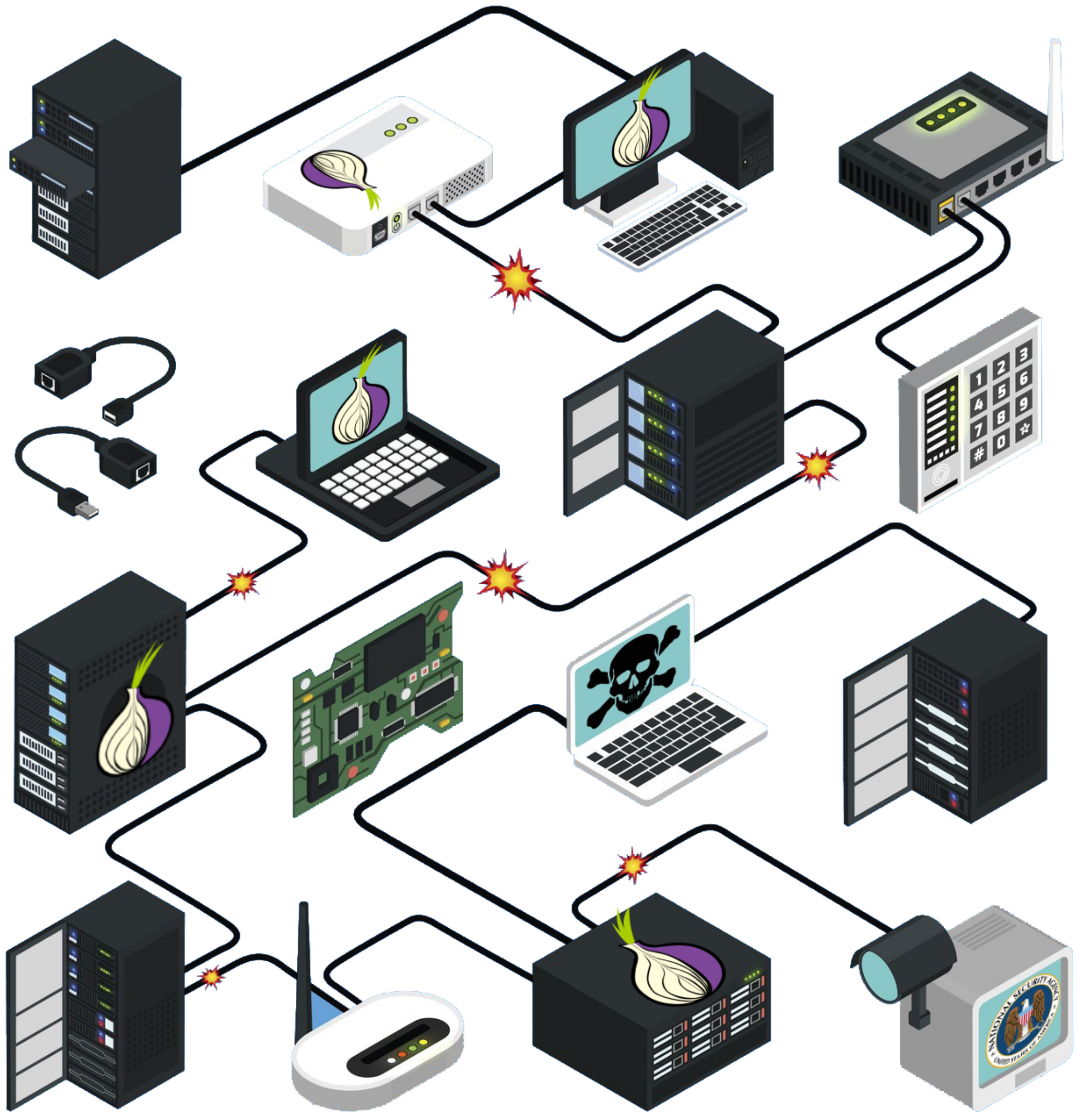
Technical introduction

The Tor Network



Sharing is Caring

Please copy, share, and remix!

grab a copy of the presentation:

github.com/francisco-core/tecnical-intro-to-tor/

On the Internet, nobody knows you're a dog.

*"Remember when, on the Internet,
nobody knew who you were?"*

Why is there a need for privacy?

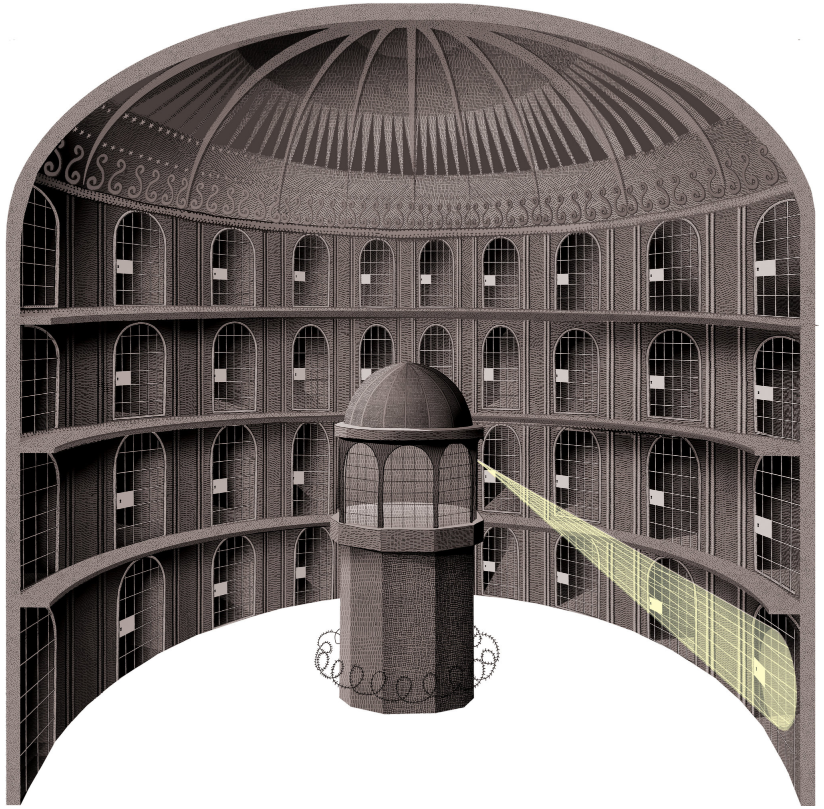
Privacy

gives people a safe place

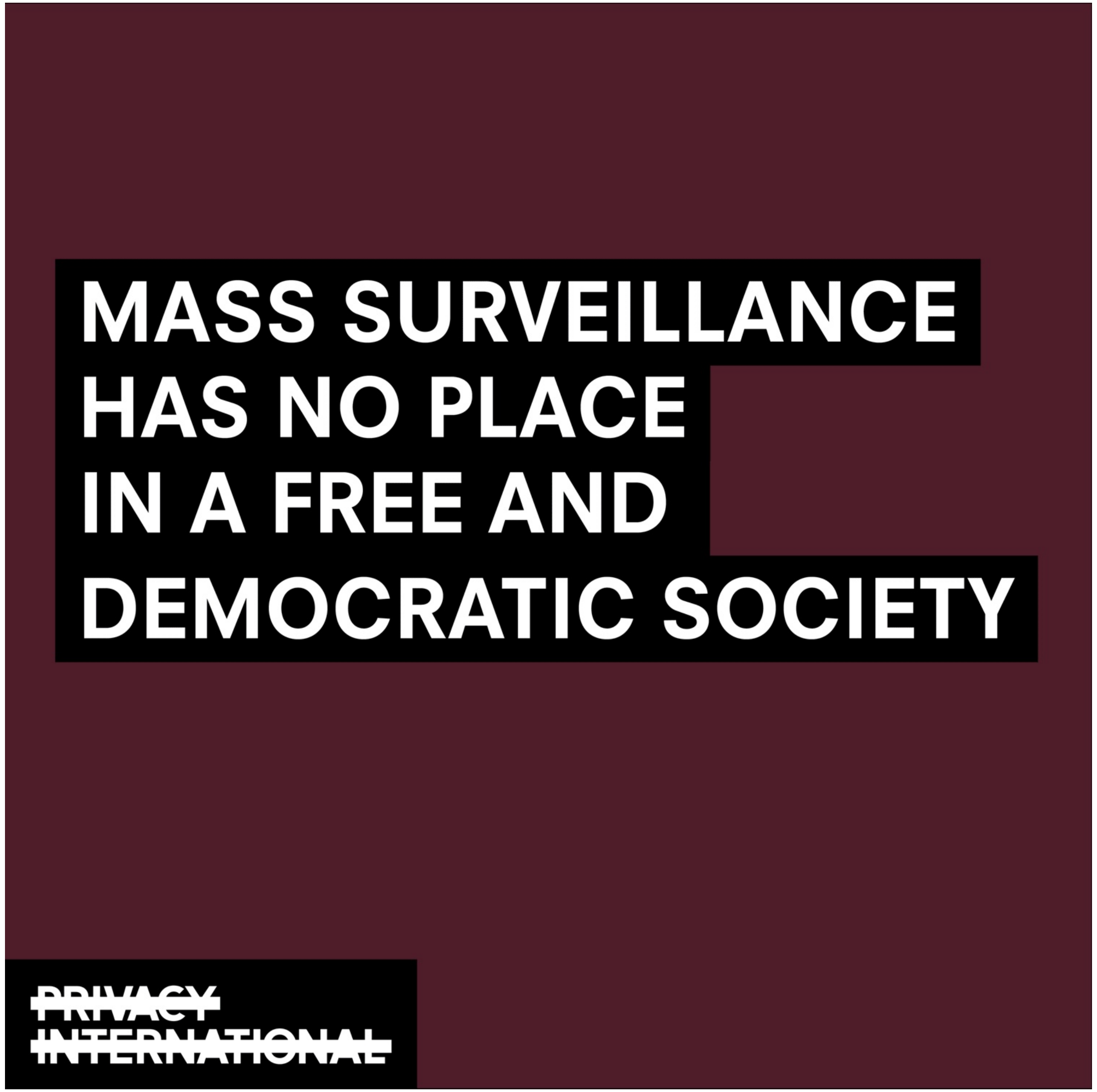
If everything is recorded, you never know what is going to be used against you

You self-censor

> Observation changes behavior



Privacy is essential for a Free Society



MASS SURVEILLANCE HAS NO PLACE IN A FREE AND DEMOCRATIC SOCIETY

PRIVACY INTERNATIONAL

But...

The Internet is NOT a private place

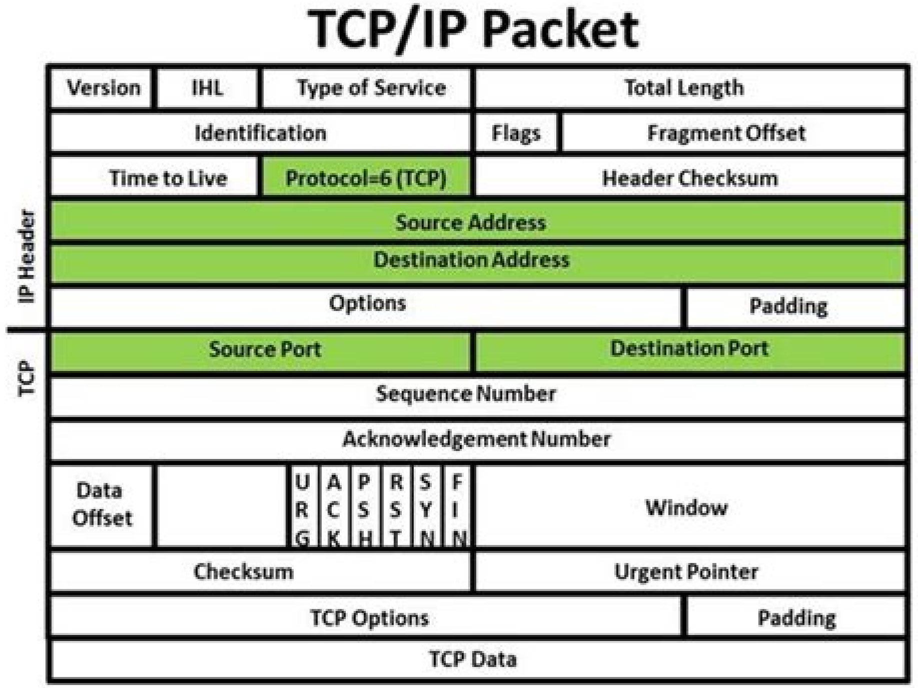
With no additional protection

we are exposed

IP addresses are geolocated

and sent allong with each message

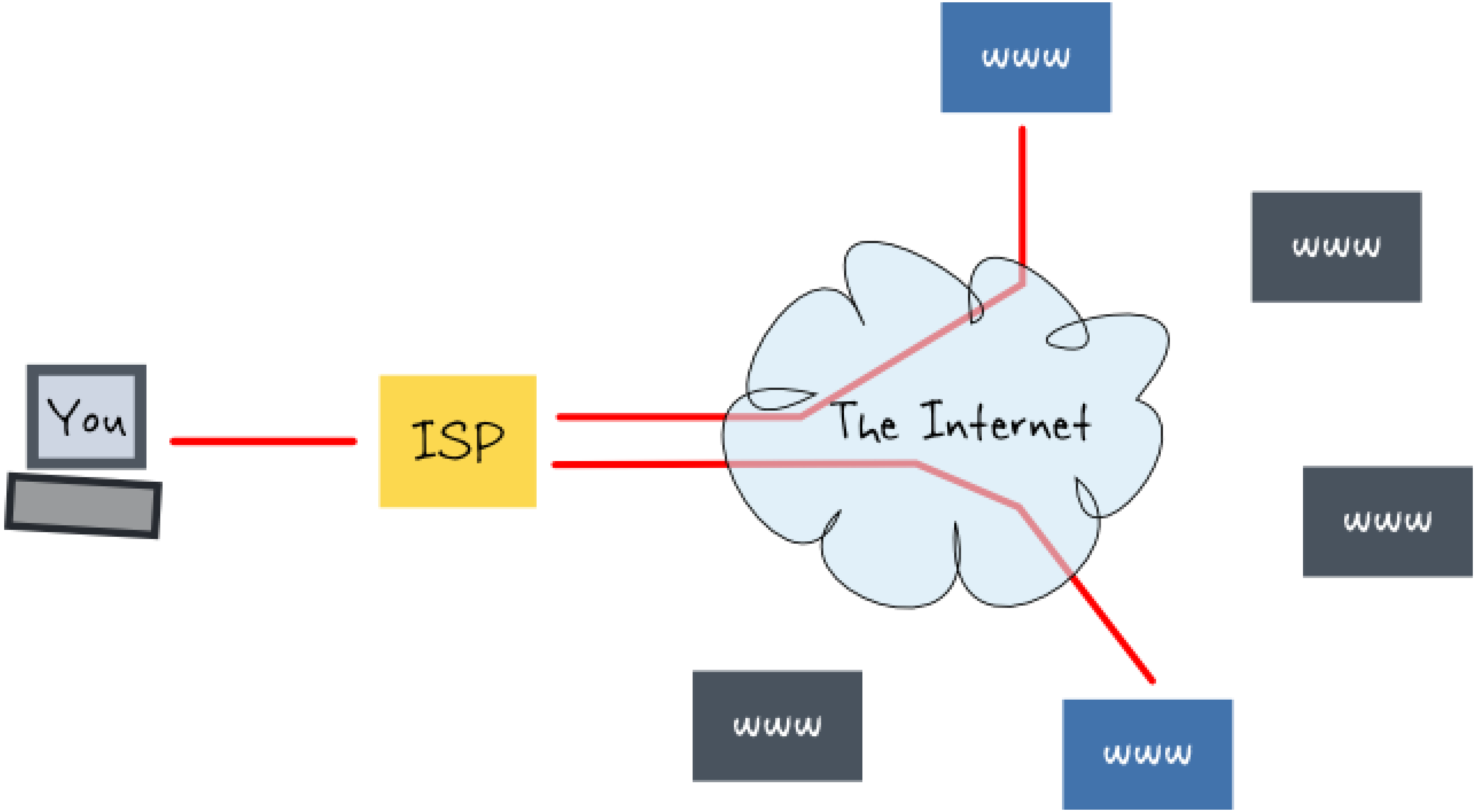
The Broad
Grand Park LA
Los Angeles
110
101
Pershing Square
S Main St
E 1st St
E 3rd St
E 4th St
E 5th St
E 1st St
E 4th St
S Los Angeles St
S Olive St
DOWNTOWN
You Are Here.
And They Know it.



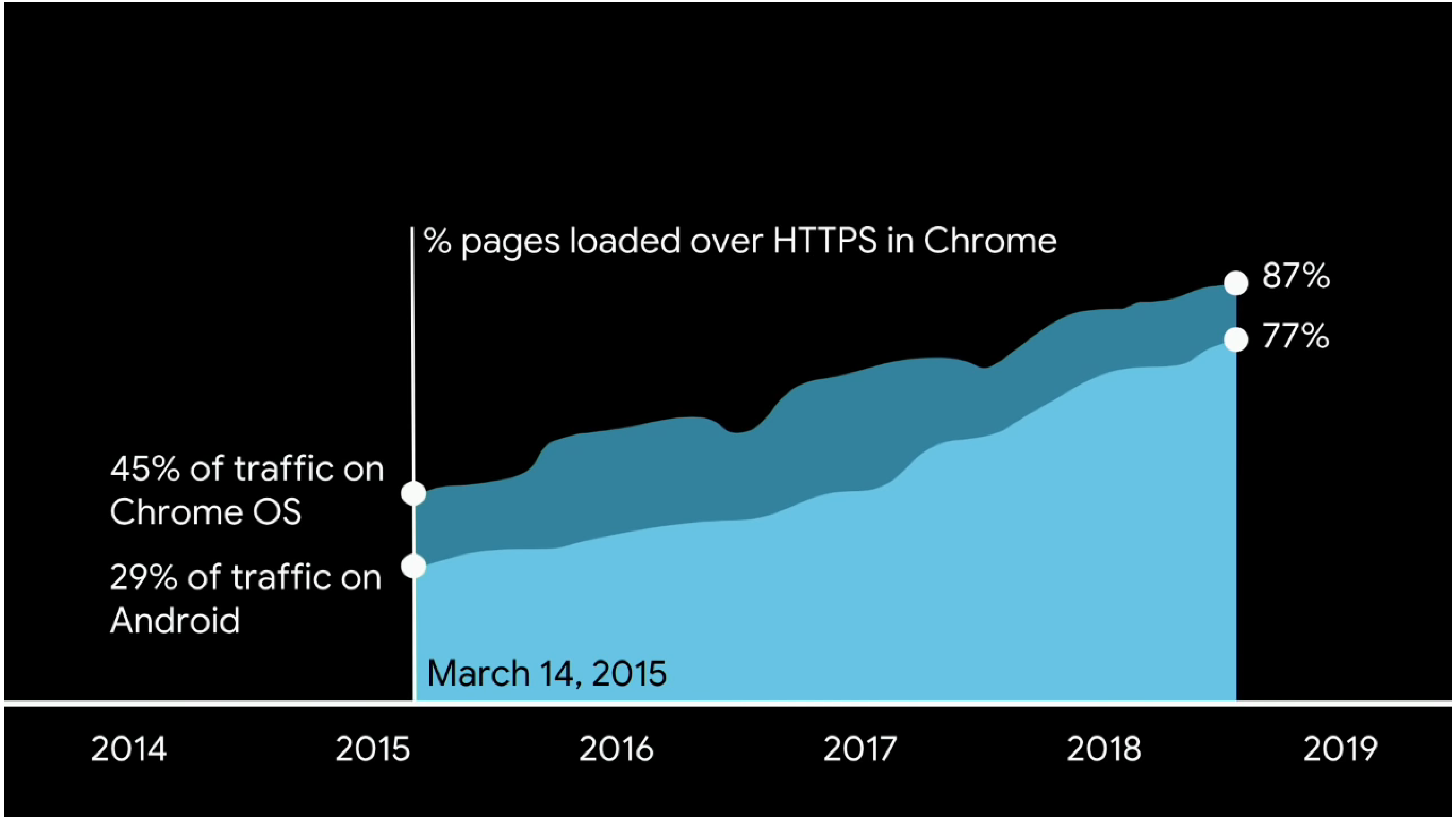
TCP/IP Packet

IP Header	Version	IHL	Type of Service						Total Length
	Identification							Flags	Fragment Offset
	Time to Live		Protocol=6 (TCP)						Header Checksum
	Source Address								
	Destination Address								
	Options								Padding
TCP	Source Port								Destination Port
	Sequence Number								
	Acknowledgement Number								
	Data Offset		U R G	A C K	P S H	R S T	S Y N	F I N	Window
	Checksum								Urgent Pointer
	TCP Options								Padding
	TCP Data								

ISPs know every website you visit / services you use

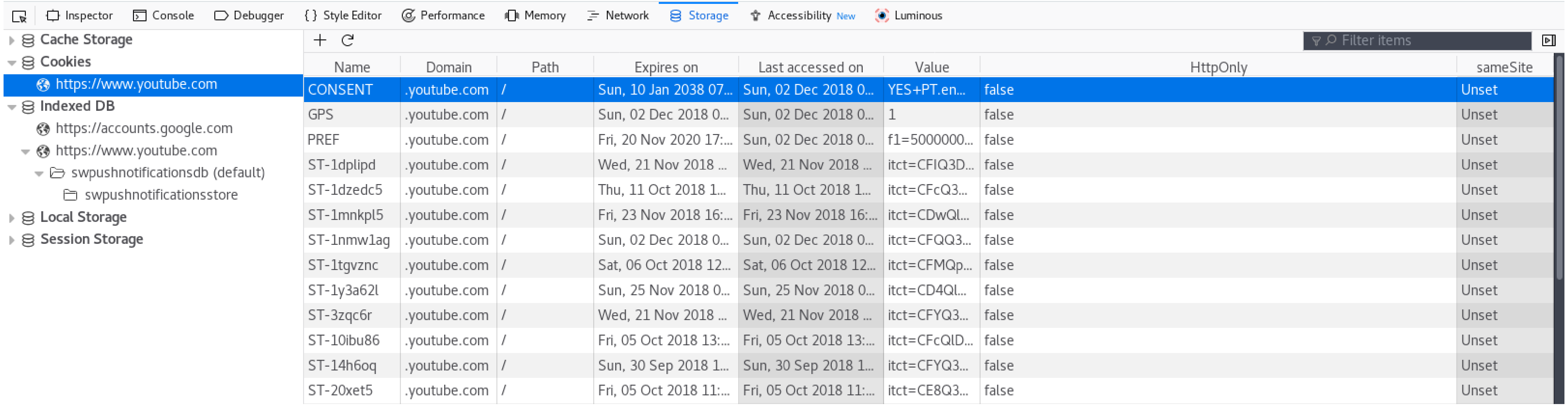


HTTPS wide deployment is very recent



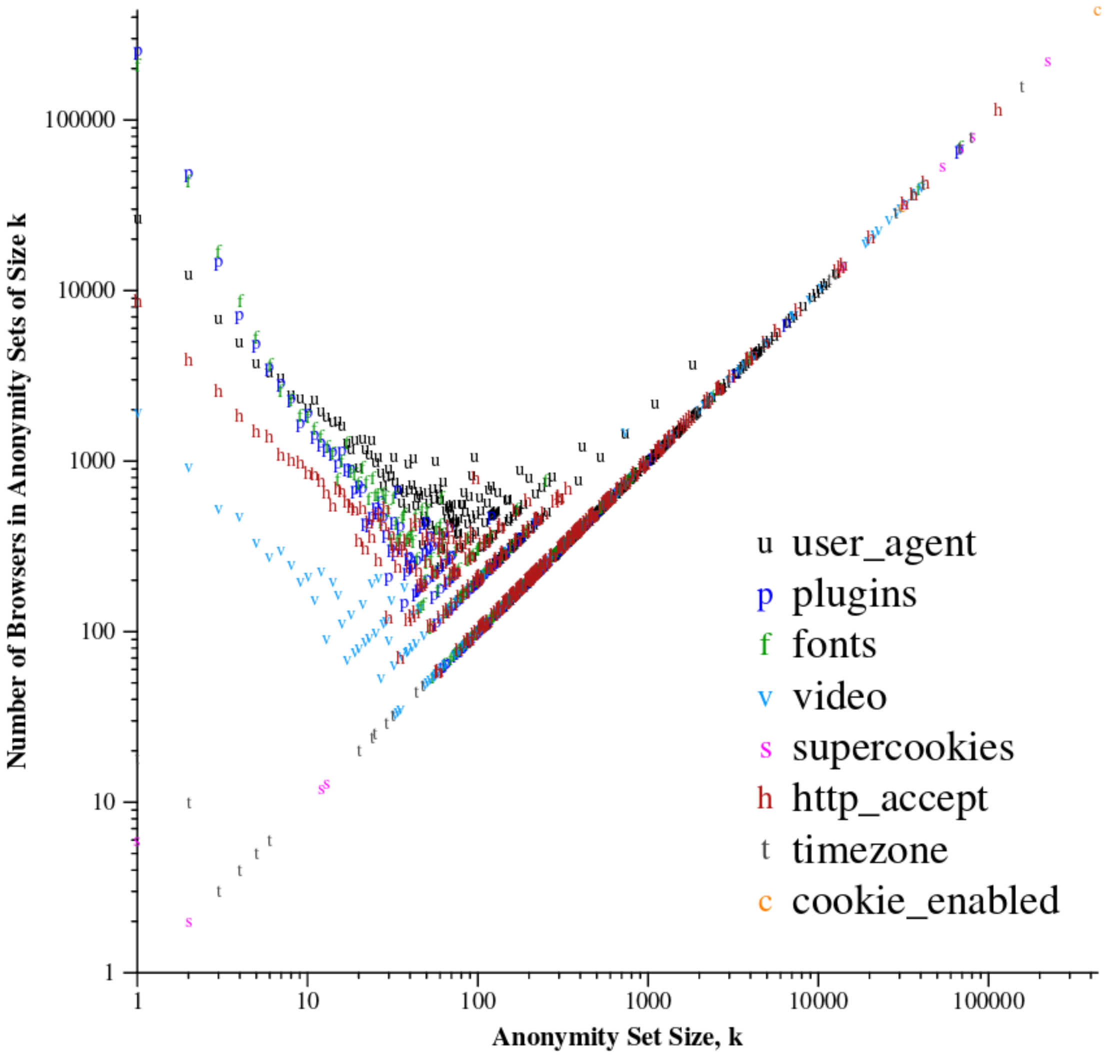
Cookies

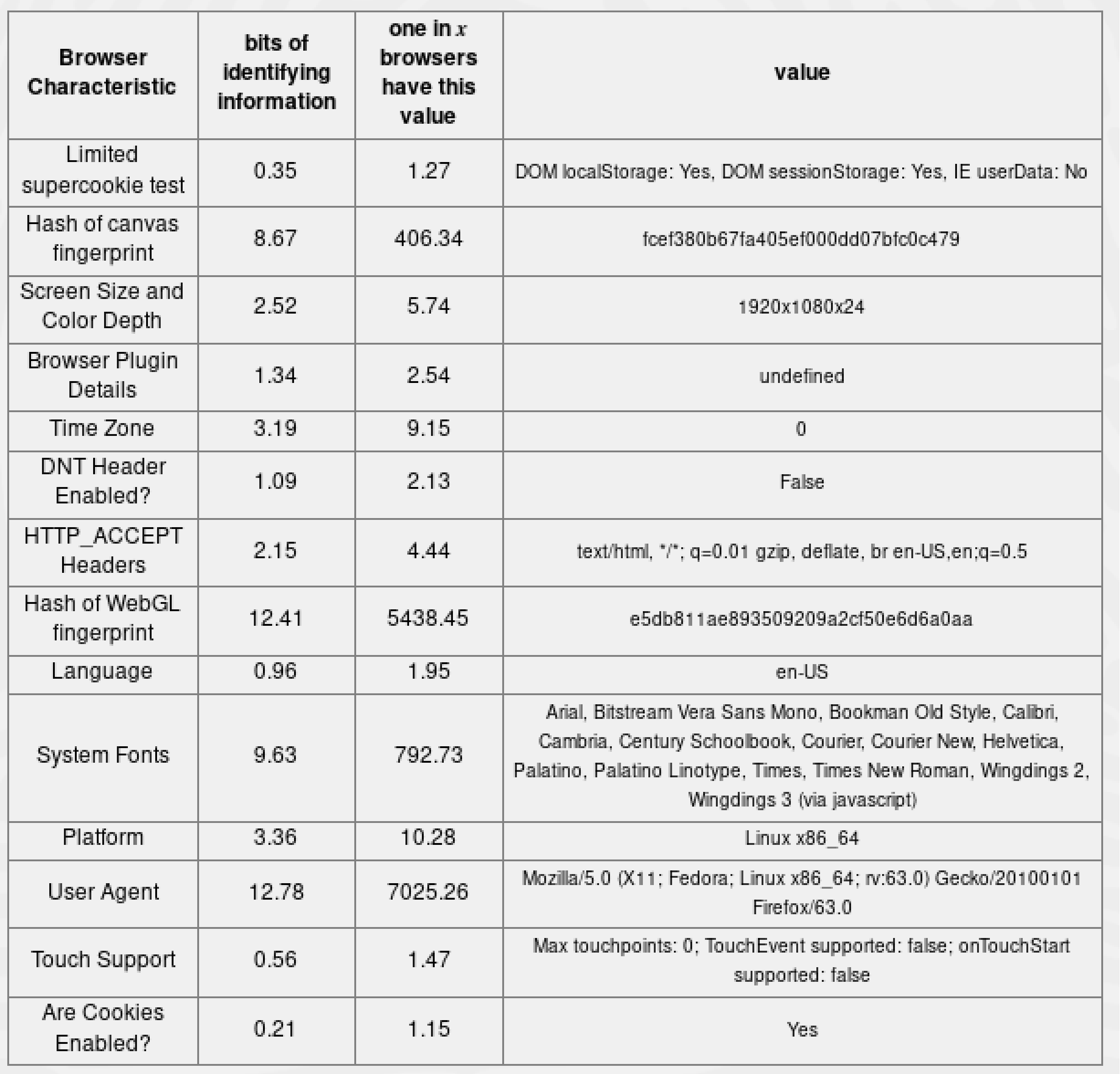
Cookies have been preverted from their original function and abused to **track people** online for marketing purposes.



Name	Domain	Path	Expires on	Last accessed on	Value	HttpOnly	sameSite
CONSENT	.youtube.com	/	Sun, 10 Jan 2038 07...	Sun, 02 Dec 2018 0...	YES+PT.en...	false	Unset
GPS	.youtube.com	/	Sun, 02 Dec 2018 0...	Sun, 02 Dec 2018 0...	1	false	Unset
PREF	.youtube.com	/	Fri, 20 Nov 2020 17:...	Sun, 02 Dec 2018 0...	f1=5000000...	false	Unset
ST-1dplipd	.youtube.com	/	Wed, 21 Nov 2018 ...	Wed, 21 Nov 2018 ...	itct=CFIQ3D...	false	Unset
ST-1dzedc5	.youtube.com	/	Thu, 11 Oct 2018 1...	Thu, 11 Oct 2018 1...	itct=CFcQ3...	false	Unset
ST-1mnkpl5	.youtube.com	/	Fri, 23 Nov 2018 16:...	Fri, 23 Nov 2018 16:...	itct=CDwQl...	false	Unset
ST-1nmw1ag	.youtube.com	/	Sun, 02 Dec 2018 0...	Sun, 02 Dec 2018 0...	itct=CFQQ3...	false	Unset
ST-1tgvznc	.youtube.com	/	Sat, 06 Oct 2018 12...	Sat, 06 Oct 2018 12...	itct=CFMQp...	false	Unset
ST-1y3a62l	.youtube.com	/	Sun, 25 Nov 2018 0...	Sun, 25 Nov 2018 0...	itct=CD4Ql...	false	Unset
ST-3zqc6r	.youtube.com	/	Wed, 21 Nov 2018 ...	Wed, 21 Nov 2018 ...	itct=CFYQ3...	false	Unset
ST-10ibu86	.youtube.com	/	Fri, 05 Oct 2018 13:...	Fri, 05 Oct 2018 13:...	itct=CFcQlD...	false	Unset
ST-14h6oq	.youtube.com	/	Sun, 30 Sep 2018 1...	Sun, 30 Sep 2018 1...	itct=CFYQ3...	false	Unset
ST-20xet5	.youtube.com	/	Fri, 05 Oct 2018 11:...	Fri, 05 Oct 2018 11:...	itct=CE8Q3...	false	Unset

Browser Fingerprinting

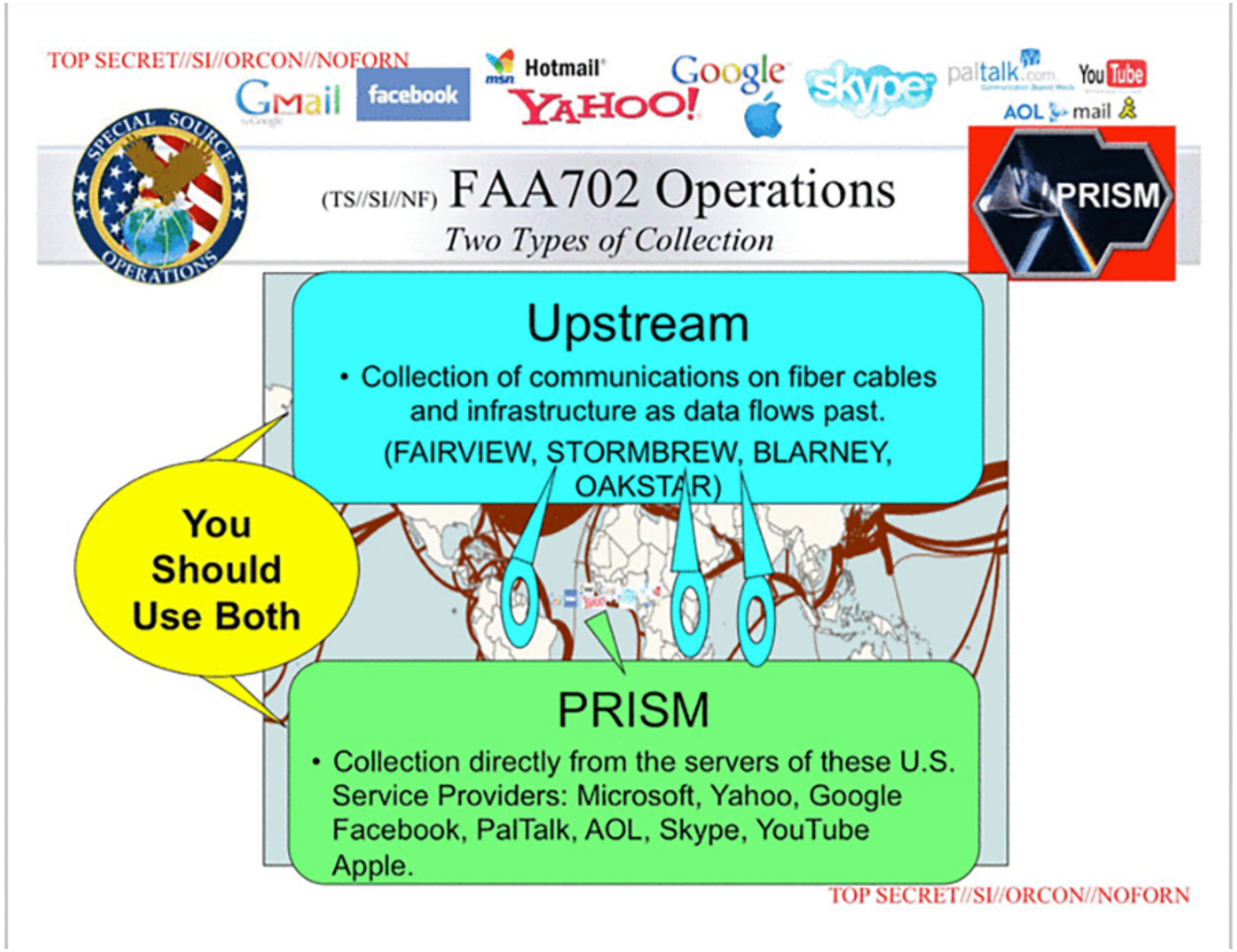




Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.35	1.27	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	8.67	406.34	fcef380b67fa405ef000dd07bfc0c479
Screen Size and Color Depth	2.52	5.74	1920x1080x24
Browser Plugin Details	1.34	2.54	undefined
Time Zone	3.19	9.15	0
DNT Header Enabled?	1.09	2.13	False
HTTP_ACCEPT Headers	2.15	4.44	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.5
Hash of WebGL fingerprint	12.41	5438.45	e5db811ae893509209a2cf50e6d6a0aa
Language	0.96	1.95	en-US
System Fonts	9.63	792.73	Arial, Bitstream Vera Sans Mono, Bookman Old Style, Calibri, Cambria, Century Schoolbook, Courier, Courier New, Helvetica, Palatino, Palatino Linotype, Times, Times New Roman, Wingdings 2, Wingdings 3 (via javascript)
Platform	3.36	10.28	Linux x86_64
User Agent	12.78	7025.26	Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:63.0) Gecko/20100101 Firefox/63.0
Touch Support	0.56	1.47	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.21	1.15	Yes

from a *"How Unique Is Your Web Browser?"* by Peter Eckersley

Passive Analysis of the Internet Backbone



Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
PRISM
SPECIAL SOURCE OPERATIONS

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

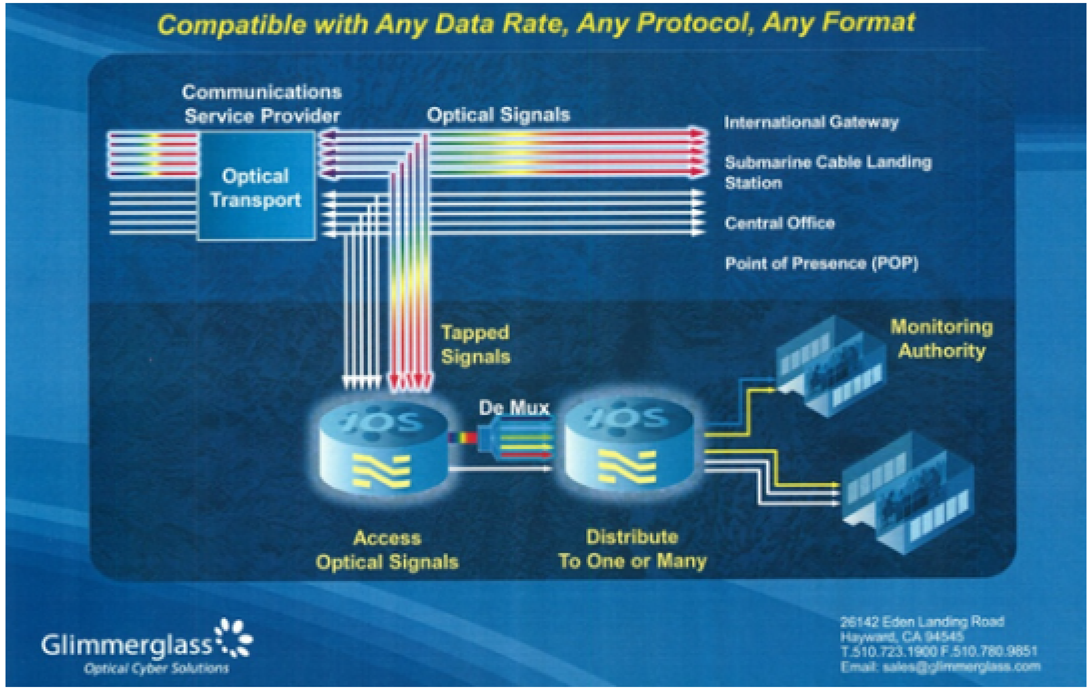
- Collection of communications on fiber cables and infrastructure as data flows past. (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

TOP SECRET//SI//ORCON//NOFORN



Surveillance Capitalism

> The business model where **data is money**

driving force
of surveillance

So, what do we do about it?

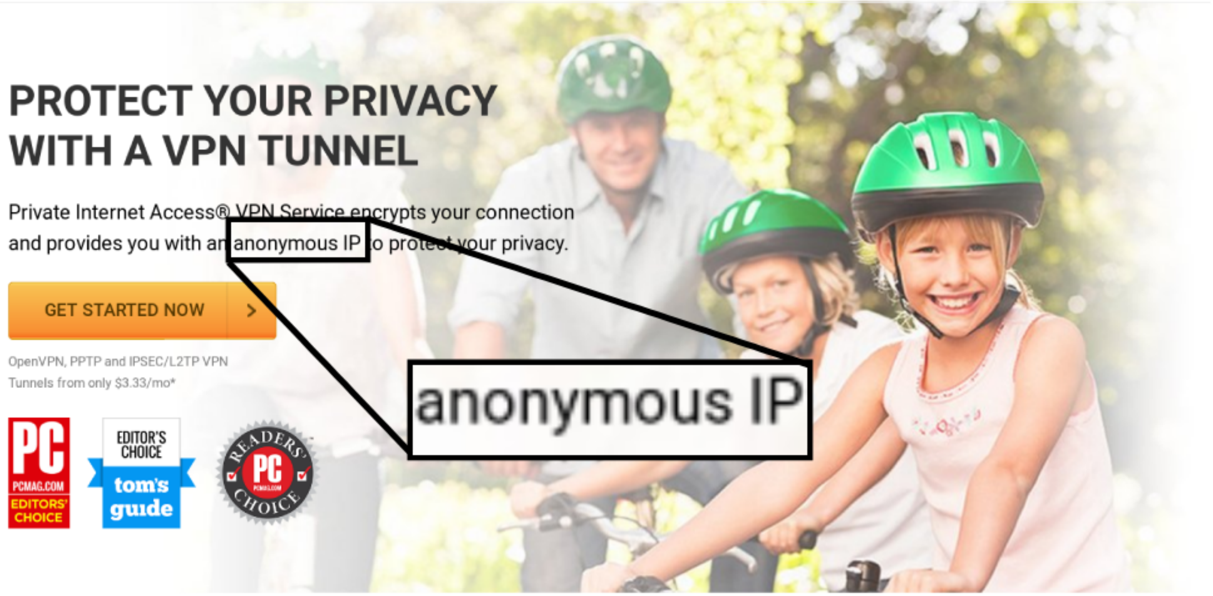
> **We create an anonymity network on top of a non-anonymous one**

yeah, Computer Science has wonders like these

Approaches to Privacy and Anonymity

There are various approaches to anonymity online, with different trade-offs.

Single Proxy / VPN



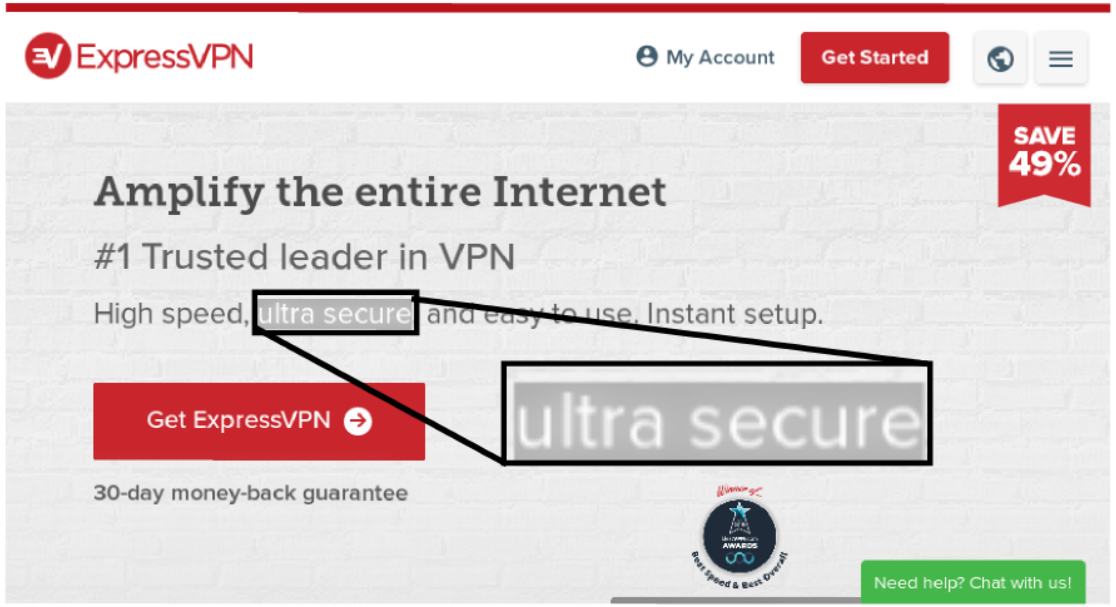
PROTECT YOUR PRIVACY WITH A VPN TUNNEL

Private Internet Access® VPN Service encrypts your connection and provides you with an anonymous IP to protect your privacy.

GET STARTED NOW >

OpenVPN, PPTP and IPSEC/L2TP VPN Tunnels from only $3.33/mo*

anonymous IP



ExpressVPN

My Account

Get Started

SAVE 49%

Amplify the entire Internet

#1 Trusted leader in VPN

High speed, ultra secure and easy to use. Instant setup.

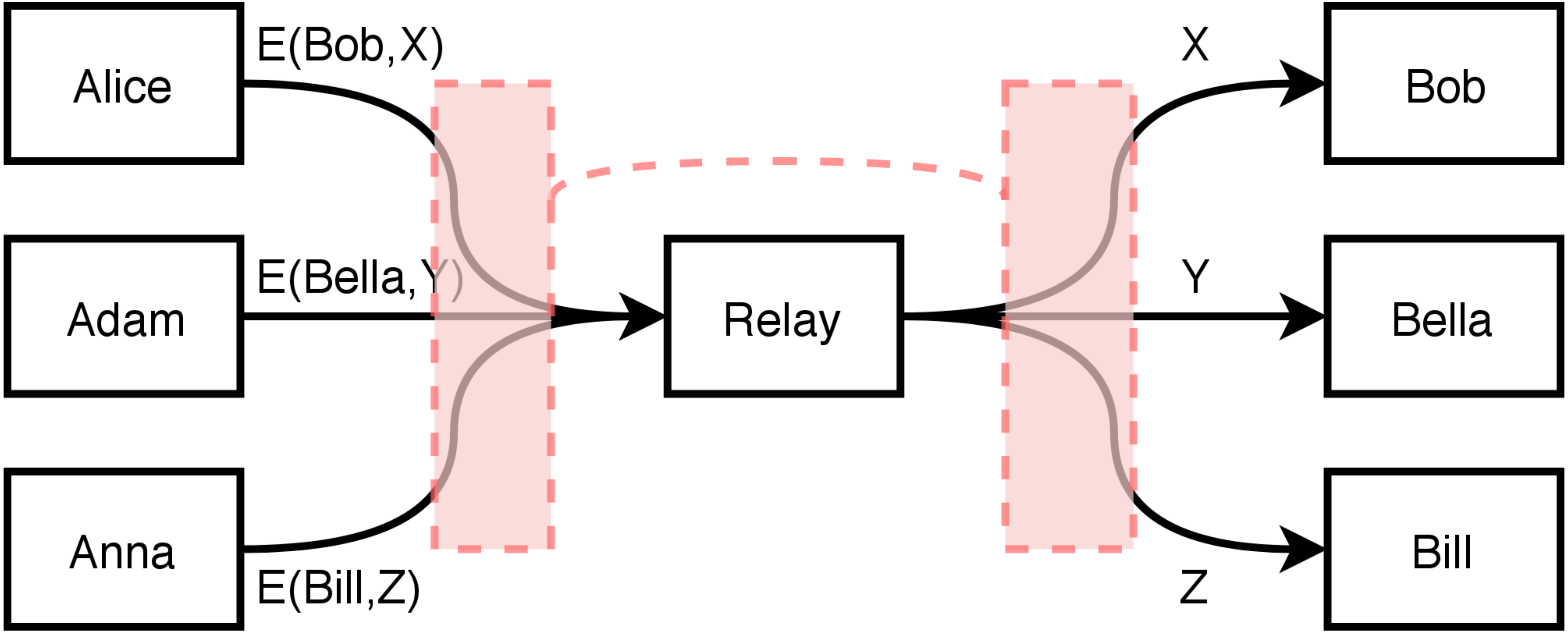
Get ExpressVPN

30-day money-back guarantee

ultra secure

Need help? Chat with us!

Single Proxy / VPN

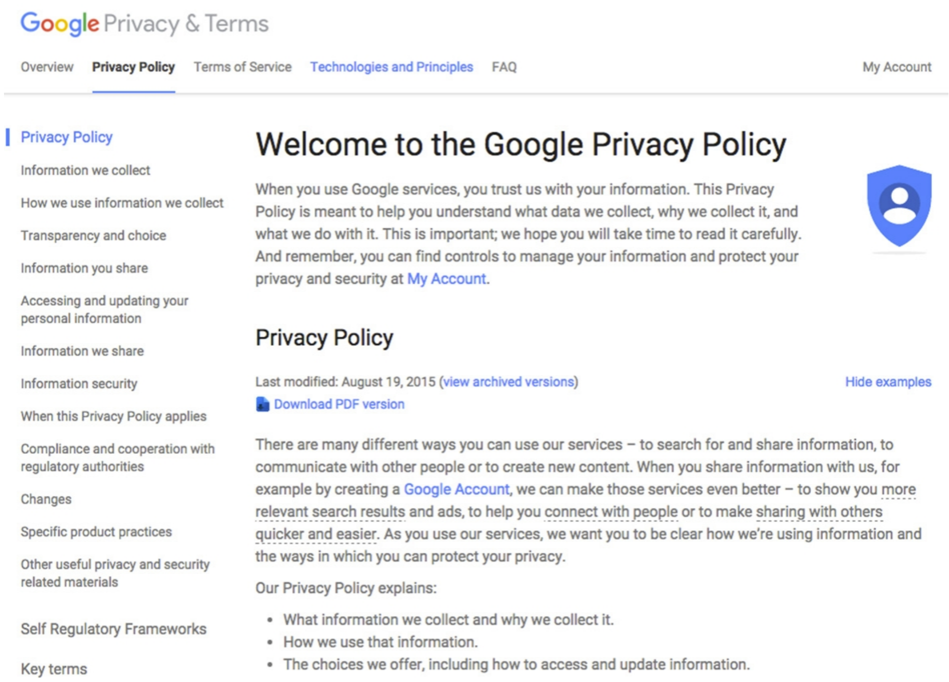


Major Flaws

1. **Trust**
2. **Liability for the Provider**
3. **Traffic Correlation**

1. We have to Trust

privacy **by Policy**



Google Privacy & Terms

Overview | **Privacy Policy** | Terms of Service | Technologies and Principles | FAQ | My Account

- Privacy Policy
- Information we collect
- How we use information we collect
- Transparency and choice
- Information you share
- Accessing and updating your personal information
- Information we share
- Information security
- When this Privacy Policy applies
- Compliance and cooperation with regulatory authorities
- Changes
- Specific product practices
- Other useful privacy and security related materials
- Self Regulatory Frameworks
- Key terms

Welcome to the Google Privacy Policy

When you use Google services, you trust us with your information. This Privacy Policy is meant to help you understand what data we collect, why we collect it, and what we do with it. This is important; we hope you will take time to read it carefully. And remember, you can find controls to manage your information and protect your privacy and security at My Account.

Privacy Policy

Last modified: August 19, 2015 (view archived versions) Hide examples

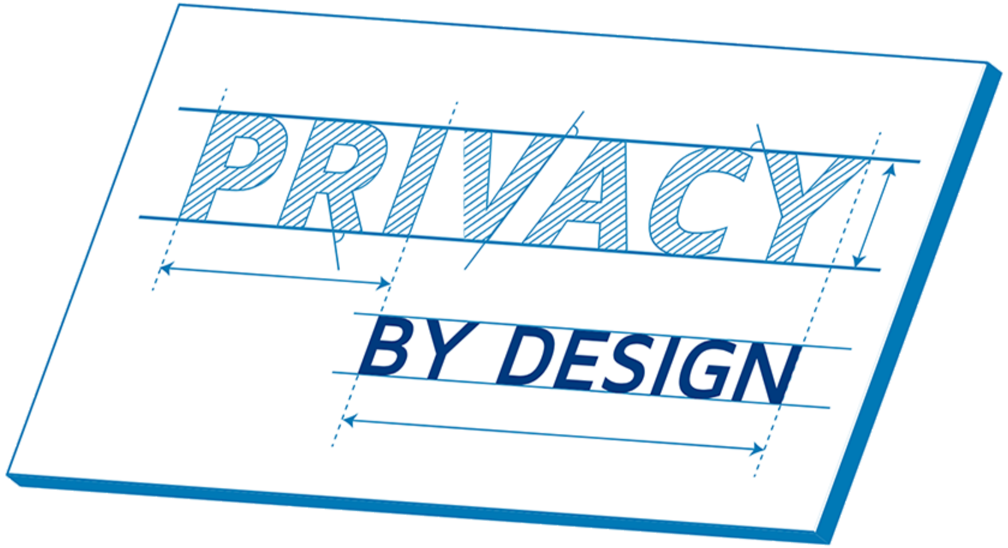
Download PDF version

There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.

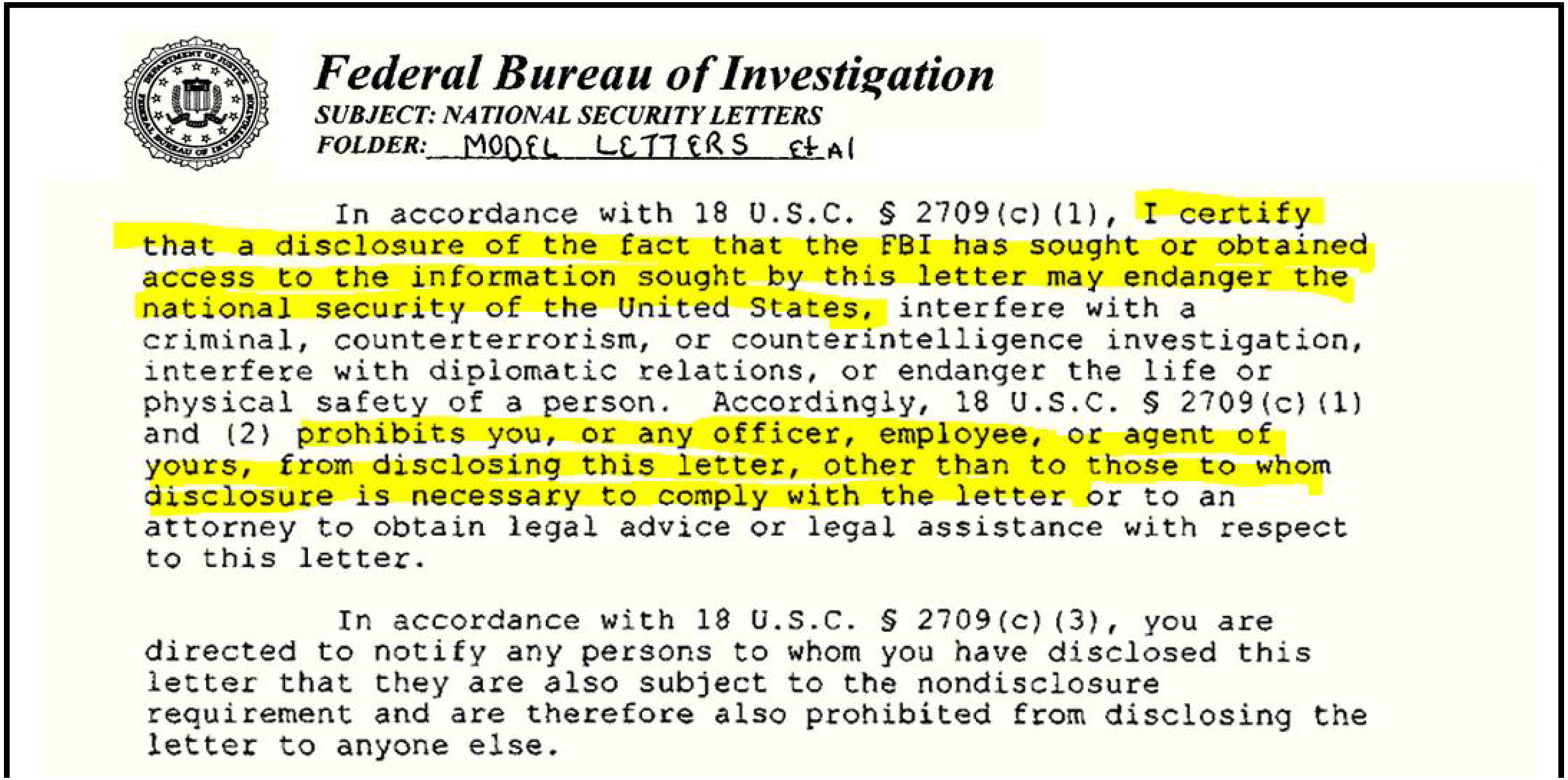
Our Privacy Policy explains:

- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

privacy **by Design**



2. Liability for the Provider



Federal Bureau of Investigation

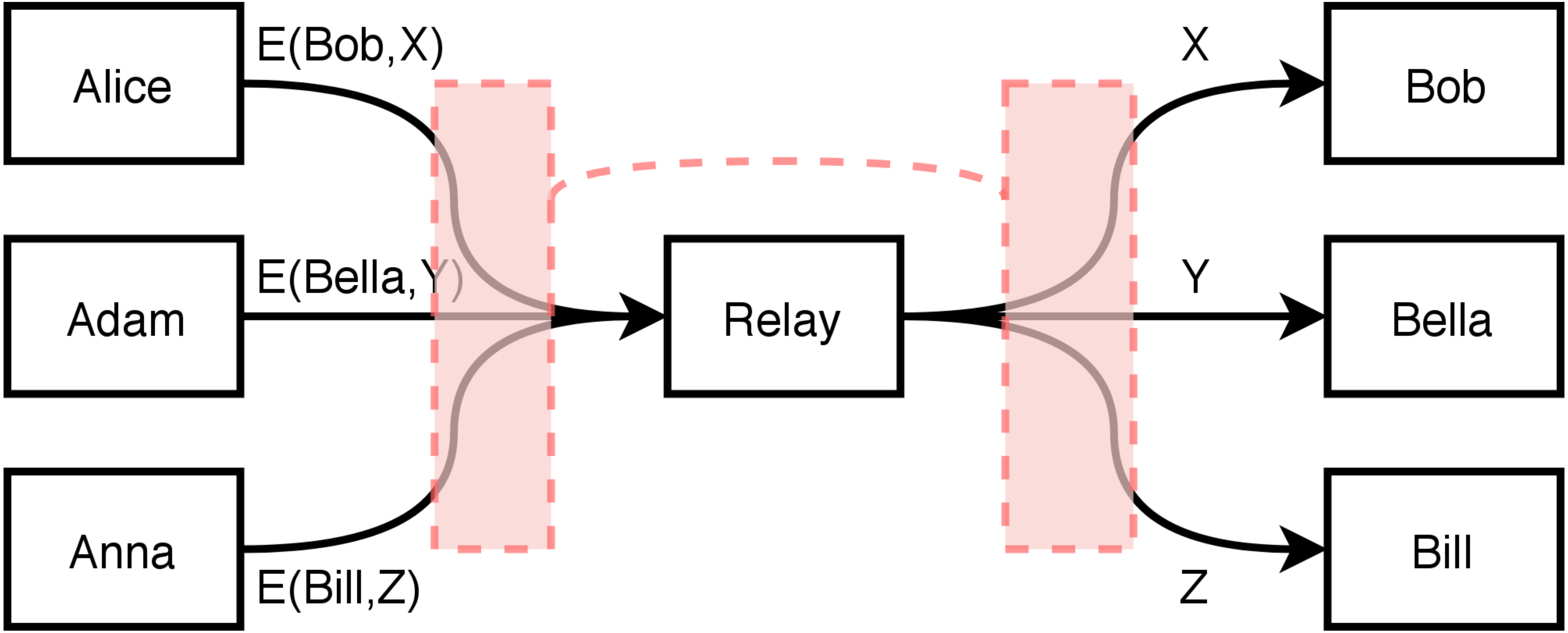
SUBJECT: NATIONAL SECURITY LETTERS

FOLDER: MODEL LETTERS et Al

In accordance with 18 U.S.C. § 2709(c)(1), I certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person. Accordingly, 18 U.S.C. § 2709(c)(1) and (2) prohibits you, or any officer, employee, or agent of yours, from disclosing this letter, other than to those to whom disclosure is necessary to comply with the letter or to an attorney to obtain legal advice or legal assistance with respect to this letter.

In accordance with 18 U.S.C. § 2709(c)(3), you are directed to notify any persons to whom you have disclosed this letter that they are also subject to the nondisclosure requirement and are therefore also prohibited from disclosing the letter to anyone else.

3. Traffic Correlation



Our activities are linkable

> A lead can lead to everything else

VPNs are Pseudonymous

Through fingerprinting it is possible to indentify users

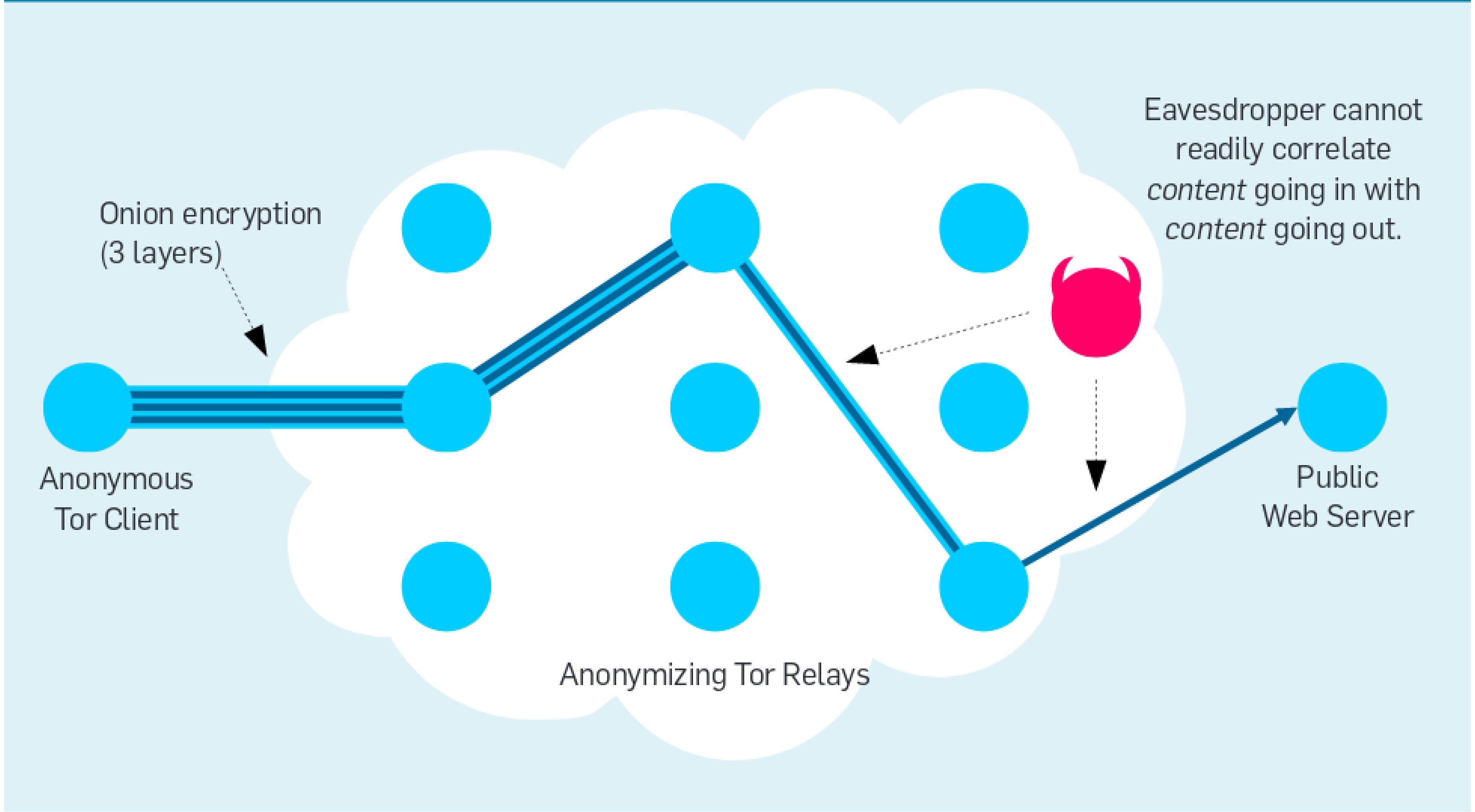
Anonymity is Hard

Onion Routing

- **use a chain of relays**
- **public key encryption for each of them**

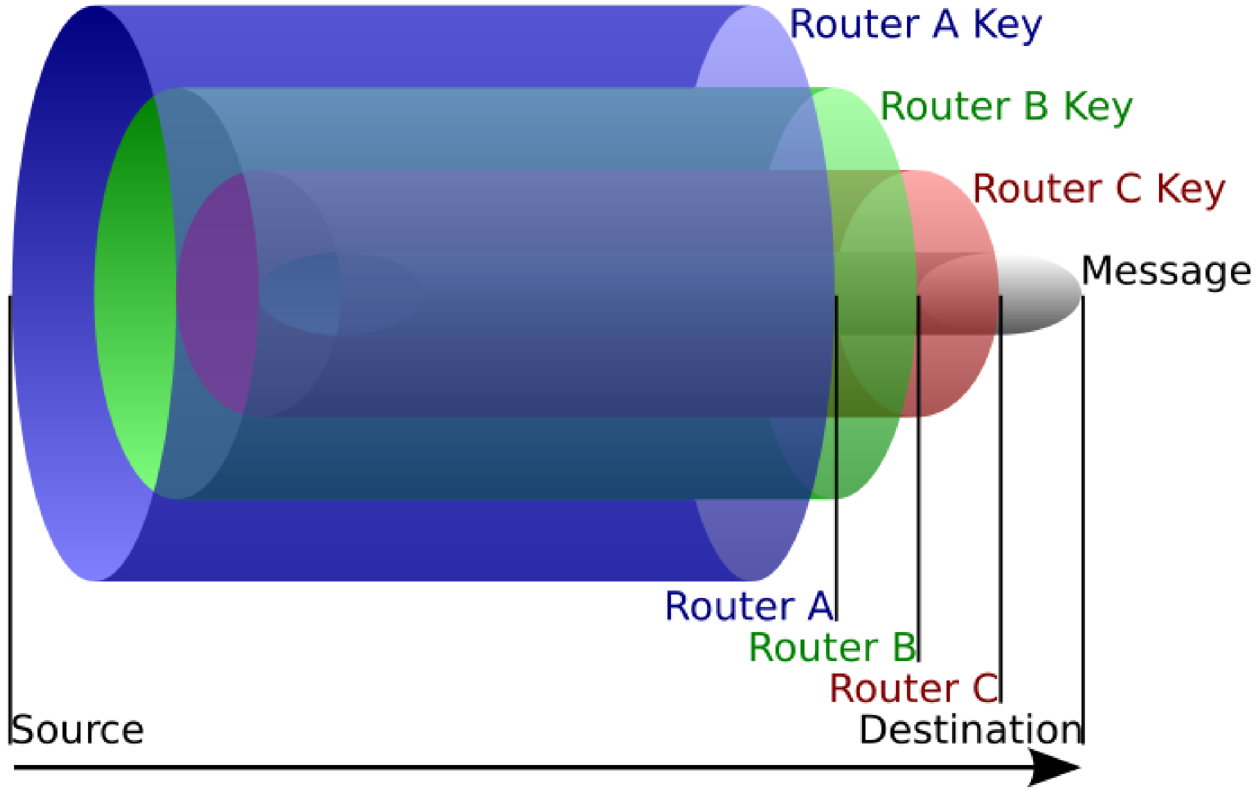
Onion Routing

Figure 1. Onion routing.



Eavesdropper cannot readily correlate *content* going in with *content* going out.

I don't see any onions there...

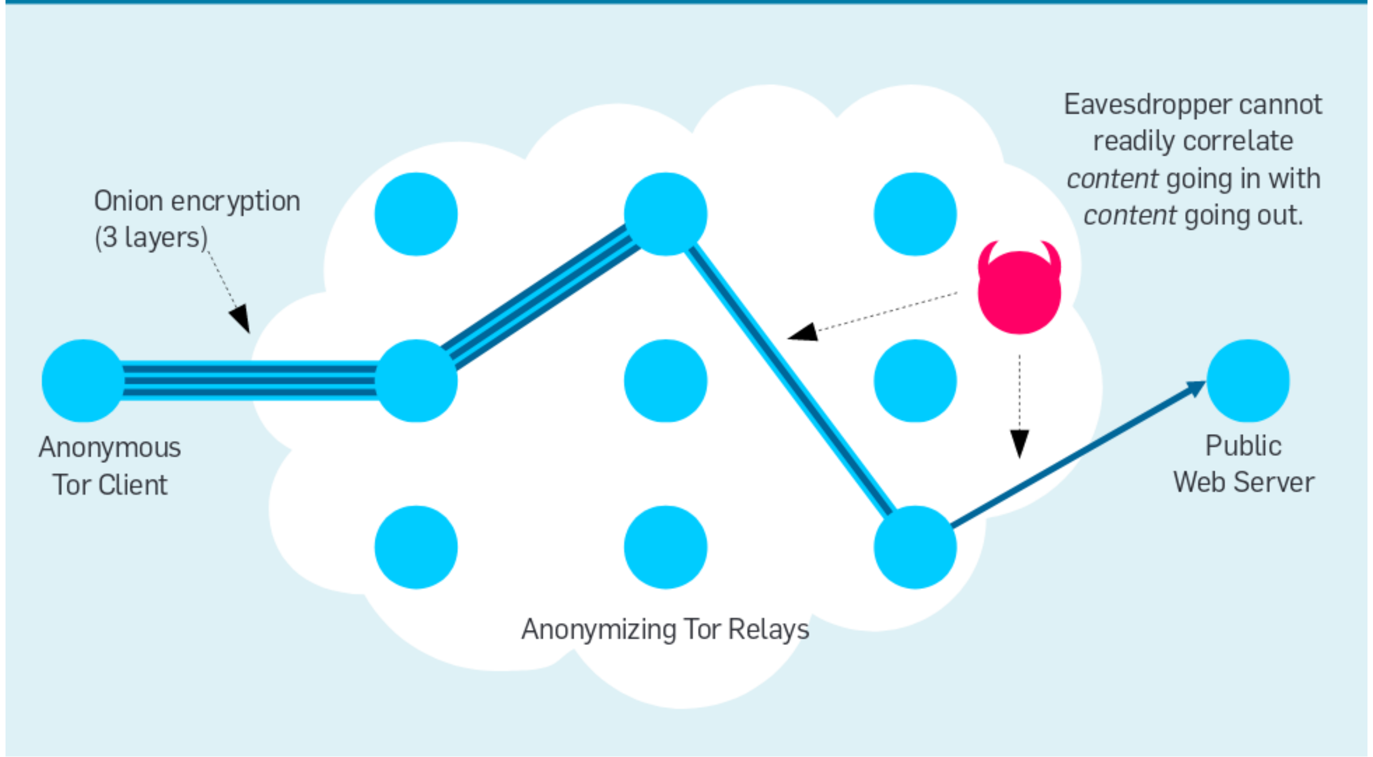


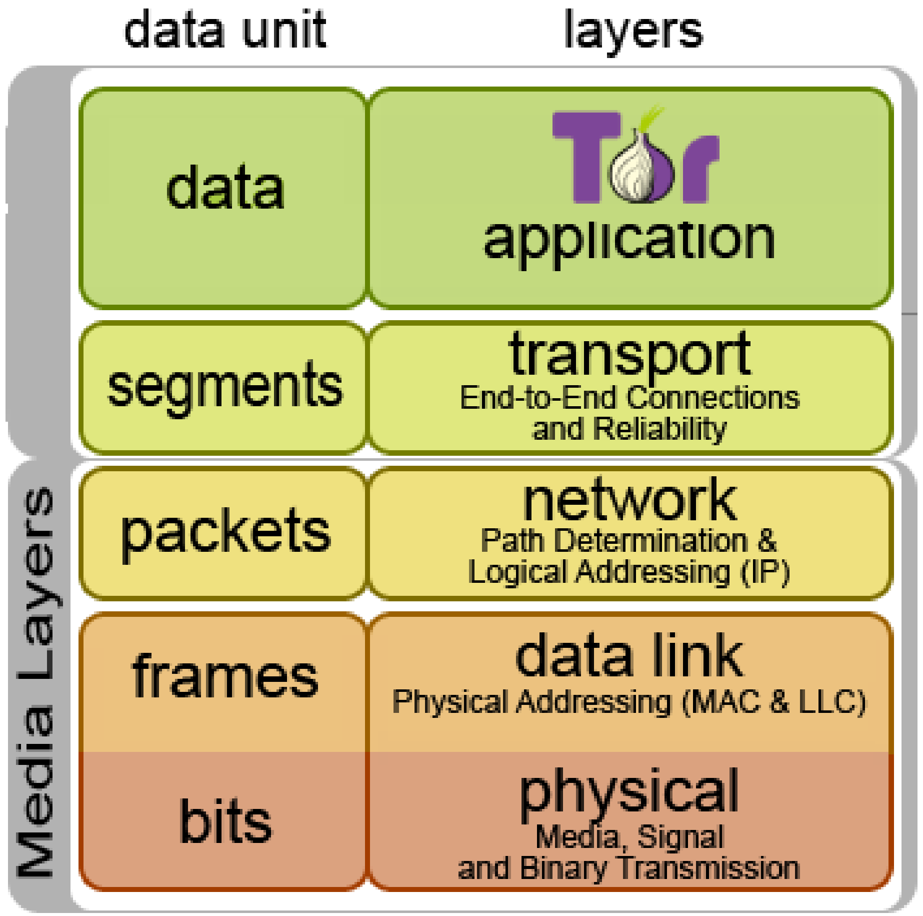
The *onion pattern* also comes up when we think of internet packets and their layers

Tor implements Onion Routing as an overlay network

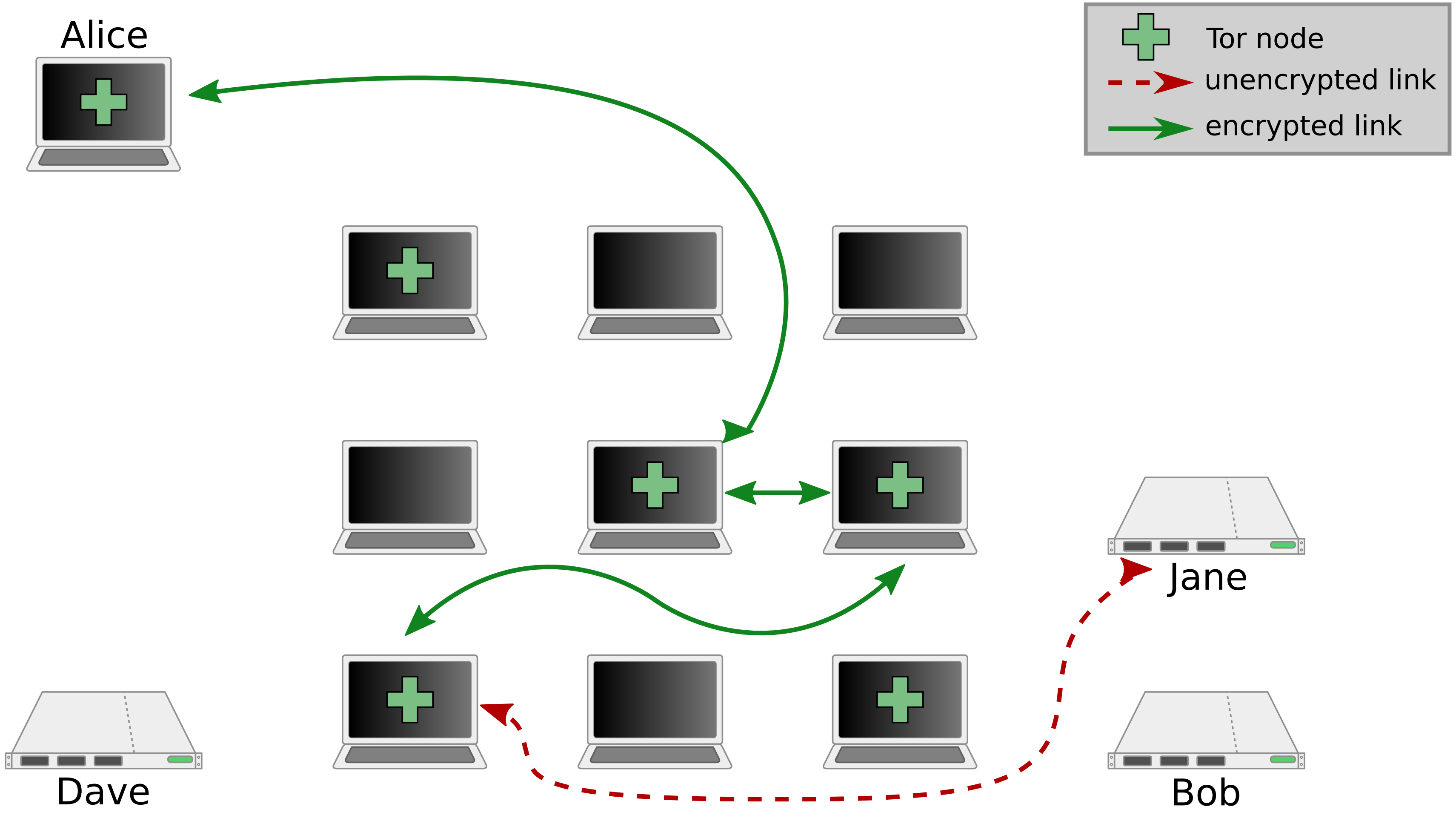
> Designed to anonymize **any TCP-based applications**
>
> through transparent proxy settings

Figure 1. Onion routing.



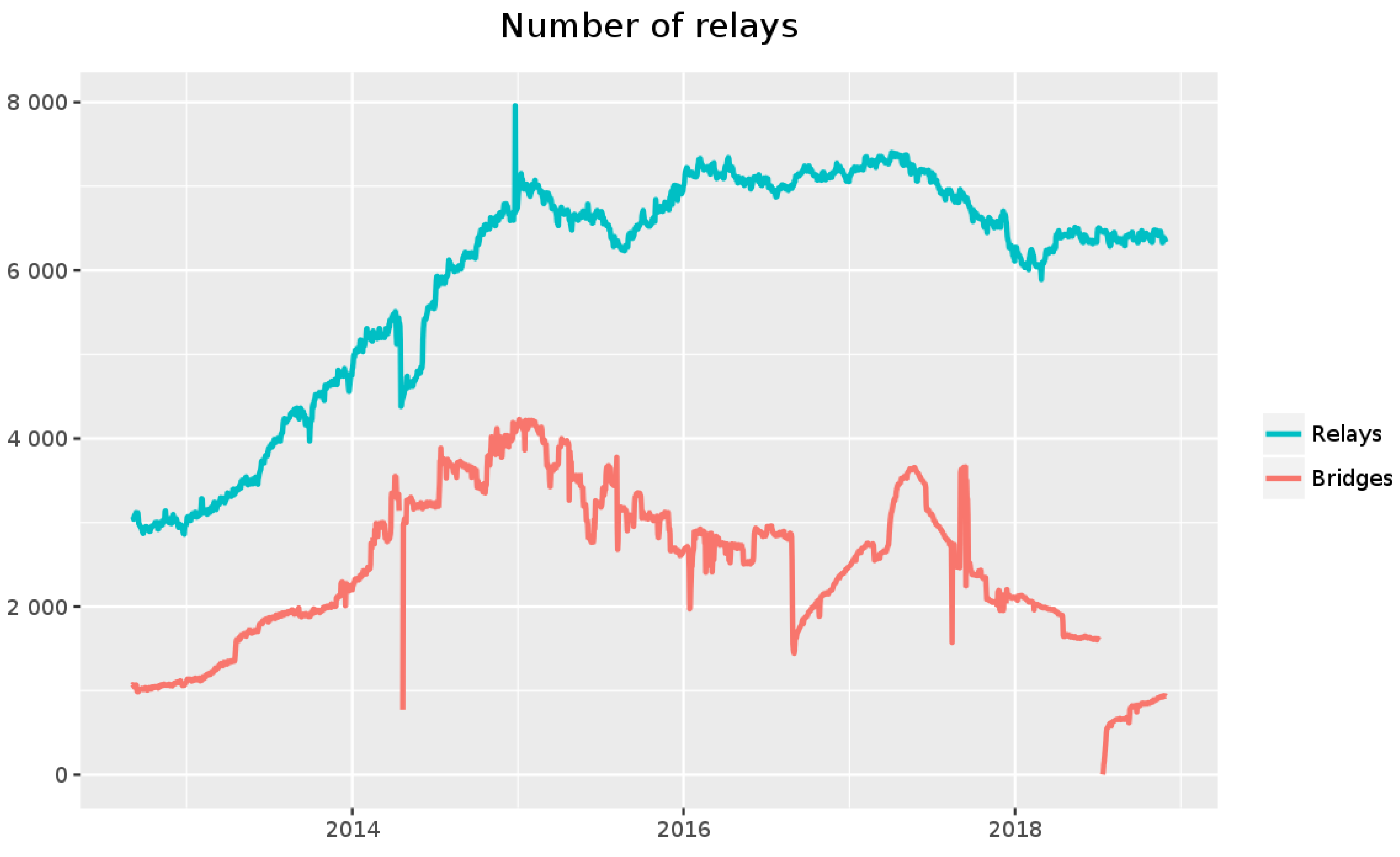


Onion Circuit



A circuit is a sequence of 3 nodes: *Guard*, *Middle* and *Exit*

Nodes are ran by Volunteers all around the World



The Tor Project - https://metrics.torproject.org/

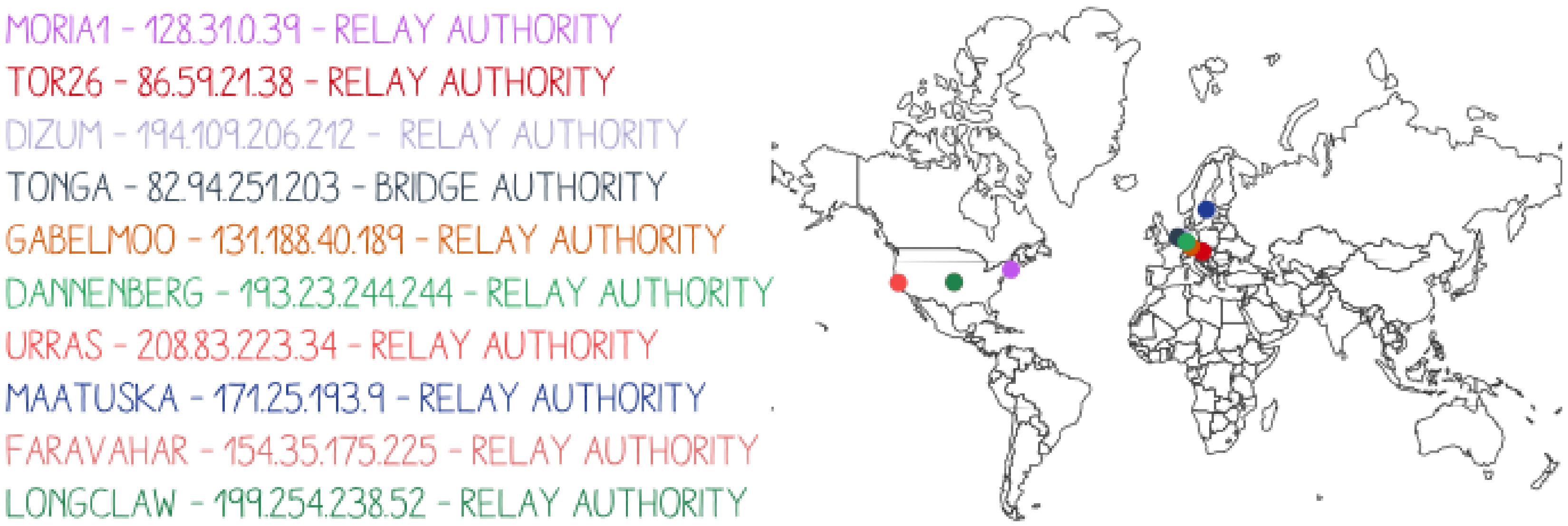
Not all Volunteers have good intentions

Tor is resistant to **bad relays** to a certain extent

But if they are too many it harms the nework and some uses might get de-anonymised

How to decide which nodes are part of the network?

Consensus Mechanism



MORIA1 - 128.31.0.39 - RELAY AUTHORITY
TOR26 - 86.59.21.38 - RELAY AUTHORITY
DIZUM - 194.109.206.212 - RELAY AUTHORITY
TONGA - 82.94.251.203 - BRIDGE AUTHORITY
GABELMOO - 131.188.40.189 - RELAY AUTHORITY
DANNENBERG - 193.23.244.244 - RELAY AUTHORITY
URRAS - 208.83.223.34 - RELAY AUTHORITY
MAATUSKA - 171.25.193.9 - RELAY AUTHORITY
FARAVAHAR - 154.35.175.225 - RELAY AUTHORITY
LONGCLAW - 199.254.238.52 - RELAY AUTHORITY

Anyone can see the votes of each relay by downloading

```
http://[directory_authority]/tor/status-vote/current/consensus/
```

Typically this is fetched trough http but now it can be fetched through tor, leaving less traces that the user is using tor.

The **consensus status** can be found here

Your computer chooses the circuit

Anonymity is Fragile

Everything we do is identifying:

- the pattern of our browsing habits
- the way we write text
- the way we code
- our typing speed, etc

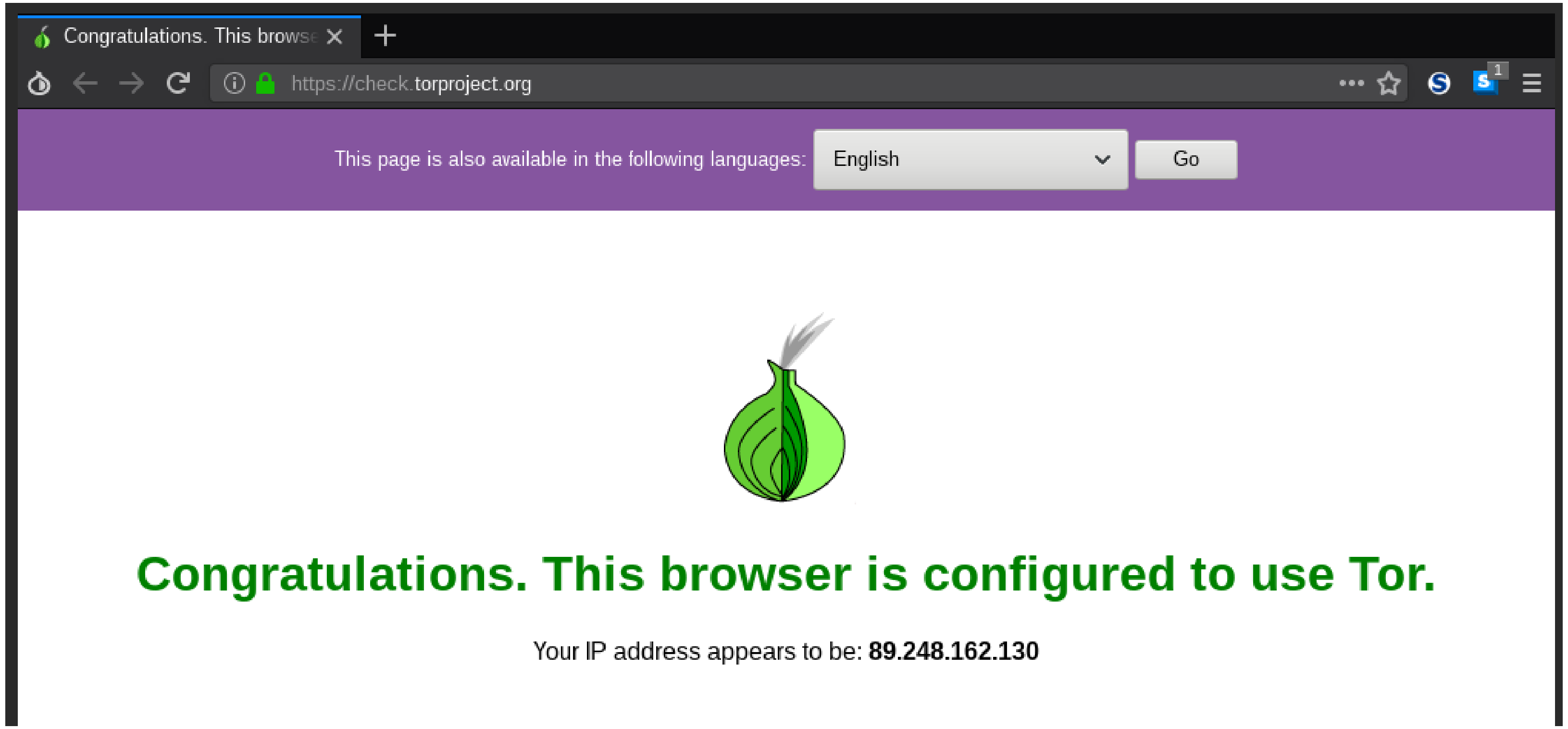
This means that

Tor alone is not enough

Tor Browser

A browser developed by the Tor Project that:

- sends traffic through the Tor network
- Implements additional measures to prevent the user to unwittingly giving away her/his identity



This page is also available in the following languages:

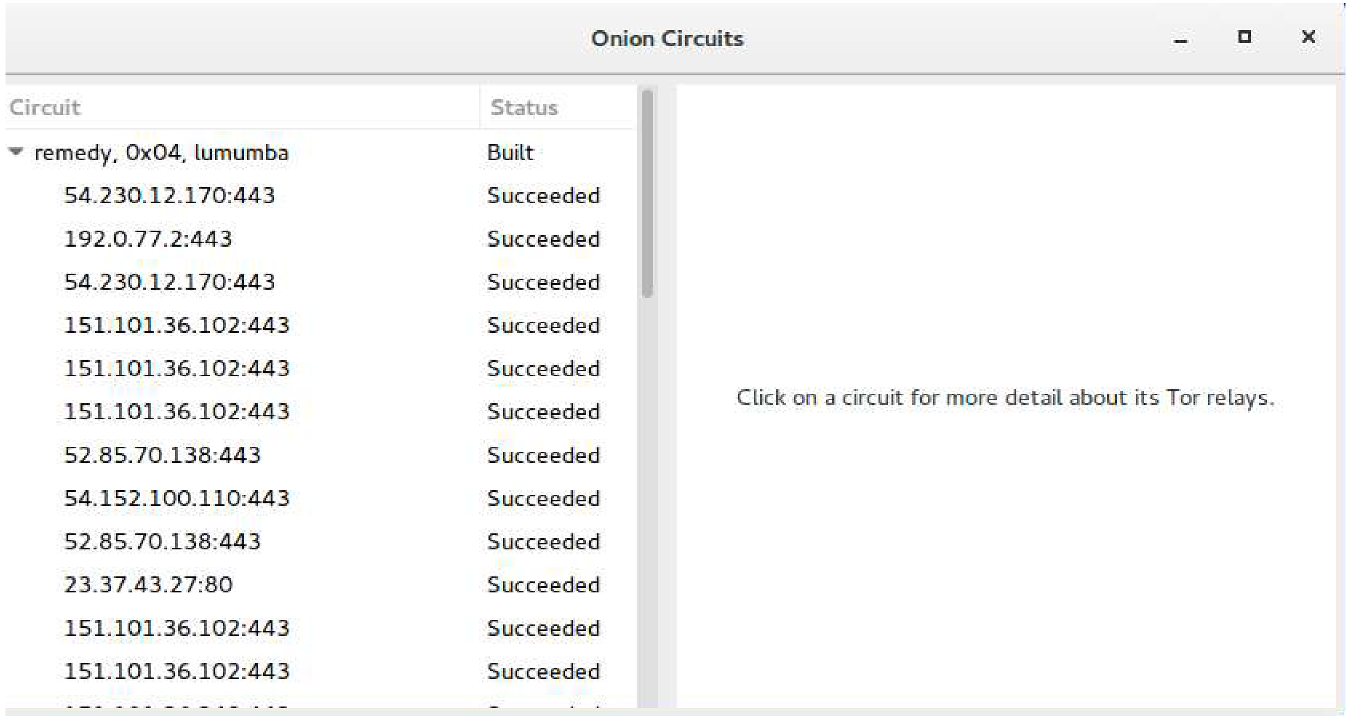
Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **89.248.162.130**

Stream Isolation

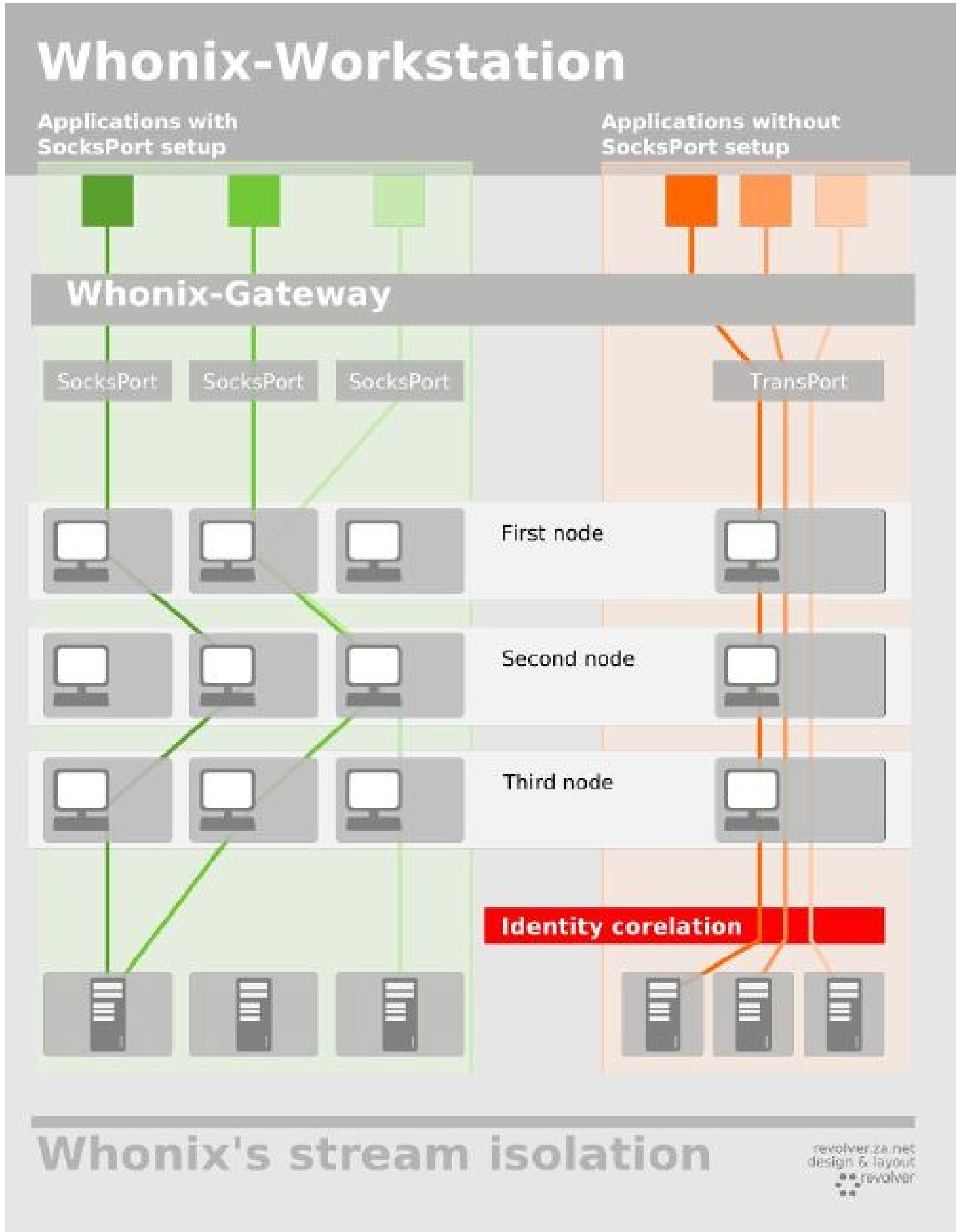
Identity Correlation: If the user is reading emails at the same time of browsing the web the activities can be correlated and the user identified

To fight this Tor implements **Stream Isolation** Creates a different circuit for each website / applic.



Circuit	Status
remedy, 0x04, lumumba	Built
54.230.12.170:443	Succeeded
192.0.77.2:443	Succeeded
54.230.12.170:443	Succeeded
151.101.36.102:443	Succeeded
151.101.36.102:443	Succeeded
151.101.36.102:443	Succeeded
52.85.70.138:443	Succeeded
54.152.100.110:443	Succeeded
52.85.70.138:443	Succeeded
23.37.43.27:80	Succeeded
151.101.36.102:443	Succeeded
151.101.36.102:443	Succeeded

Click on a circuit for more detail about its Tor relays.



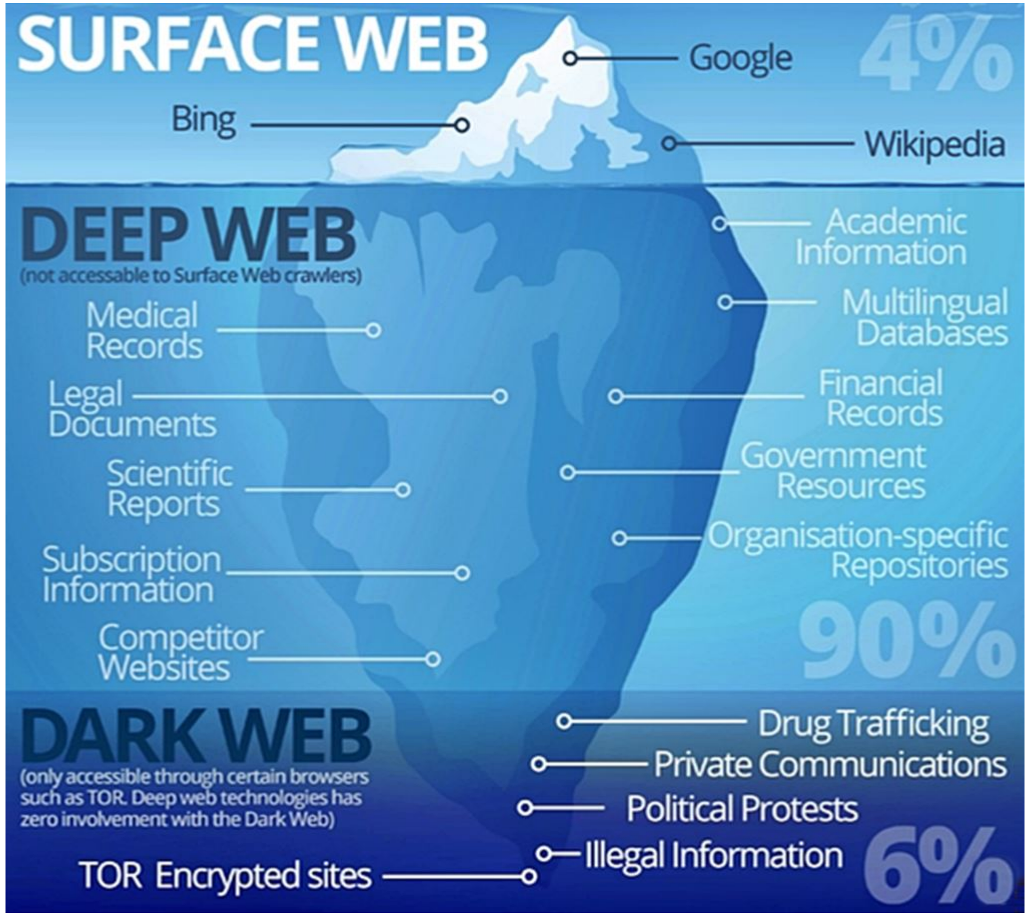
Whonix-Workstation
Applications with SocksPort setup
Applications without SocksPort setup
Whonix-Gateway
SocksPort
SocksPort
SocksPort
TransPort
First node
Second node
Third node
Identity corelation
Whonix's stream isolation
revolver.za.net design & layout revolver

Onion Services

> "End-to-End" Anonymity
>
> Aka. "" The Dark Web ""

The traffic never leaves the Tor network

Privacy for the user and the website operator.



example of **misinformation**
about onion services

(they only account for 3% of all tor traffic)

How does it look like?

Version 2: http://qubesos4rrrrz6n4.onion/

Version 3: http://sik5nlgfc5qylnnsr57qrbm64zbdx6t4lreyhpon3ychmxmiem7tioad.onion/

Self Authentication

No need for Certificate Authorites

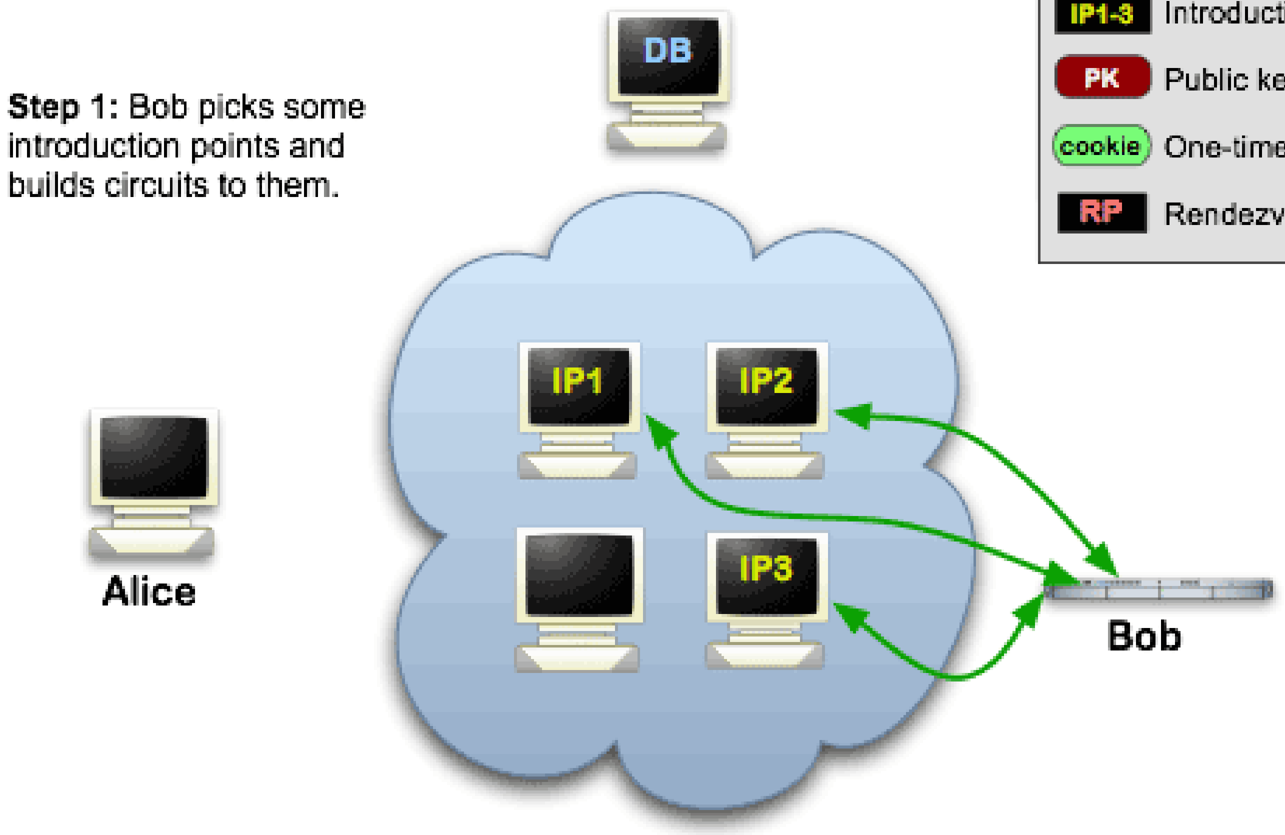
The URL is the publick key

correct URL = correct website

http://sik5nlgfc5qylnnsr57qrbm64zbdx6t4lreyhpon3ychmxmiem7tioad.onion/

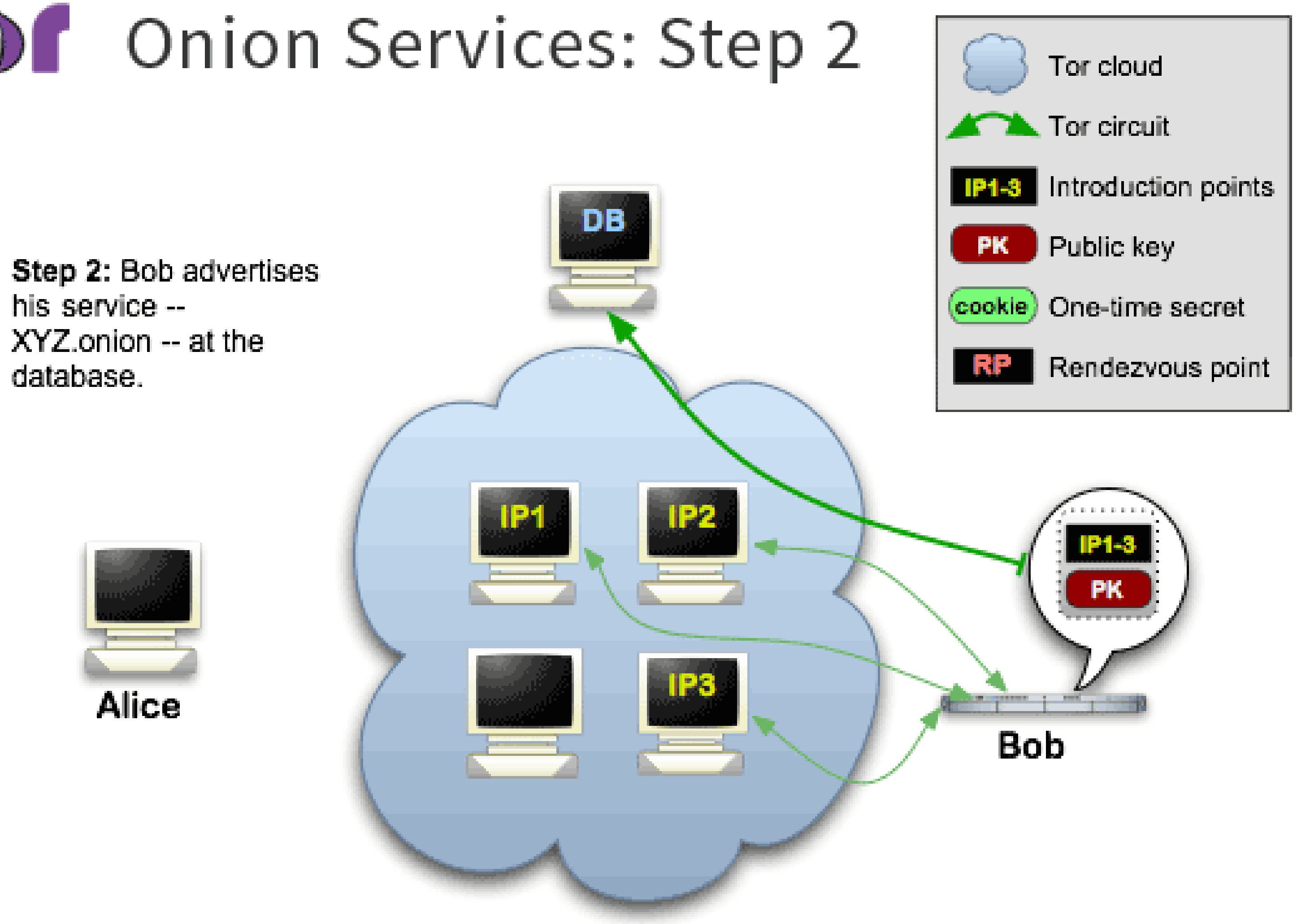
Onion Services: Step 1

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



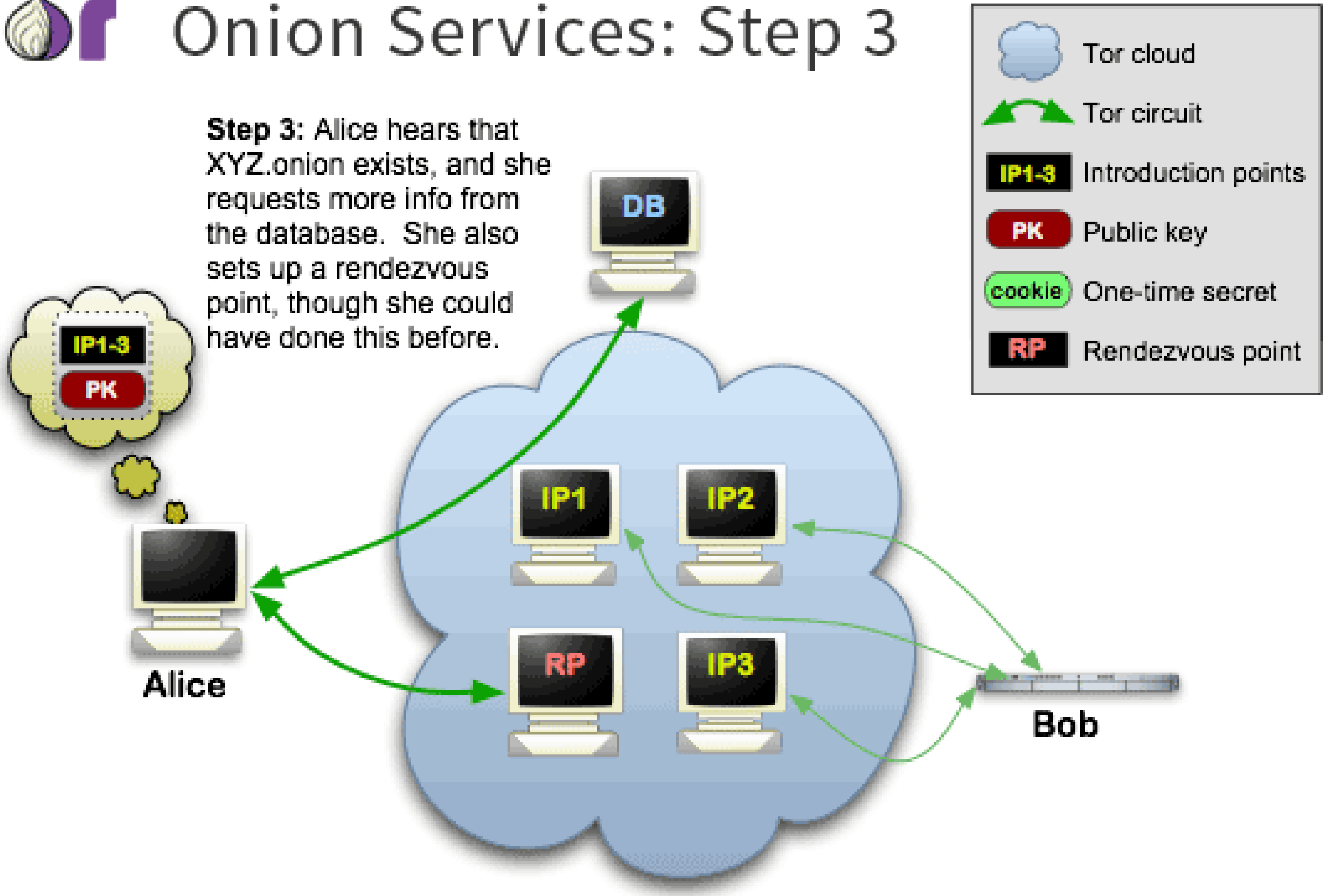
Step 1: Bob picks some introduction points and builds circuits to them.

Onion Services: Step 2



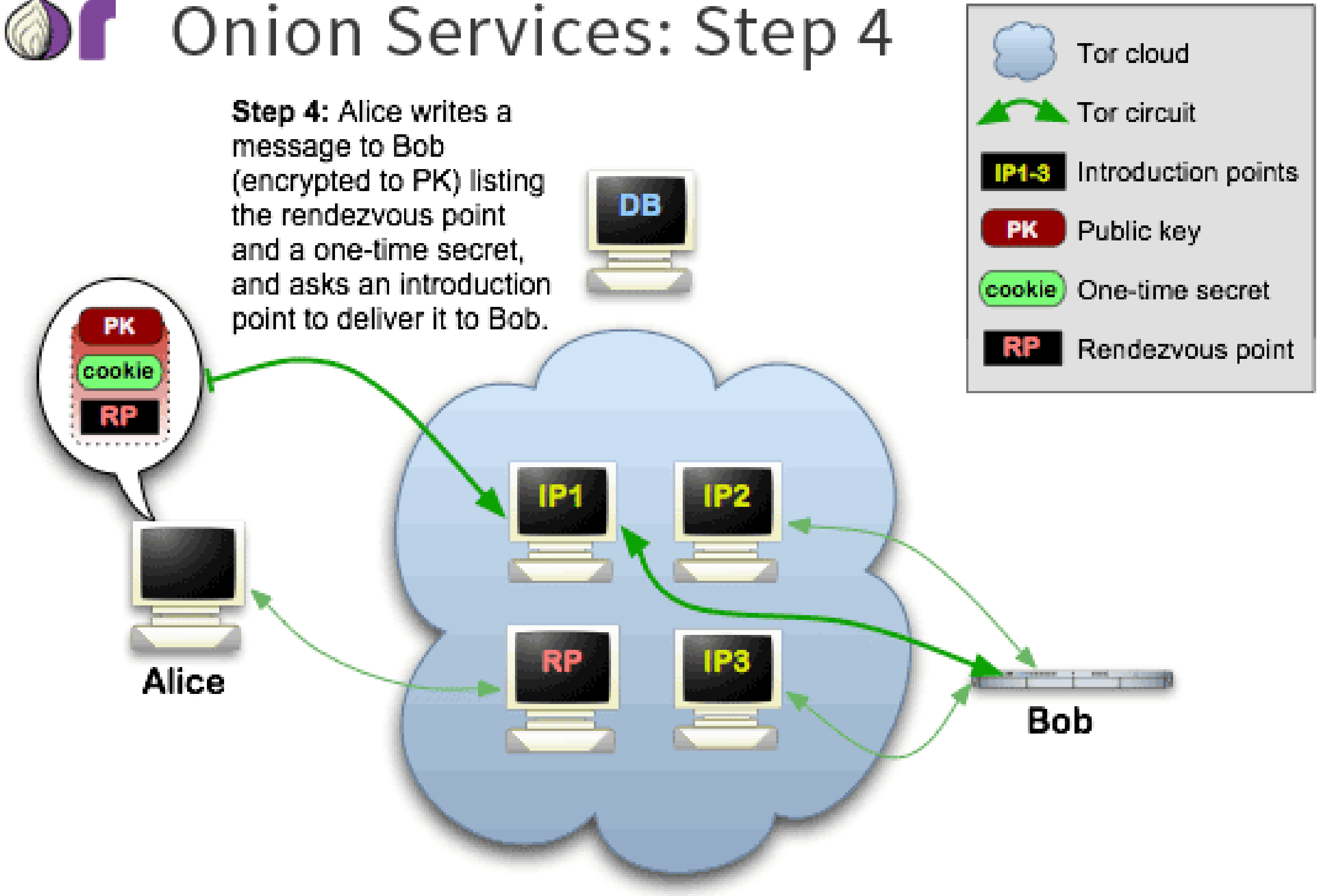
Step 2: Bob advertises his service -- XYZ.onion -- at the database.

Onion Services: Step 3



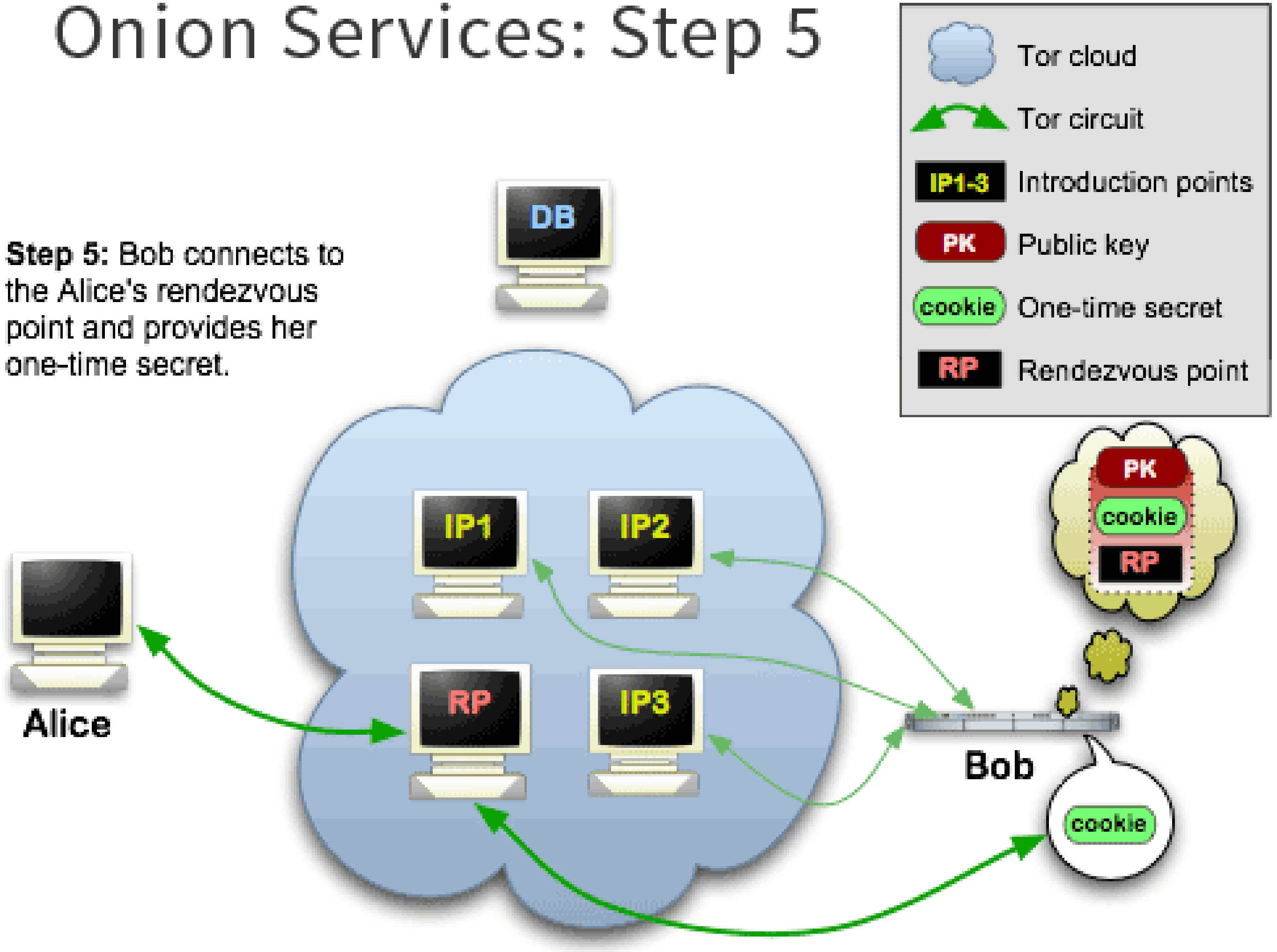
Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

Onion Services: Step 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.

Onion Services: Step 5



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

Censorship Resistance

A direct consequence of anonymity

> If I don't know who you are or where you go,
> I cannot block you access based on that information

Resources

Where you can find more information about how Tor works:

- A soft introduction to the Tor network written in Spanish
- Read the Orignal paper of tor
- Thirteen key design changes since the original 2004 paper: part one, part two, part three.
- Tor Documentation

Image credits

Copyright of the images to their respective owner. Used for the purpose of illustration

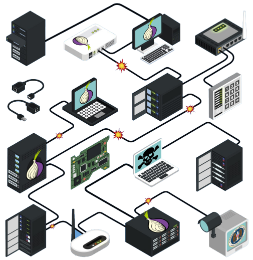
image	credit
	Hard to credit but it seems to come from an article from wired. The image was based on that one, but modified to add all of tor and nsa's logos.
	"On the Internet, nobody knows you're a dog" The famous cartoon by Peter Steiner.

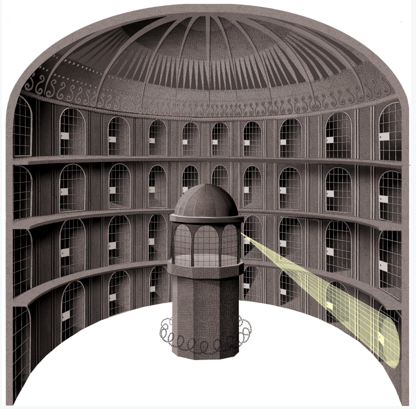
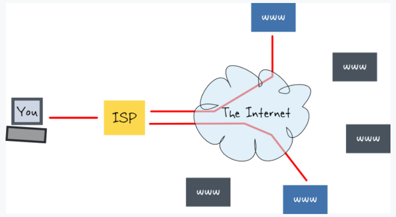
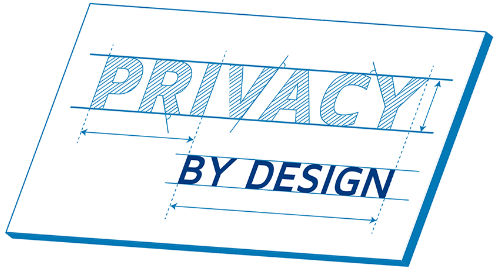
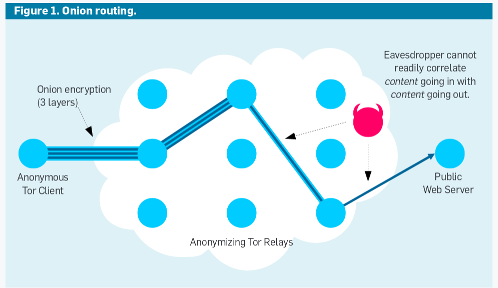
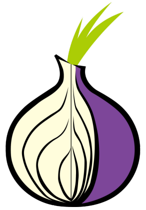
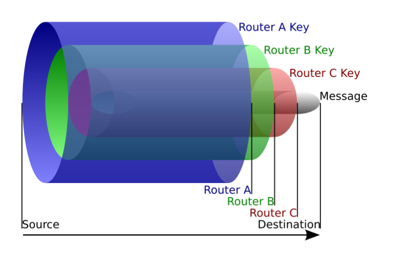
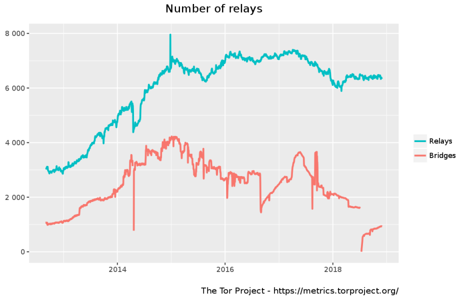
image	credit
   “Remember when, on the Internet, nobody knew who you were?”	The 2015 upgrade to the decades-old cartoon made by Kaamran Hafeez and published in The New Yorker on February 23, 2015
	A very nice illustration of the Panopticon prision concept. Taken from an NYtimes article

image	credit
MASS SURVEILLANCE HAS NO PLACE IN A FREE AND DEMOCRATIC SOCIETY ~~PRIVACY INTERNATIONAL~~	made by Privacy International
 You ISP The Internet www www www www www	Taken from this blog
	privacy by design logo is from the Privacy by Design Foundation
 Figure 1. Onion routing. Onion encryption (3 layers) Eavesdropper cannot readily correlate *content* going in with *content* going out. Anonymous Tor Client Public Web Server Anonymizing Tor Relays	From Brian Ford's article "Seeking Anonymity in an Internet Panopticon"

<table>
<tr><th>image</th><th>credit</th></tr>
<tr><td>

</td><td>Tor's logo</td></tr>
<tr><td>


</td><td>Wikimedia Commons</td></tr>
<tr><td>


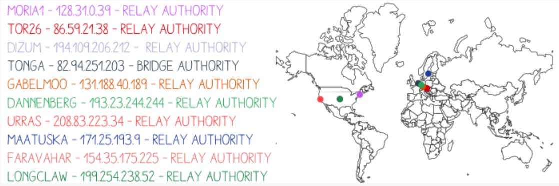
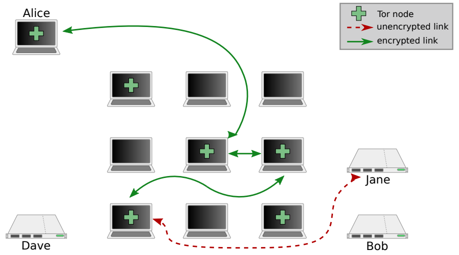
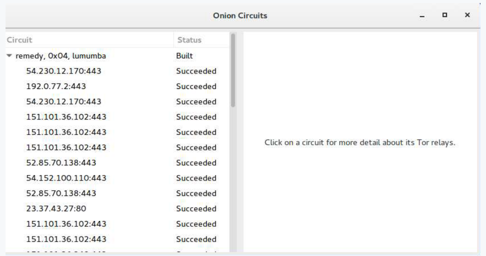
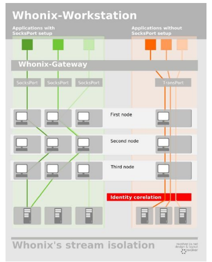
</td><td>You can find more fancy graphics of on tor metrics</td></tr>
<tr><td>

MORIA1 - 128.31.0.39 - RELAY AUTHORITY
TOR26 - 86.59.21.38 - RELAY AUTHORITY
DIZUM - 194.109.206.212 - RELAY AUTHORITY
TONGA - 82.94.251.203 - BRIDGE AUTHORITY
GABELMOO - 131.188.40.189 - RELAY AUTHORITY
DANNENBERG - 193.23.244.244 - RELAY AUTHORITY
URRAS - 208.83.223.34 - RELAY AUTHORITY
MAATUSKA - 171.25.193.9 - RELAY AUTHORITY
FARAVAHAR - 154.35.175.225 - RELAY AUTHORITY
LONGCLAW - 199.254.238.52 - RELAY AUTHORITY
</td><td>Taken from this article detailing the consensus mechanism</td></tr>
</table>

image	credit
 Alice Tor node unencrypted link encrypted link Jane Dave Bob	more similar diagrams here
 Onion Circuits Circuit Status remedy, 0x04, lumumba Built 54.230.12.170:443 Succeeded 192.0.77.2:443 Succeeded 54.230.12.170:443 Succeeded 151.101.36.102:443 Succeeded 151.101.36.102:443 Succeeded 151.101.36.102:443 Succeeded 52.85.70.138:443 Succeeded 54.152.100.110:443 Succeeded 52.85.70.138:443 Succeeded 23.37.43.27:80 Succeeded 151.101.36.102:443 Succeeded 151.101.36.102:443 Succeeded Click on a circuit for more detail about its Tor relays.	Onion Circuits is an application for viewing the current open and build tor circuits. It's quite good for new people using tor as they can see all that is going on in the background without it being too technical.
 Whonix-Workstation Applications with SocksPort setup Applications without SocksPort setup Whonix-Gateway SocksPort SocksPort SocksPort TransPort First node Second node Third node Identity corelation Whonix's stream isolation revolver.za.net design & layout revolver	Image of stream isolation of whonix. Taken from their wiki.
 	Hard to credit, but easy to love. It seems the oldest version of the image comes from here.