Downsides

No protocol-level encryption (SOCKS)

Requires you to trust the proxy operator

SSH Tunneling

Uses an SSH connection to relay traffic

Securely encrypted

Can redirect a single port

Can act as a SOCKS proxy

SSH Tunneling

Extremely easy to use

To forward a single port (3389) from you to example.com:

```
ssh example.com -L 3389:localhost:3389
```

To create a SOCKS proxy on port 8080:

```
ssh example.com -D 8080
```

Downsides

Requires access to an SSH server

Not easily compatible with mobile devices

VPNs

Create a secure virtual connection between you and a remote network (or the whole internet)

Easy to set up on iOS/Android

VPN Protocols

IPSec/L2TP

- Mostly secure
- Immensely difficult to set up (last time I tried, anyway)

PPTP

- Cryptographically broken
- Don't use it for anything

VPN Protocols

OpenVPN

- Secure
- Not terrible to set up

SSTP

- Proprietary Microsoft VPN
- Available in Vista SP1+
- Similar to OpenVPN

Downsides

Requires you to trust the VPN operator

Tor

Global volunteer-run onion-routing anonymity network

Designed with anti-censorship in mind, difficult to block

Controversial: used by criminals, activists, spies, journalists, whistleblowers, law enforcement, etc.

Allows access to both regular internet and Tor-only “Hidden Services”

How Tor Works: 1



Tor node



unencrypted link



encrypted link

Alice



Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.



Dave

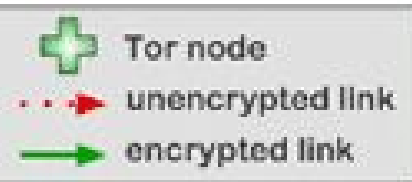


Jane



Bob

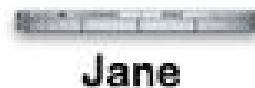
How Tor Works: 2



Alice



Step 2: Alice's Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.



Jane



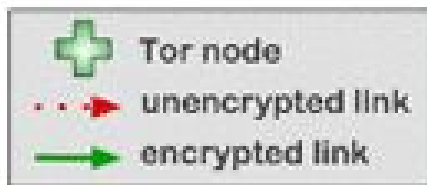
Dave



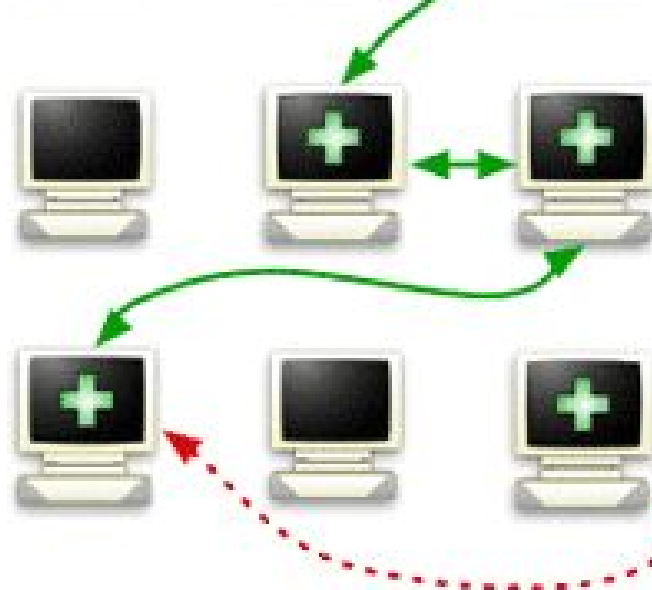
Bob



How Tor Works: 3

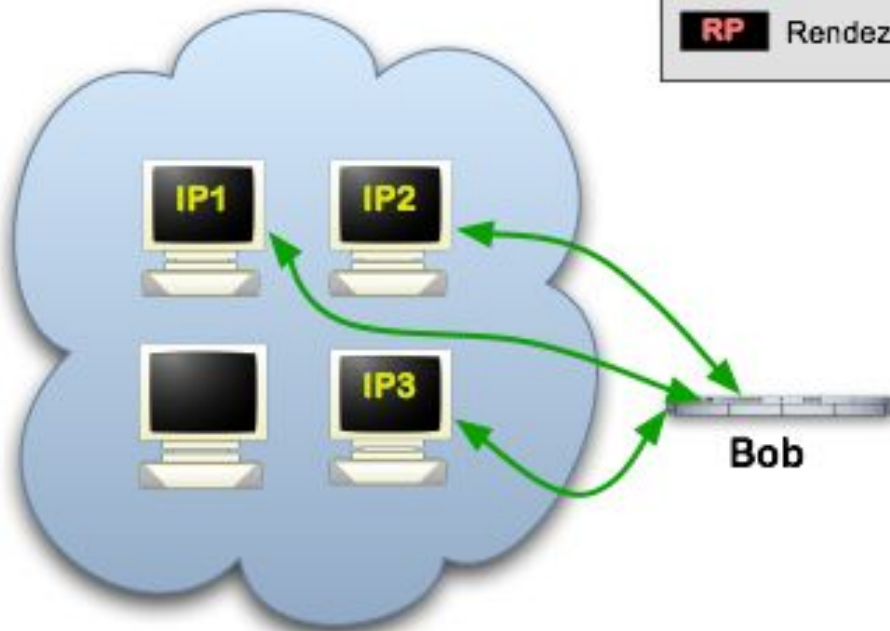


Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.



Tor Hidden Services: 1

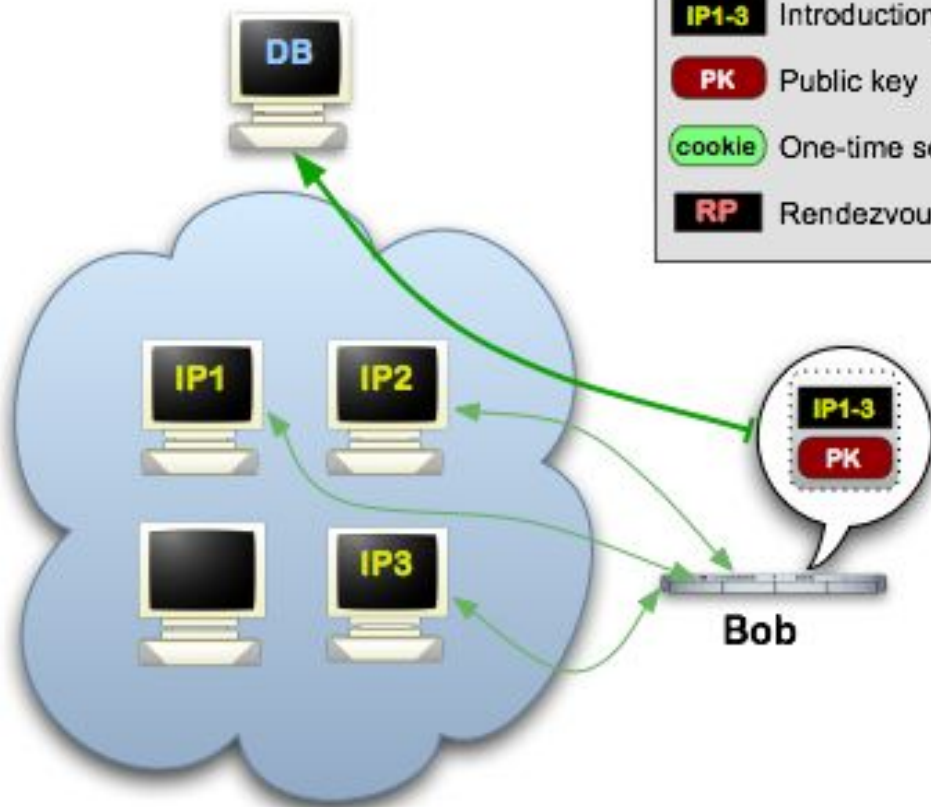
Step 1: Bob picks some introduction points and builds circuits to them.









-  Tor cloud
-  Tor circuit
-  IP1-3 Introduction points
-  PK Public key
-  cookie One-time secret
-  RP Rendezvous point

Tor Hidden Services: 2

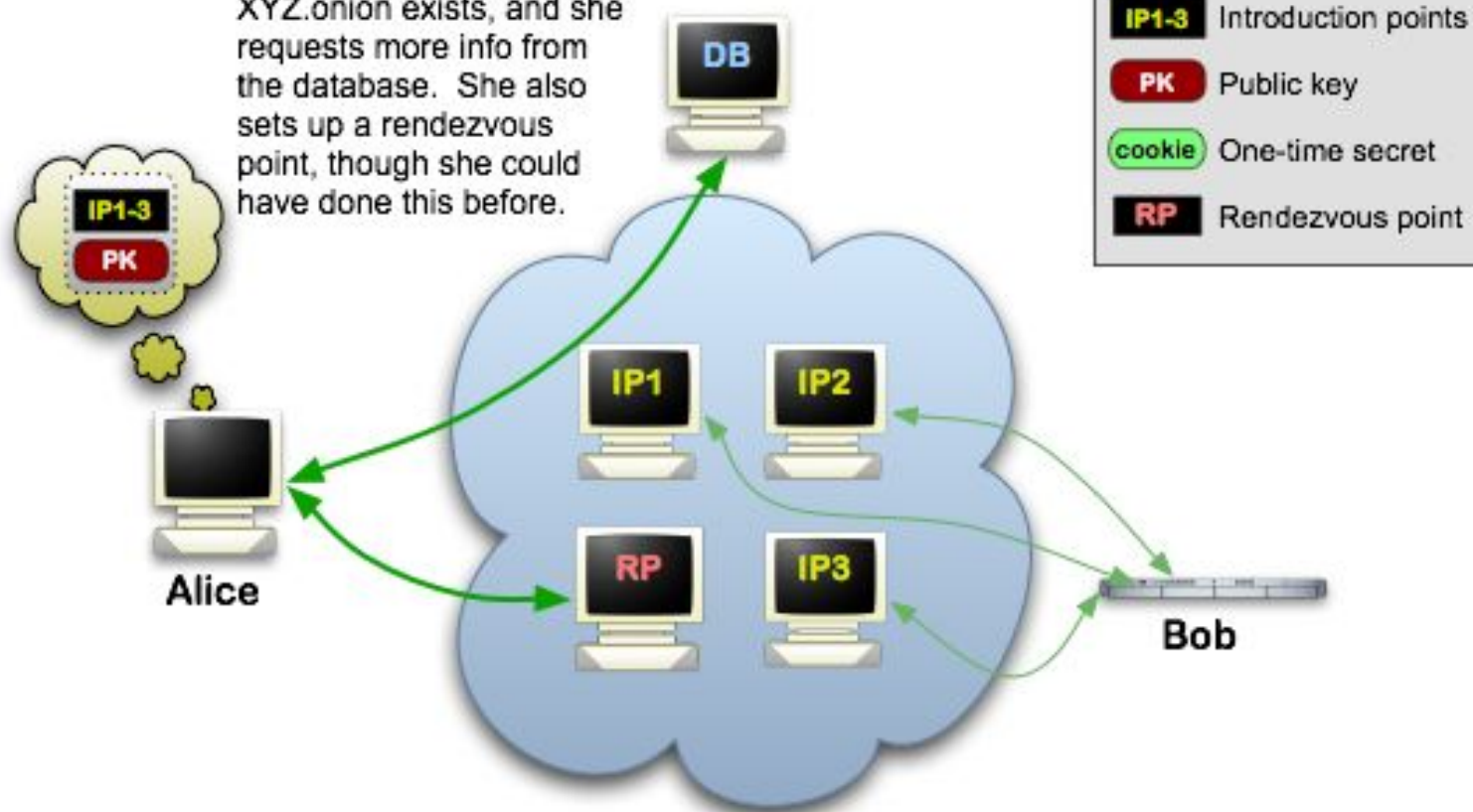
Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.



-  Tor cloud
-  Tor circuit
-  Introduction points
-  Public key
-  One-time secret
-  Rendezvous point

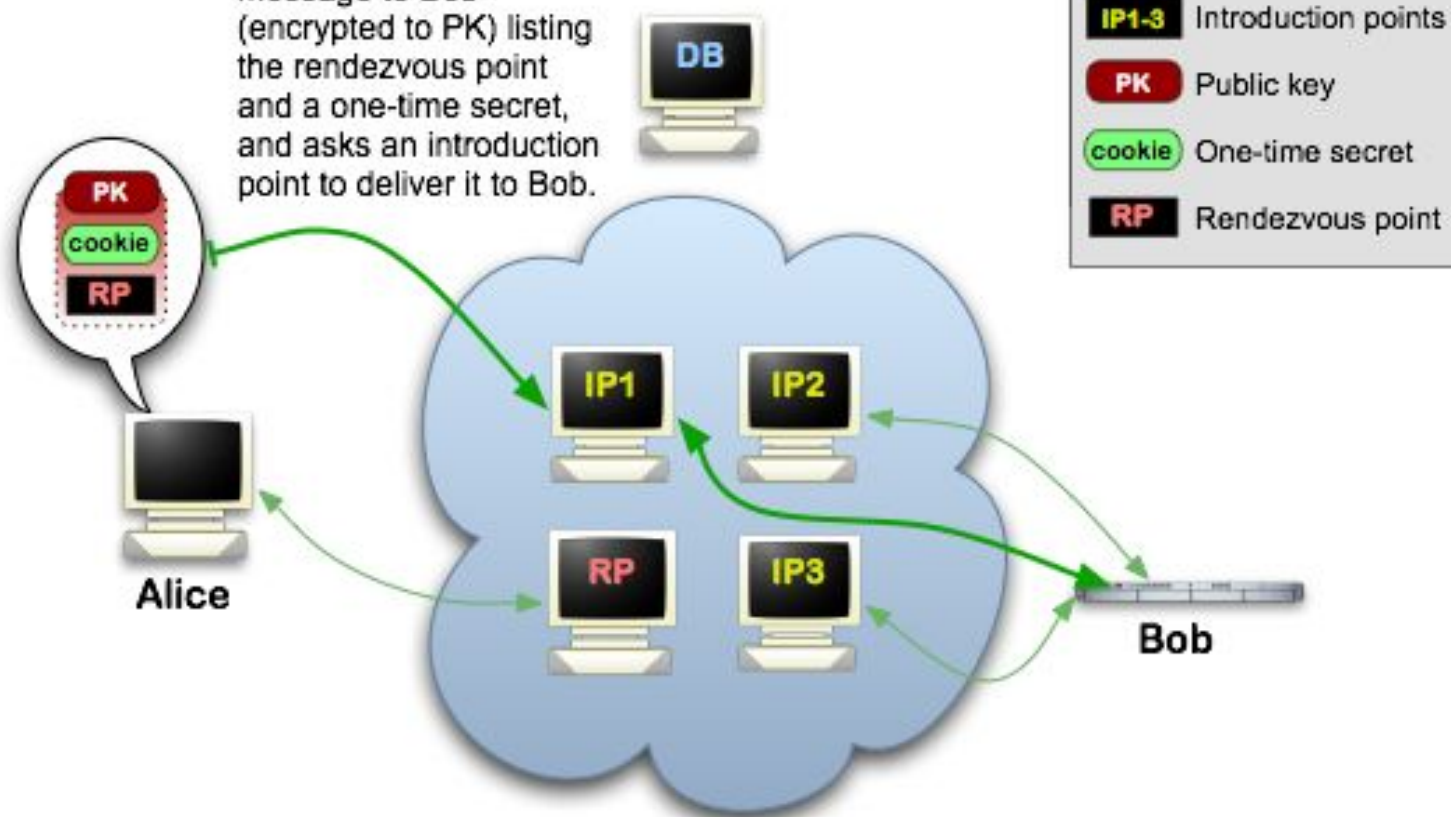
Tor Hidden Services: 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



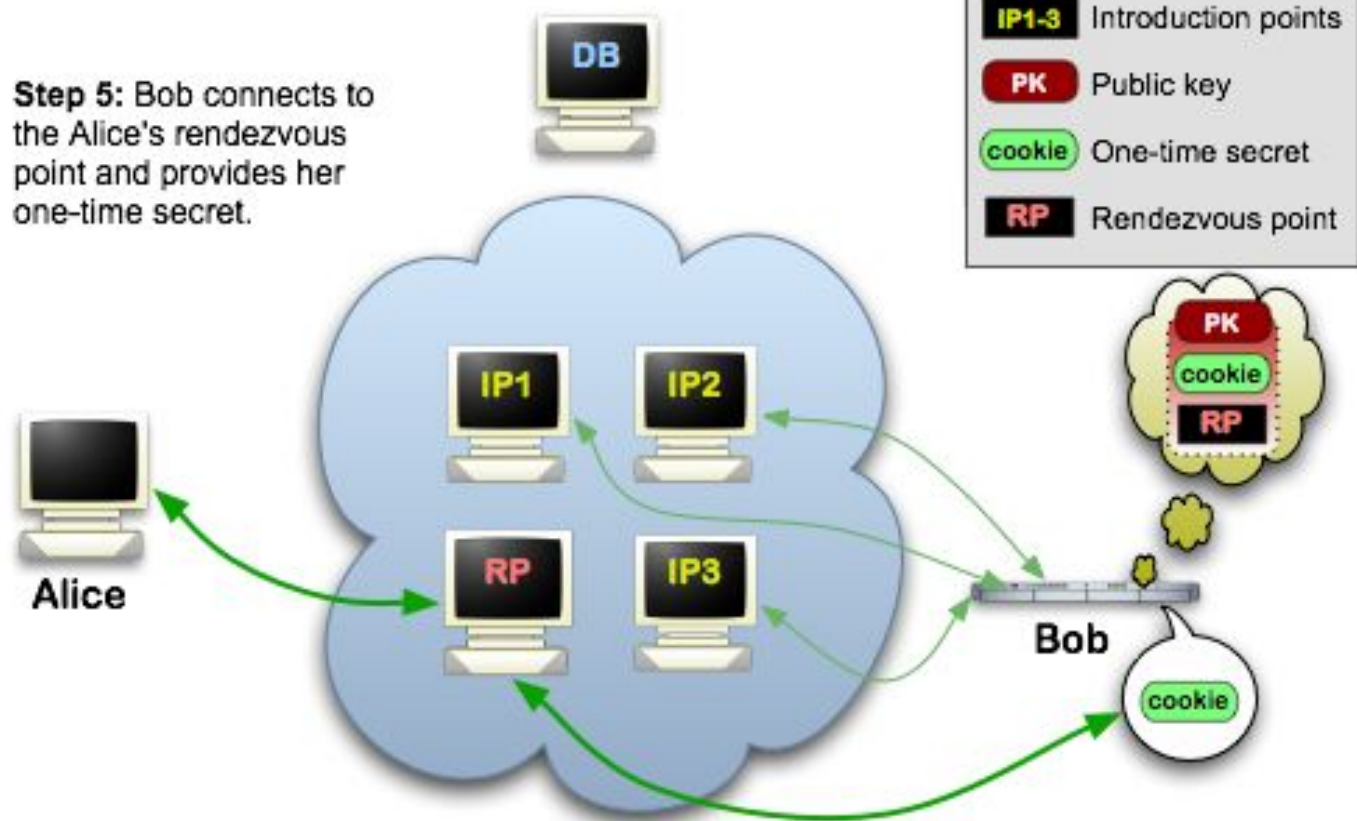
Tor Hidden Services: 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



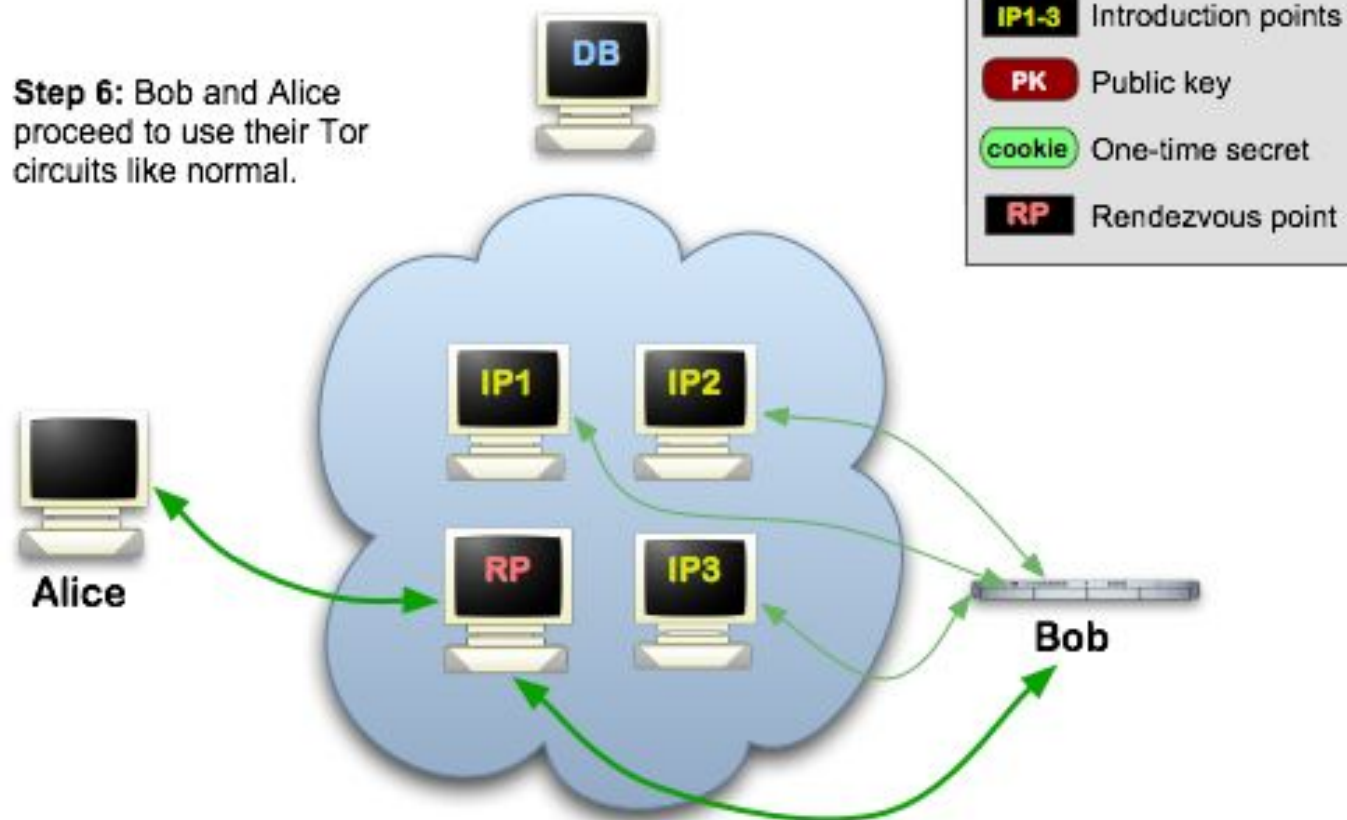
Tor Hidden Services: 5

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



Tor Hidden Services: 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.



Legitimate Hidden Services

New York Times SecureDrop

- nytimes2tsqtnxek.onion

Debian

- sejnfjr6szgca7v.onion

Facebook

- facebookcorewwi.onion

Downsides

Exit nodes can be and frequently are untrustworthy

If someone owns enough relays, they can deanonymize users

Not perfect -- Vulnerabilities in Firefox, etc. can still leak your real IP

Summary

Raw SOCKS proxies aren't a great idea

SSH tunnels and VPNs are great, but require trusting providers -- run your own!

Tor is cool, but be careful about the traffic you send through it, and make sure it's encrypted beyond what Tor provides

Which one should I use for crime?

None of them, because crime is bad

Even with secure technology, you can still be deanonymized through poor OPSEC

If the NSA wants to track you down, they will

Lab Scenario

You're a journalist working with a source in the Free People's Democracy of Authoritaria, a brutal Southeast-Canadian dictatorship.

Your goal is to use techniques discussed today to make contact with your source and retrieve a cache of government documents.

Further briefing can be found at

<https://innocuous.biz/lab/>