Hacking//Hustling: Intro to Tor and VPNs

Sophie Searcy

Who are we

t4tech leads trans-centered tech education around NYC

Keep up with us to see upcoming events teaching:

- Resume writing
- Web development
- Python
- Javascript
- Data Science

@t4techNYC

Who I am

- I teach data science at a local Bootcamp: Metis.
- Along with t4tech, I lead free trans-centered educational workshops.
- I write and work at the intersection of Technology, Ethics, and Gender

@defsophiaray

Objectives

By end of workshop:

- I understand what VPNs and Tor can do for security.
  - And what they **cannot** do for security.
- I know basically what VPNs and Tor are and how they differ.
- I can use a VPN to **privately** connect to the web.
- I can use Tor to **anonymously** connect to the web.
- I know the best practices for using Tor.

What Tor doesn’t do

- SESTA & FOSTA created an exception to section 230 of the 1996 Communications Decency Act.

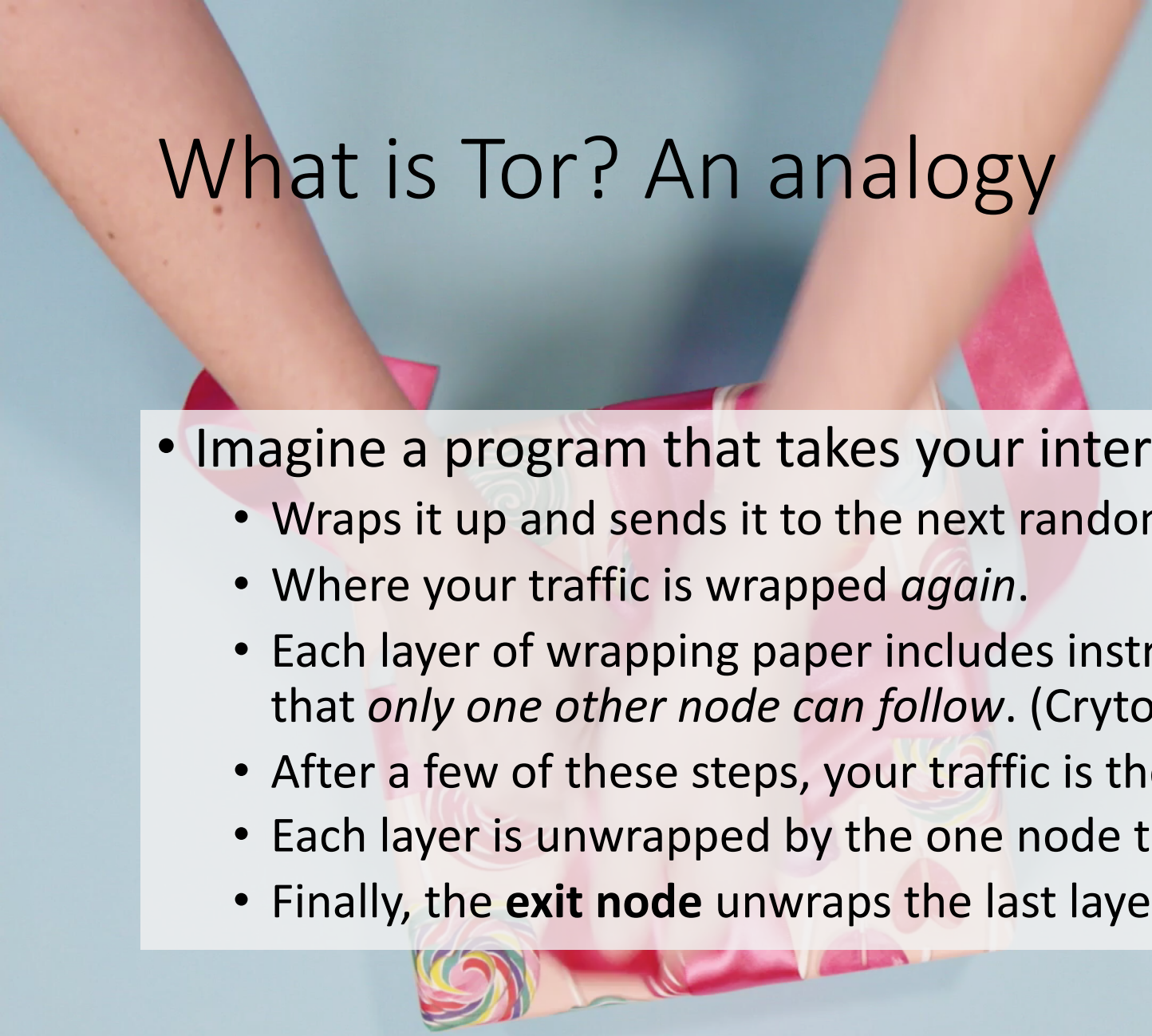
“No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider”

- Sites are held responsible if *any* user is found to be engaging in sex work.

What Tor doesn’t do

- Websites are now at risk, and are passing that risk out on their users.
- **Privacy/anonymity doesn’t solve any of this.**
- **Sites will still target sex workers, even if those accounts cannot be traced to specific persons.**
- Tor and VPNs *can* limit (but not eliminate!) your exposure to risk of being personally tracked by law enforcement, but it won’t fix many of the problems created by SESTA/FOSTA.

What is Tor? An analogy



- Imagine a program that takes your internet traffic
  - Wraps it up and sends it to the next random node in the tor network
  - Where your traffic is wrapped *again*.
  - Each layer of wrapping paper includes instructions for unwrapping that layer that *only one other node can follow*. (Crytopgraphy! Math!)
  - After a few of these steps, your traffic is then routed out of the Tor network.
  - Each layer is unwrapped by the one node that is able to.
  - Finally, the **exit node** unwraps the last layer and sends the traffic on its way.

VPNs vs Tor

- A VPN is for **privacy**
  - VPN is similar to a single layer Tor network where the node is known.
  - Must trust VPN
  - Hides activity from your ISP but does not anonymize.
- Tor is for **anonymity** (and also privacy)
  - Layers of random relays obfuscate source of traffic.
  - Does not require trust.

Discuss: Vulnerable Data

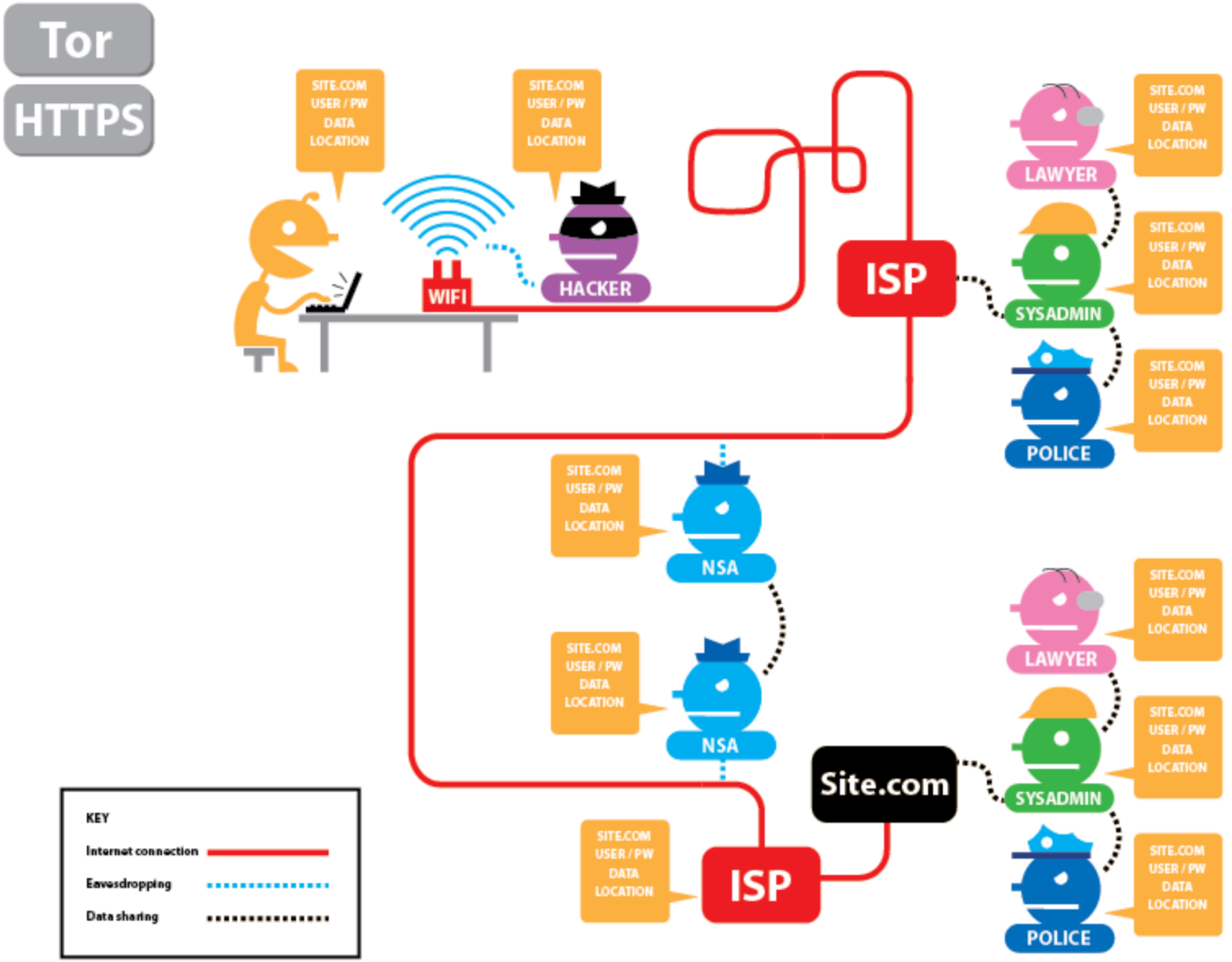
- Site.com: which website you're visiting
- User/PW: your confidential usernames and passwords
- Data: All other transferred data. Images, text, anything.
- Location: Your IP address. Points to the specific network (wifi router) you are using.

Threats

Vulnerable data

- Site.com: which website you're visiting
- User/PW: your confidential usernames and passwords
- Data: All other transferred data. Images, text, anything.
- Location: Your IP address. Points to the specific network (wifi router) you are using.

Images from EFF
https://www.eff.org/pages/tor-and-https



Local Threats

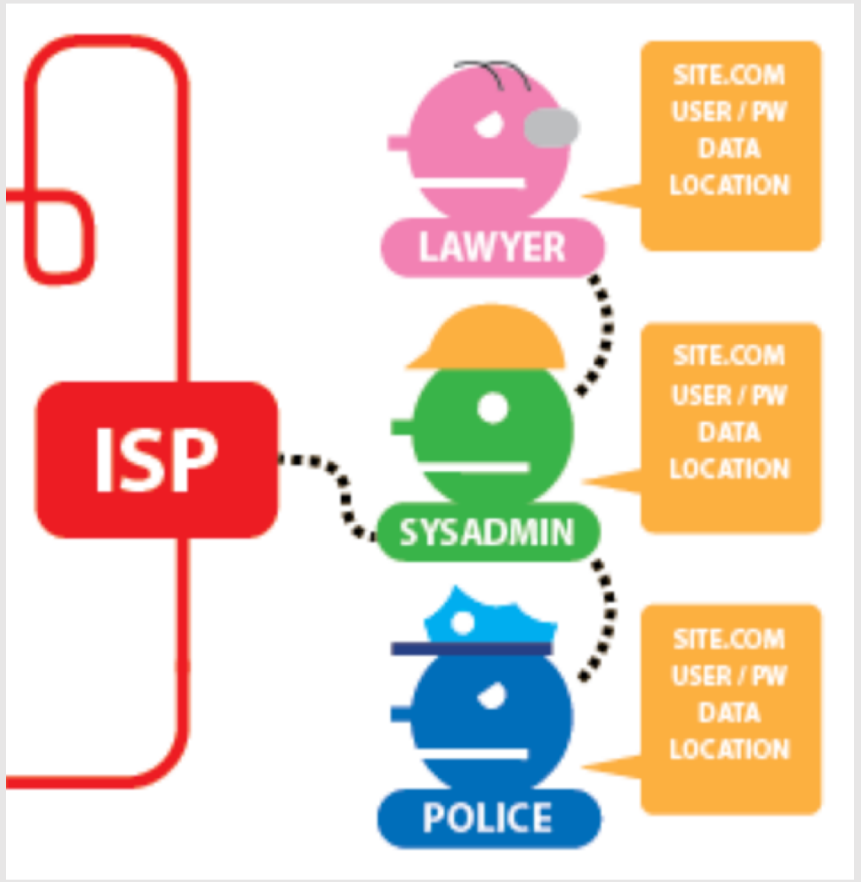
Local threats have access to the network we are currently using.

Right now, we are all potential local threats to each other!

Our Internet Service Provider

Your ISP is the company you pay for internet access.

Your ISP sees **all** traffic you send over the internet.



External sites

Any external site you access has its own ISP as well.

The external site necessarily sees any data you send its way.

Many of these sites generate revenue by storing and selling your data.

Post SESTA/FOSTA, these sites also track your data to manage their legal exposure.

External sites: horror stories

DENMARK | By Joseph Cox | May 12 2016, 1:44pm

70,000 OkCupid Users Just Had Their Data Published

Just because data is sort-of public, doesn't mean that it's ethical to collect en masse.

Grindr Sets Off Privacy Firestorm After Sharing Users' H.I.V.-Status Data

By Natasha Singer

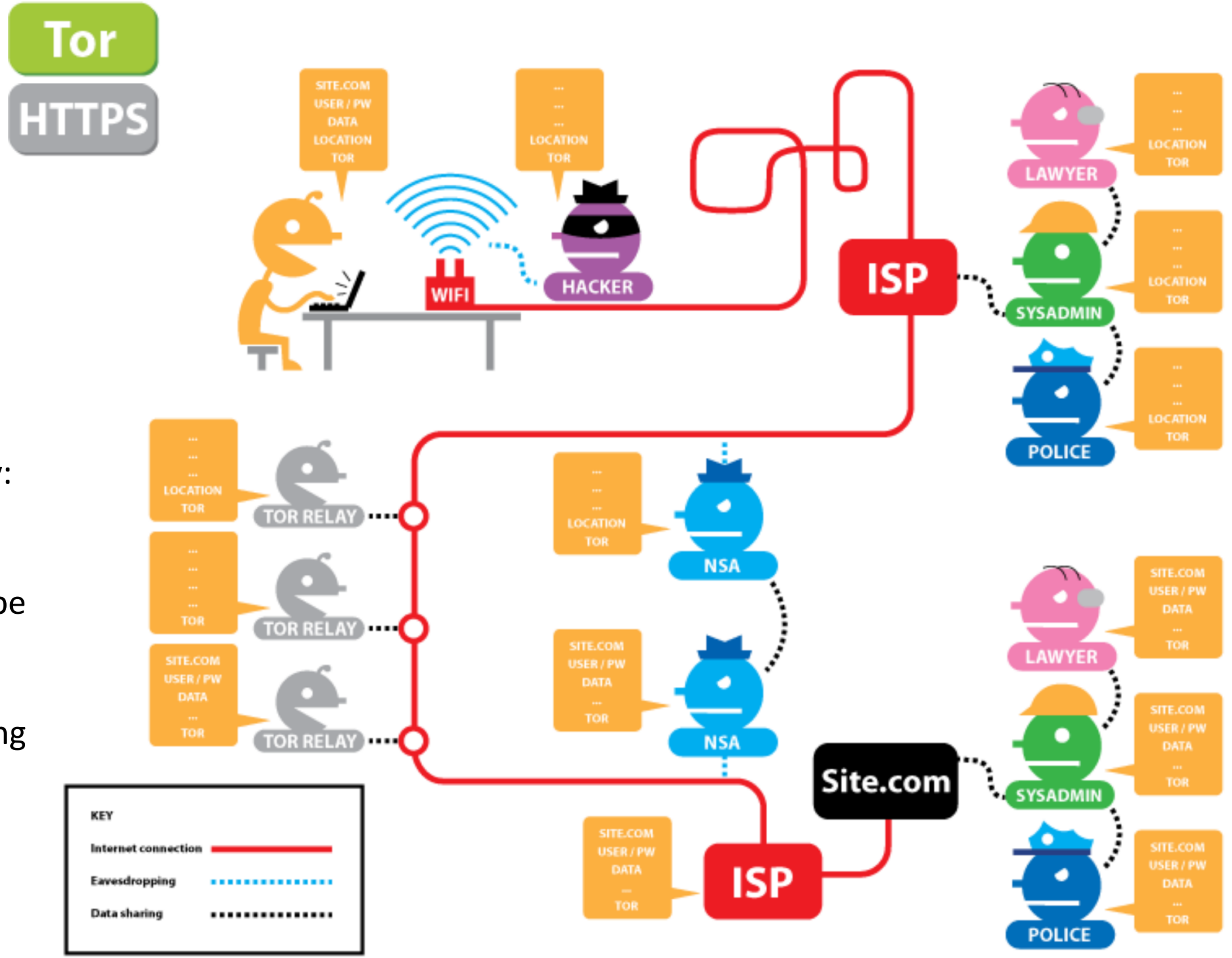
April 3, 2018

What does Tor Do?

Obscures “location” (IP address) and data.

Limitations:

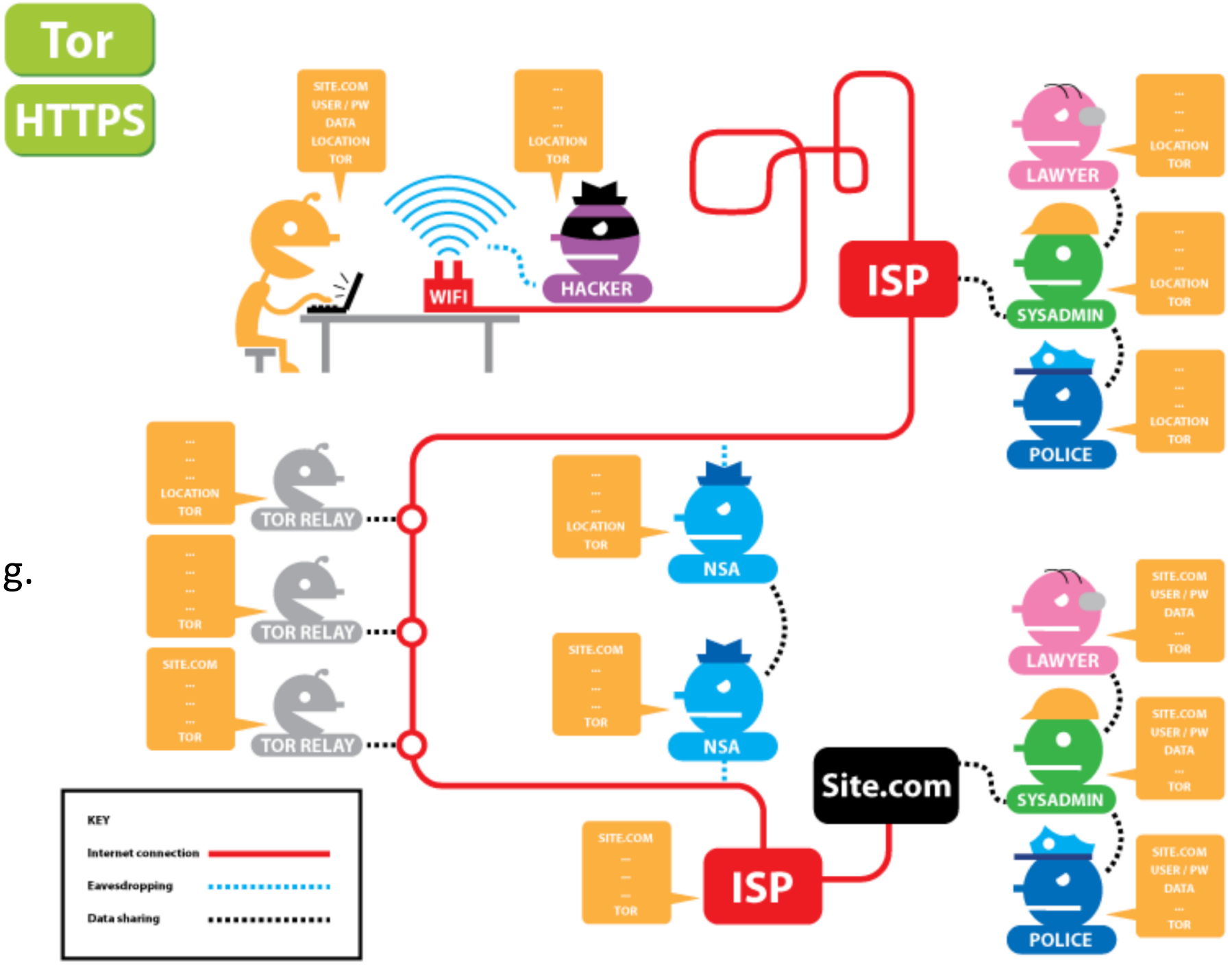
- IP address can still be seen by: local threats, our ISP, and the entry node.
- Data and passwords can still be seen by: exit node, external sites, and their ISP
- Everyone will know we’re using Tor.



What does Tor + HTTPS do?

Our Data and passwords are now hidden from all but the external site we are accessing.

Entry node still sees our IP address.



Words of Caution

- Tor’s main vulnerabilities are the entry and exit nodes.
  - Entry nodes see your IP address (but see VPNs later)
  - Exit nodes see your traffic (so use encryption!)
- By default, Tor only works through the browser.
  - Not on mobile.
- If used correctly, Tor offers some protection for your identity. It **does not** affect how external sites regulate or use your data and activity.

Words of Caution

KIM ZETTER SECURITY 09.10.07 02:00 AM

ROGUE NODES TURN TOR ANONYMIZER INTO EAVESDROPPER'S PARADISE

NEWS

Rogue Tor 'exit node' server added malware to legitimate downloads

By Jeremy Kirk

Australia Correspondent, IDG News Service | OCT 27, 2014 5:55 AM PT

POLICY —

Judge confirms what many suspected: Feds hired CMU to break Tor

A 1992 case about paper shredders may also shed some light on Tor privacy question.

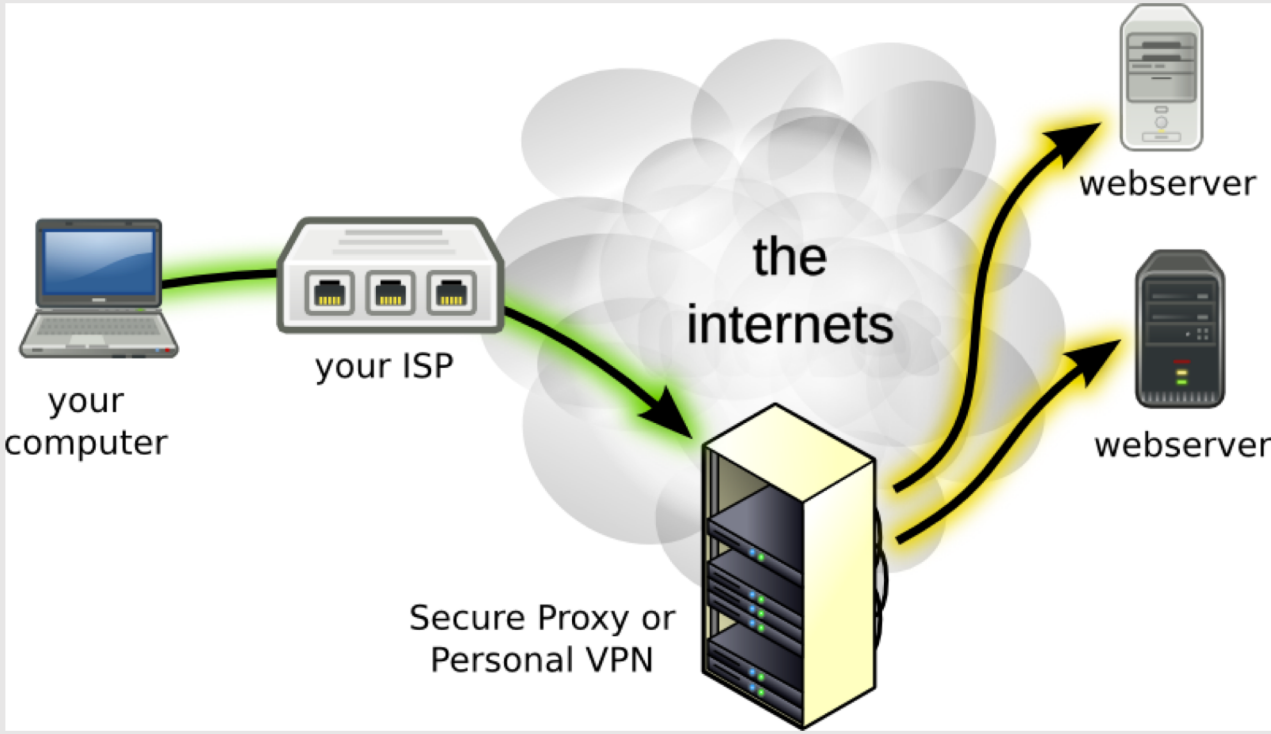
CYRUS FARIVAR - 2/24/2016, 2:24 PM

Good Tor Hygiene

- Use HTTPS everywhere
- Don’t torrent on Tor!
  - Torrent protocols send your IP address along with the packets, so it’s not anonymous by design.

What is a VPN?

- Similar to Tor but with a single, known relay.
- Your traffic is encrypted, sent through your ISP to the VPN, which then decrypts it and passes it onto the larger web.
- Hides your IP address from all but your ISP and local network.
- Relies on trust in VPN.



How to Choose a VPN

- Don’t trust free VPNs: your traffic is their revenue source.
- It’s a personal choice. Your security is only as good as your VPN is trustworthy. Do your own research.
  - TorrentFreak
  - That one privacy site
  - The Wirecutter
- Good defaults
  - ExpressVPN
  - IVPN

	Tor only	VPN only	Tor+VPN
Location Visible to	Local threats, ISP, Entry node	Local threats, ISP, VPN host	Local threats, ISP, VPN host
Non-HTTPS Data Visible to	Exit Node, Site ISP, Site	VPN host, Site ISP, Site	VPN host, Site ISP, Site
HTTPS Data Visible to	Site	Site	Site
Knows you're using Tor	Everyone	-	No one
Speed	Slow. Text and images.	Medium-Fast. Streaming.	Slowest. Text and images.

Security on Mobile

- Tor does not protect mobile apps by default
- VPN only
- Tor Router
  - Creates a secure network whose traffic is routed through Tor.

Tor Router: How to use Tor + VPN on mobile apps

- A Tor Router routes *all* network traffic through the Tor network (and possibly a VPN)
- Easy option: Purchase an Tor+VPN enabled router: anonbox
- Hard option: See further reading

What to use? Recommendations

- Always On
  - HTTPS everywhere: extension that forces all websites to use HTTPS
  - VPN. Configure once on all devices and then forget about it.
- In browser, mostly text.
  - Tor or Tor+VPN
- Mobile app
  - VPN or Tor router
- Streaming
  - VPN only

Breakout: Set up Tor Browser

- How to use Tor for Mac
- How to use Tor for Linux
- How to use Tor for Windows

Further Reading

- Common Tor Myths
- How to set up a .onion website
- Build your own Tor router using an existing router or a raspberry pi