

Privacy, Anonymity, and Censorship

CS155 Computer and Network Security

Stanford University

What is Privacy?

Privacy is control over your own information. Freedom from intrusion into personal matters

Privacy is a person's right or expectation to control the disclosure of his/her personal information, including activity metadata

Privacy is the “right to be let alone” — Louis Brandeis

Privacy means something like what the Founders meant by “liberty” — Jacob Appelbaum

Free speech, free association, autonomy, ...

freedom from censorship and constant surveillance

Privacy-motivating examples in U.S. History

Martin Luther King Jr. “blackmailed” by FBI

McCarthyism witch-hunt for communists

Direct Sharing

The Incredible Story Of How Target Exposed A Teen Girl's Pregnancy



GUS LUBIN
FEB. 16, 2012, 10:27 AM

Target broke through to a new level of customer tracking with the help of statistical genius Andrew Pole, according to a [New York Times Magazine cover story by Charles Duhigg](#).

Pole identified 25 products that when purchased together indicate a woman is likely pregnant. The value of this information was that Target could send coupons to the pregnant woman at an expensive and habit-forming period of her life.

Plugged into Target's customer tracking technology, Pole's formula was a beast. Once it even exposed a teen girl's pregnancy:





Roll over image to zoom in

First Response Early Result Pregnancy Test, 3 tests, Packaging May Vary

by First Response

★★★★★ 486 customer reviews | 17 answered questions

#1 Best Seller in Pregnancy Tests

amazon student 47 Amazon Students rated this highly ★★★★★

List Price: \$19.57

Price: \$12.98 ✓Prime & Free Returns. Details

You Save: \$6.59 (34%)

Note: Available at a lower price from other sellers, potentially without free Prime shipping.

In Stock.

Ships from and sold by Amazon.com. Gift-wrap available.

Want it Tuesday, March 24? Order within **29 hrs 56 mins** and choose **One-Day Shipping** at checkout. Details

Package Quantity: 1

1	2	3
\$12.98 ✓Prime	\$41.00 ✓Prime	\$57.99

Customers Who Bought This Item Also Bought

Page 6 of 14 | [Start over](#)



Vitafusion Prenatal DHA and Folic Acid Gummy Vitamins, 180 Count
★★★★★ 140
\$20.25 ✓Prime



One A Day Women's Prenatal One Pill, 30 Count
★★★★★ 18
\$13.48 ✓Prime



Mayo Clinic Guide to a Healthy Pregnancy... the pregnancy experts...
★★★★★ 804
#1 Best Seller in Motherhood



Summer's Eve Cleansing Wash, Morning Paradise, 15 Ounce
★★★★★ 44
\$3.99



Nexcare 524560 Basal Digital Thermometer
★★★★★ 19
\$14.06 ✓Prime



Nature Made Prenatal Multi Vitamin Value Size, Tablets, 250-Count
★★★★★ 213
\$16.79 ✓Prime



Trojan Condom Pleasure Pack Lubricated, 40 Count
★★★★★ 126
\$18.12 ✓Prime




Third Party Tracking

☰ COSMOPOLITAN LOVE | CELEBS | BEAUTY & STYLE | FITNESS 🔍

18 Things You Should Know Before Dating a Cat Lady


She knows the difference between a guy who's allergic to cats and a guy who's "allergic to cats."



By Anna Breslaw


12.3k
Shares

f SHARE 12.2K
TWEET 46
PIN 6


MOST READ


Does Seafood Make Guys Horny?


13 Things You Should Know Before Dating Someone Wh...



Instagram

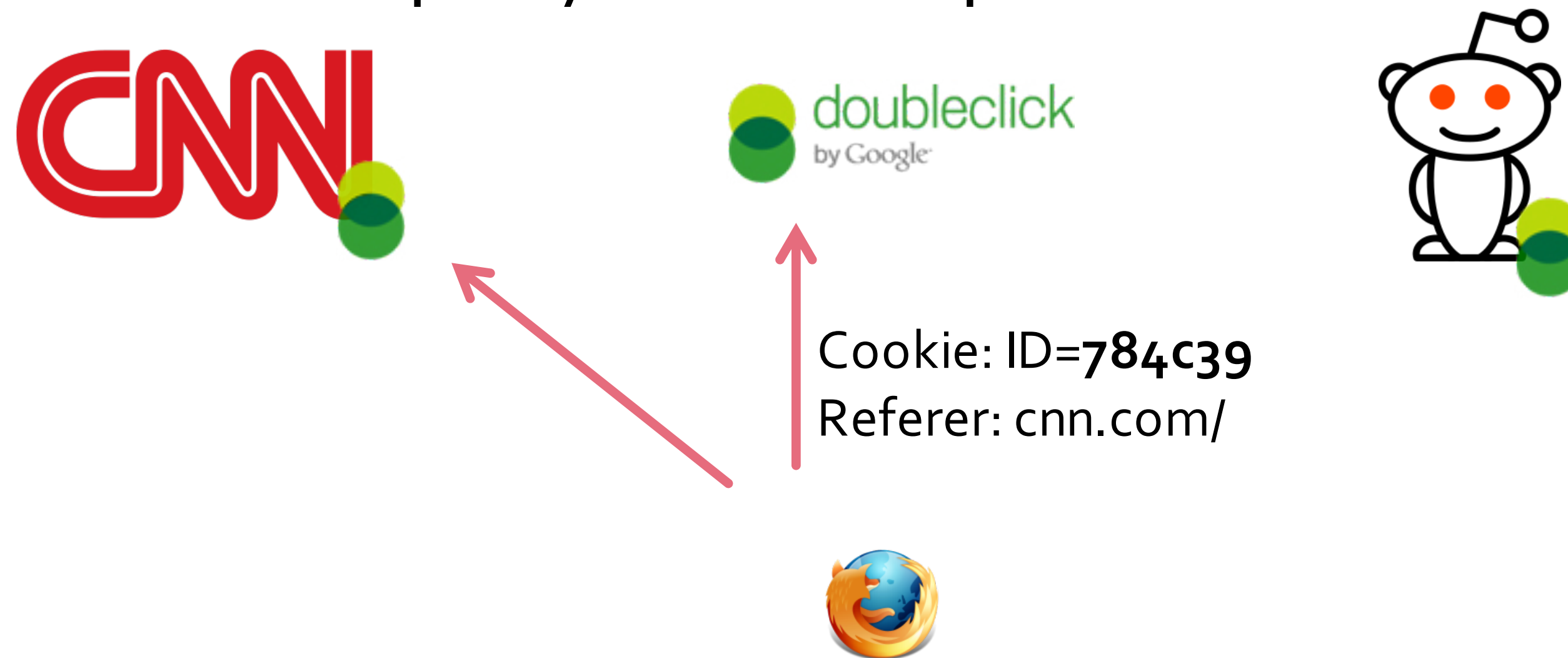


f T P

- 1. First of all, define "cat lady."** Does one cat = cat lady? Two cats = cat lady? Does joking about being a cat lady à la sparkling, outgoing multimillionaire Taylor Swift automatically make one a cat lady? It is my personal belief that most female cat owners below the age of 40 fall into the "not a cat girl, not yet a cat lady" category.
- 2. Cat ladies mostly look like ... normal ladies.** You know. Like regular women. Not like the old hag who sits in front of your local Shop Rite with aluminum foil on her head.

Third Party Cookies

- Site A's page requests a third-party resource (image, script, iframe)
 - Normally, browser sends cookie associated with that third-party in that request



Third Party Cookies

- Site A's page requests a third-party resource (image, script, iframe)
 - Normally, browser sends cookie associated with that third-party in that request



Third Party Cookies

Facebook, DoubleClick, etc. know much more about you than actual website does because they can track you across websites.

Domain	Top 1M	Domain	Top 1M
google-analytics.com	67.8%	ajax.googleapis.com	23.1%
gstatic.com	50.1%	googlesyndication.com	19.6%
fonts.googleapis.com	42.8%	googleadservices.com	14.1%
doubleclick.net	40.5%	twitter.com	12.8%
facebook.com	33.7%	fbcdn.net	10.7%
google.com	33.2%	adnxs.com	10.5%
facebook.net	27.4%		

For quick access, place your bookmarks here on the Bookmarks bar. [Import bookmarks now...](#)



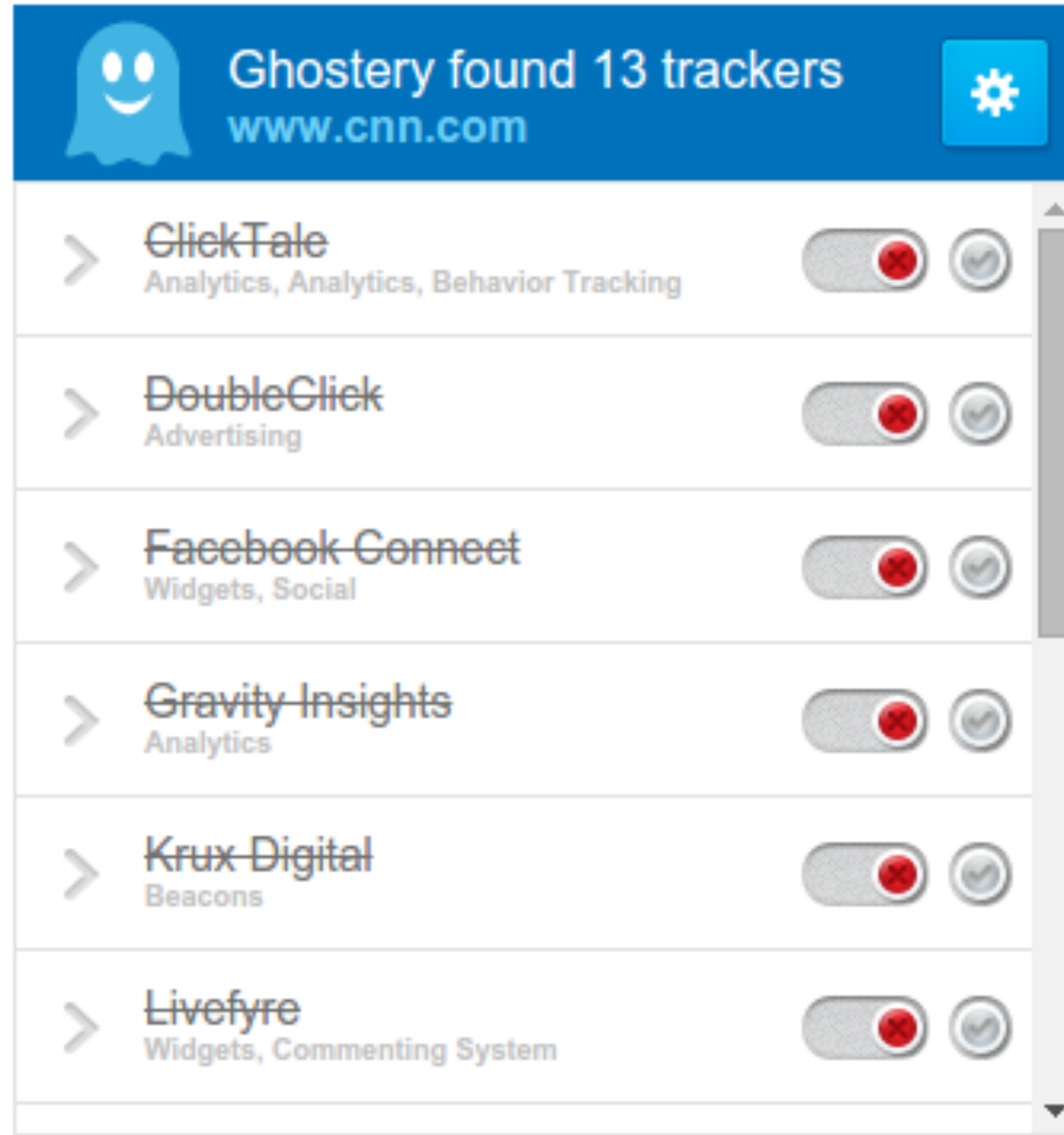
You've gone incognito

Pages you view in Incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your Incognito tabs. Any files you download or bookmarks you create will be kept.

However, you aren't invisible. Going Incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

[LEARN MORE](#)

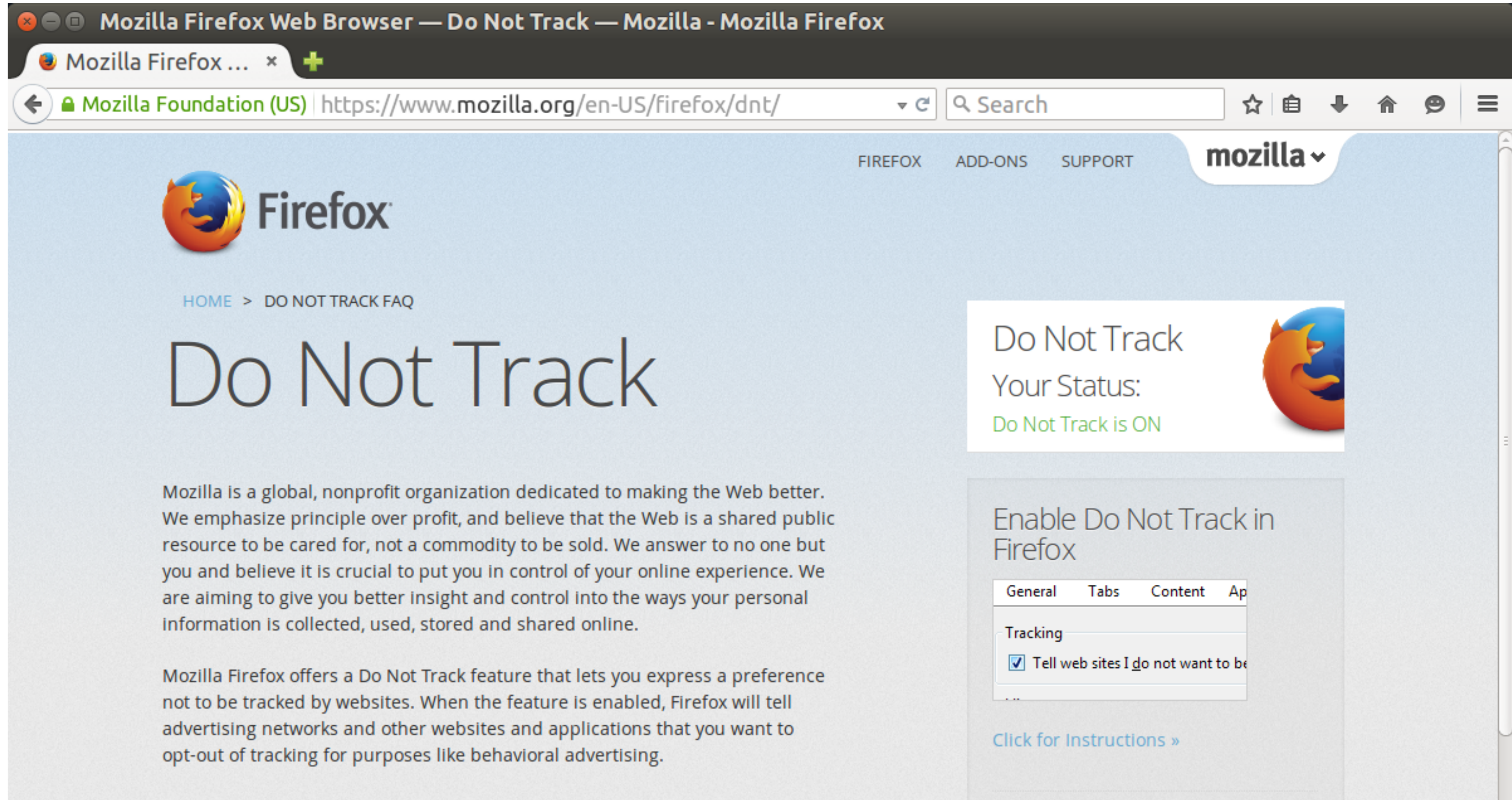
Ghostery



The screenshot displays the Ghostery browser extension interface. At the top, a blue header bar contains the Ghostery logo (a blue ghost), the text "Ghostery found 13 trackers", the URL "www.cnn.com", and a settings gear icon. Below the header, a list of detected trackers is shown, each with a chevron icon on the left, the tracker name, a brief description, a toggle switch, and a settings icon. The trackers listed are:

Tracker Name	Description	Status
ClickTale	Analytics, Analytics, Behavior Tracking	Blocked
DoubleClick	Advertising	Blocked
Facebook Connect	Widgets, Social	Blocked
Gravity Insights	Analytics	Blocked
Krux Digital	Beacons	Blocked
Livefyre	Widgets, Commenting System	Blocked

DNT




The screenshot shows a Mozilla Firefox browser window with the title "Mozilla Firefox Web Browser — Do Not Track — Mozilla - Mozilla Firefox". The address bar displays "Mozilla Foundation (US) | https://www.mozilla.org/en-US/firefox/dnt/". The page content includes the Firefox logo, a breadcrumb "HOME > DO NOT TRACK FAQ", and a large heading "Do Not Track". A status box on the right indicates "Do Not Track Your Status: Do Not Track is ON". Below this, a section titled "Enable Do Not Track in Firefox" shows a settings panel with the "Tracking" tab selected and the checkbox "Tell web sites I do not want to be tracked" checked. A link "Click for Instructions »" is also visible.

Mozilla Firefox Web Browser — Do Not Track — Mozilla - Mozilla Firefox

Mozilla Firefox ... x +


← Mozilla Foundation (US) | https://www.mozilla.org/en-US/firefox/dnt/ Search ☆ 📁 ↓ 🏠 🗨 ☰

FIREFOX ADD-ONS SUPPORT mozilla ▾

 **Firefox**

HOME > DO NOT TRACK FAQ

Do Not Track

Do Not Track
Your Status:
Do Not Track is ON 

Mozilla is a global, nonprofit organization dedicated to making the Web better. We emphasize principle over profit, and believe that the Web is a shared public resource to be cared for, not a commodity to be sold. We answer to no one but you and believe it is crucial to put you in control of your online experience. We are aiming to give you better insight and control into the ways your personal information is collected, used, stored and shared online.

Mozilla Firefox offers a Do Not Track feature that lets you express a preference not to be tracked by websites. When the feature is enabled, Firefox will tell advertising networks and other websites and applications that you want to opt-out of tracking for purposes like behavioral advertising.

Enable Do Not Track in Firefox

General Tabs Content Ap

Tracking

Tell web sites I do not want to be tracked

[Click for Instructions »](#)



Email Updates

Federal Court Finder

Careers

News

Listen to this page

Search uscourts.gov



About Federal Courts

Judges & Judgeships

Services & Forms

Court Records

Statistics & Reports

Rules & Policies

Services & Forms

★ Bankruptcy

Bankruptcy Basics

Filing Without an Attorney

Credit Counseling and Debtor Education

Trustees and Administrators

Approved Bankruptcy Notice Providers

Share This Page



Bankruptcy

Bankruptcy helps people who can no longer pay their debts get a fresh start by liquidating assets to pay their debts or by creating a repayment plan. Bankruptcy laws also protect financially troubled businesses. This section explains the bankruptcy process and laws.

About Bankruptcy

Filing bankruptcy can help a person by discarding debt or making a plan to repay debts. A bankruptcy case normally begins when the debtor files a petition with the bankruptcy court. A petition may be filed by an individual, by spouses together, or by a corporation or other entity.

All bankruptcy cases are handled in federal courts under rules outlined in the U.S. Bankruptcy Code.

There are different types of bankruptcies, which are usually referred to by their chapter in the U.S. Bankruptcy Code.

- Individuals may file [Chapter 7](#) or [Chapter 13](#) bankruptcy, depending on the specifics of their situation.
- Municipalities—cities, towns, villages, taxing districts, municipal utilities, and school districts may file under [Chapter 9](#) to reorganize.

Related Links

[Bankruptcy Fees](#)

[Bankruptcy Forms](#)

[Chapter 7 Fee Waiver Procedures & Resources](#)

[Protection of Tax Information Guidance](#)

[Pending Bankruptcy Forms](#)

[Permitted Changes to Official Bankruptcy Forms](#)

Federal Court Finder

Location

Court Name

Address, city, state, or ZIP

Privacy Enhancing Technologies

Methods for protecting personal data

Most Common/Successful? TLS.

Comes with browser. Also used for protecting email. It just works, without you having to configure anything. Protects *contents* of communication from passive eavesdroppers and active MITM attacks.

Tools that provide confidentiality also provide some privacy. You probably don't want your landlord or coffee shop customers to learn things about you.

Encouraging HTTPS Adoption

2014: HTTPS used as a page rank indicator

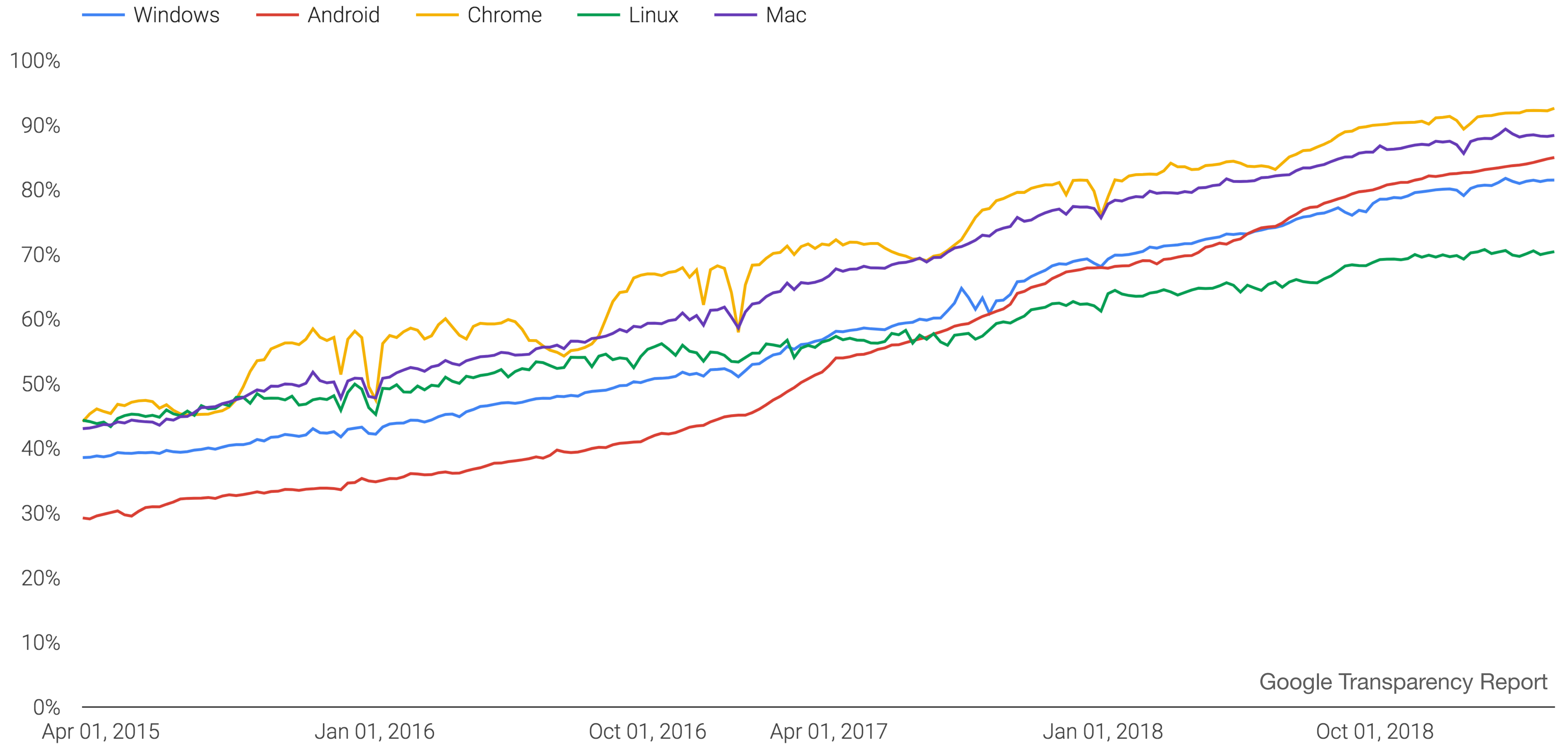
Early 2018: Mozilla announces that new features will require HTTPS

Late 2018: New Chrome HTTPS indicators

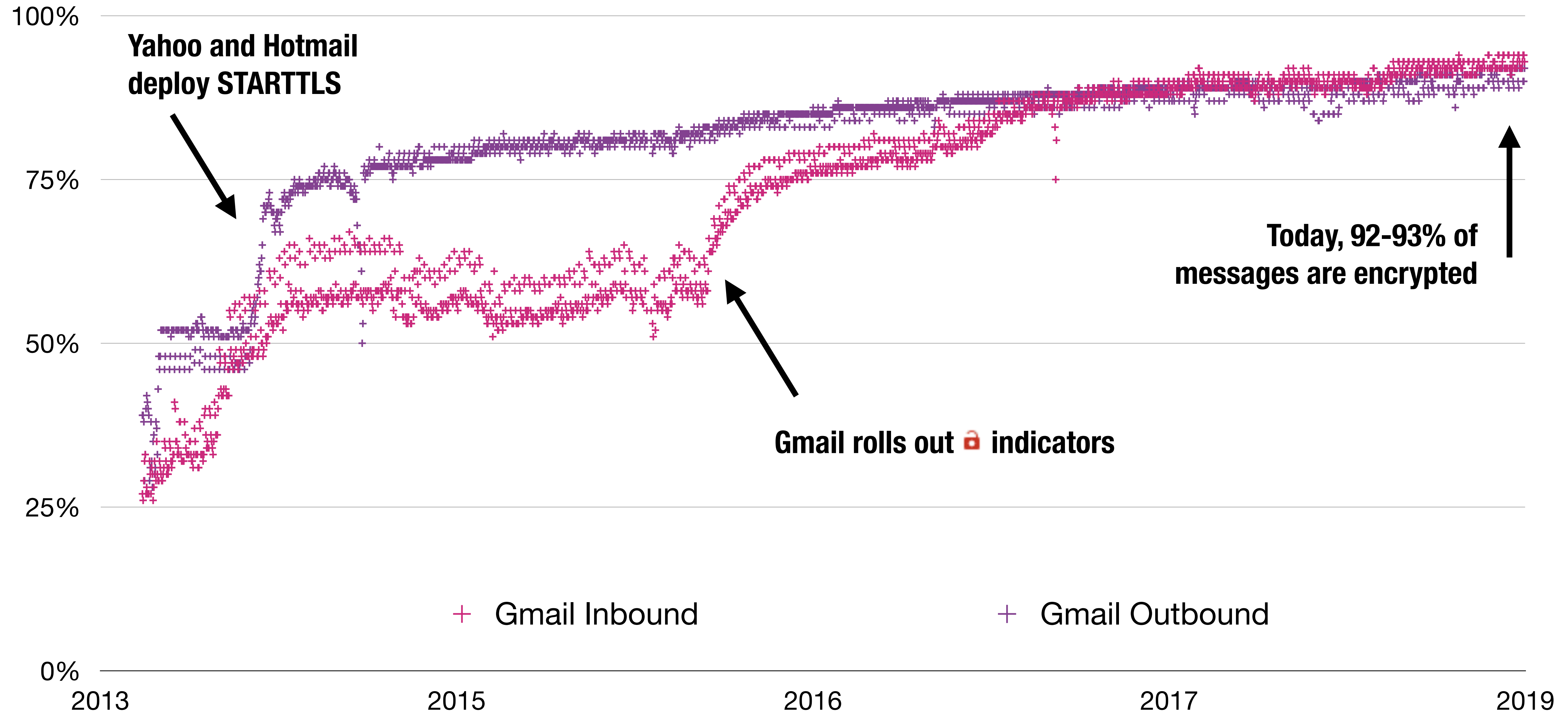
 example.com **(HTTPS)**

 Not secure | example.com **(HTTP)**

Chrome Page Loads over HTTPS



STARTTLS as seen by Gmail



Protecting Metadata

TLS only protects content. What doesn't TLS protect against?

We may want to protect metadata:

- Who is visiting what websites? Who is sending messages to whom?
- Gov't might not like that you're visiting Human Rights Watch website
- Gov't might not be amused that you're sending messages to Human Rights Watch
- We may want to hide the existence of the message (maybe sending an encrypted message at all is going to cause you problems)

What is Anonymity?

Anonymity (“without name”) means that a person is not identifiable within a set of subjects

Unlinkability of action and identity

- For example, sender and his email are no more related after adversary’s observations than they were before
- Who talks to whom

Unobservability

- Adversary cannot tell whether someone is using a particular system and/or protocol

Why Anonymity?

To protect privacy:

- Avoid tracking by advertising companies
- Viewing sensitive content
 - Information on medical conditions
 - Advice on bankruptcy

Protection from prosecution

- Not every country guarantees free speech

To prevent chilling-effects

- It's easier to voice unpopular or controversial opinions if you are anonymous

Anonymity is Hard

Internet anonymity is hard...

Right there in every packet is the source and destination IP address

ISPs store communications records

- Law enforcement can subpoena these records

Wireless traffic can be trivially intercepted

Tier 1 ASs and IXPs are compromised — NSA, GCHQ, “Five Eyes”

Anonymity

Difficult if not impossible to achieve on your own

You generally need help.

State of the art technique: Ask someone else to send it for you

Naive approach VPNs



Naive approach VPNs



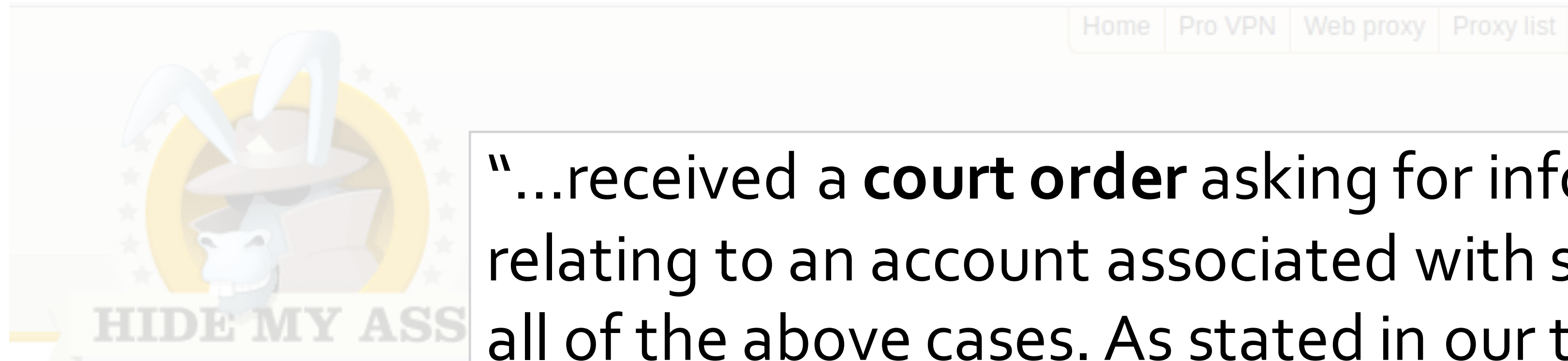
Lulzsec fiasco

Posted on [September 23, 2011](#)

We have received concerns by users that our VPN service was utilized by a member or members of the hacktivist group 'lulzsec'. Lulzsec have been ALLEGEDLY been responsible for a number of high profile cases such as:

- The hacking of the Sony Playstation network which compromised the names, passwords, e-mail addresses, home addresses and dates of birth of thousands of people.
- The DDOS attack which knocked the British governments SOCA (Serious Organised Crime Agency) and other government websites offline.
- The release of various sensitive and confidential information from companies such as AT&T, Viacom, Disney, EMI, NBC Universal, and AOL.
- Gaining access to NATO servers and releasing documents regarding the communication and information services (CIS) in Kosovo.
- The defacement of British newspaper websites The Sun & The Times

Naive approach VPNs



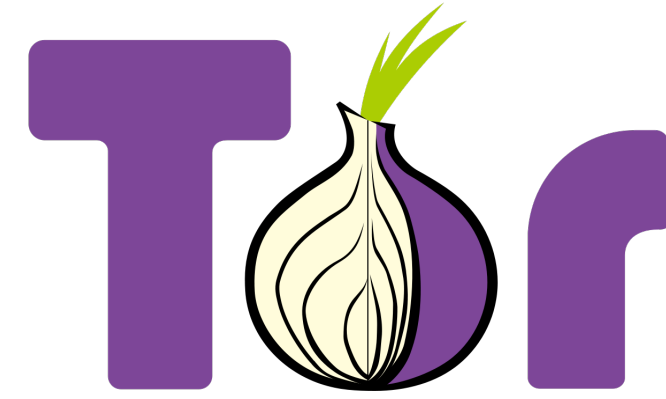
Lulzsec fiasco

Posted on [September 23, 2011](#)

We have received concerns by our users regarding the actions of the hacker/hacktivist group 'lulzsec'. Lulzsec has been responsible for actions such as:

- The hacking of the Sony Playstation network which compromised the names, passwords, e-mail addresses, home addresses and dates of birth of thousands of people.
- The DDOS attack which knocked the British governments SOCA (Serious Organised Crime Agency) and other government websites offline.
- The release of various sensitive and confidential information from companies such as AT&T, Viacom, Disney, EMI, NBC Universal, and AOL.
- Gaining access to NATO servers and releasing documents regarding the communication and information services (CIS) in Kosovo.
- The defacement of British newspaper websites The Sun & The Times

“...received a **court order** asking for information relating to an account associated with some or all of the above cases. As stated in our terms of service and **privacy policy** our service is not to be used for illegal activity, and as a legitimate company ***we will cooperate with law enforcement if we receive a court order***”



Tor is a successful privacy enhancing technology that works at the transport layer

Millions of active users.

Normally, a TCP connection reveals your IP address

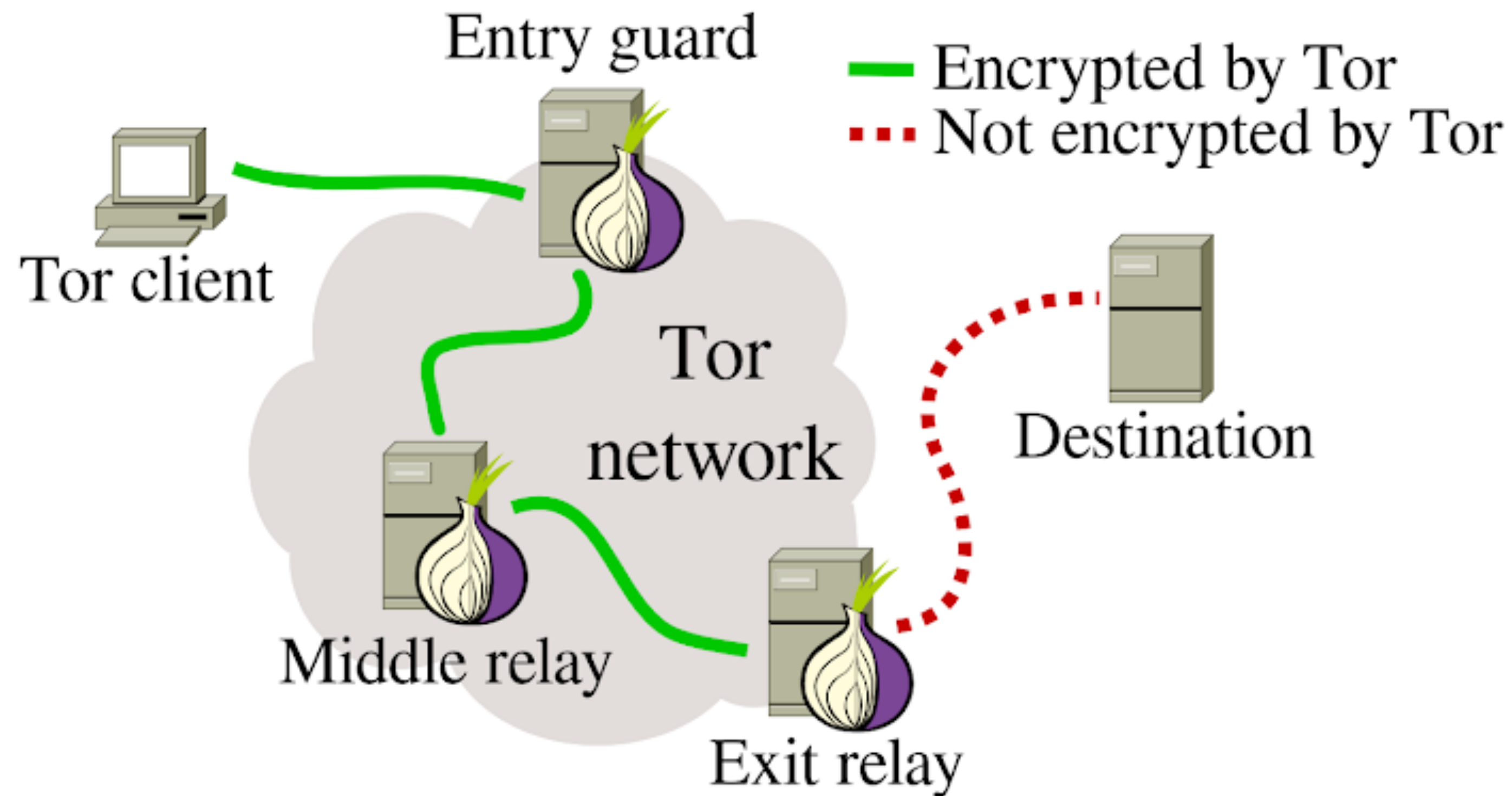
Tor allows TCP connections without revealing your IP

Directly connecting users



Tor (“The Onion Router”)

Tor operates by tunneling traffic through multiple “onion routers” using public key cryptography



Who Knows What?

Entry node: knows Alice is using Tor, and identity of middle node, but not destination

Exit node: knows some Tor user is connecting to destination, but not which user

Destination: knows a Tor user is connecting to it via the exit node

Tor does not provide encryption between exit and destination (use HTTPS!)

Does Tor Provide Anonymity?

Tor provides for anonymity in TCP connections over the Internet, both unlinkably (long-term) and linkably (short-term).

What does this mean?

- There's no long-term identifier for a Tor user
- If a web server gets a connection from Tor today, and another one tomorrow, it won't be able to tell whether those are from the same person
- But two connections in quick succession from the same Tor node are more likely to in fact be from the same person

Tor Challenges

Performance: message bounces around a lot (can be slow)

Attack: government can coerce server operates in one country

Defense: use mix servers in different legal jurisdictions

Attack: adversary operates all of the mixes

Defense: have lots of mix servers (Tor has ~7,000 onion routers today). Use diverse set.

Attack: adversary observes when Alice sends and when Bob receives, links the two together

A side channel attack – exploits timing information

Defenses: pad messages, introduce significant delays

Tor does the former, but notes that it's not enough for defense

Guard Relays

How do you protect against an adversary creating a large number of onion routers and performing timing observation at entrance and exits?

Limit the servers used for initial connection to a subset of trusted nodes:

- Have long and consistent uptimes...
- Have high bandwidth...
- Are manually vetted by the Tor community

Tor client selects 3 guard relays and uses them for 3 months

Exit Nodes

Relays must self-elect to be exit nodes. Why?

- Legal problems
- If someone does something malicious or illegal using Tor and the police trace the traffic, the trace leads to the exit node

Tor Hidden Services

As described, Tor protects the identity of the client, but not the server

What if we want to run an anonymous service?

- a website, where nobody knows the IP address?

Tor supports Hidden Services...

- Allows you to run a server without disclosing the IP or DNS name

Many hidden services

- Duck Duck Go, Tor Chat, Wikileaks

Tor Hidden Services: 1

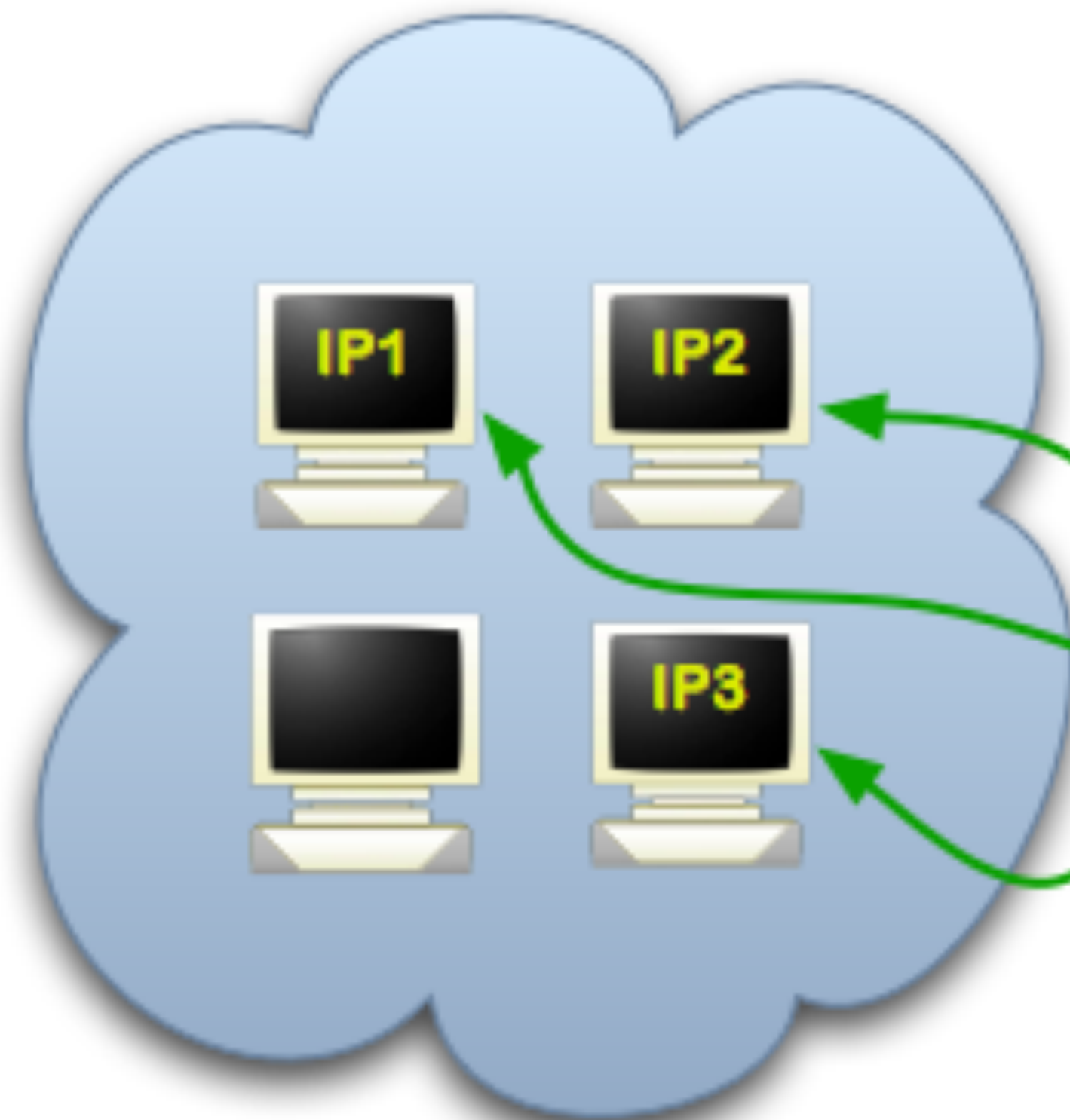
Step 1: Bob picks some introduction points and builds circuits to them.



Alice



DB



Tor cloud



Tor circuit

IP1-3

Introduction points

PK

Public key

cookie

One-time secret

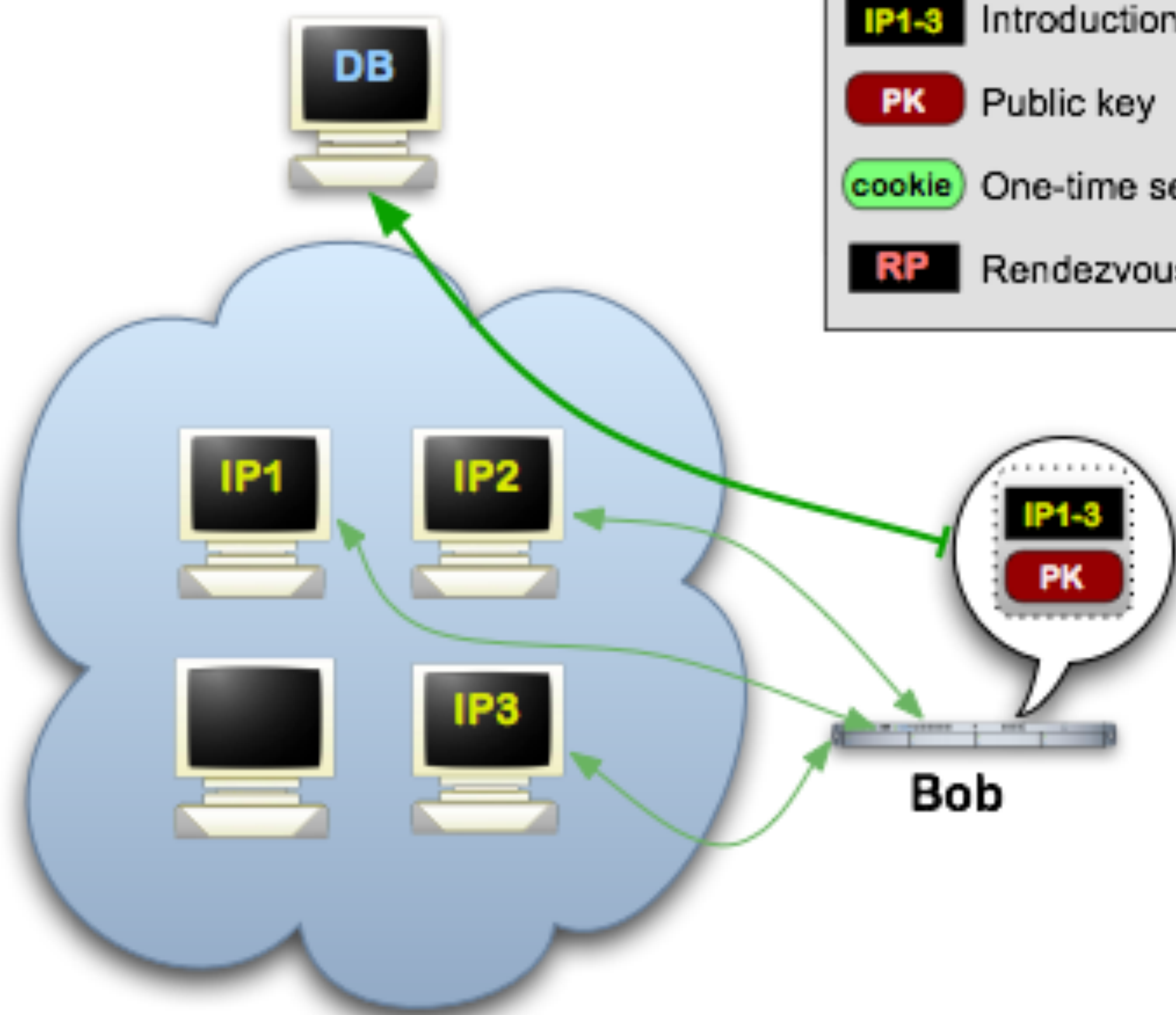
RP




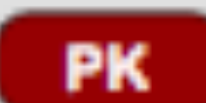
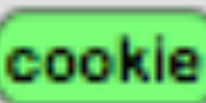

Rendezvous point

Bob

Tor Hidden Services: 2

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



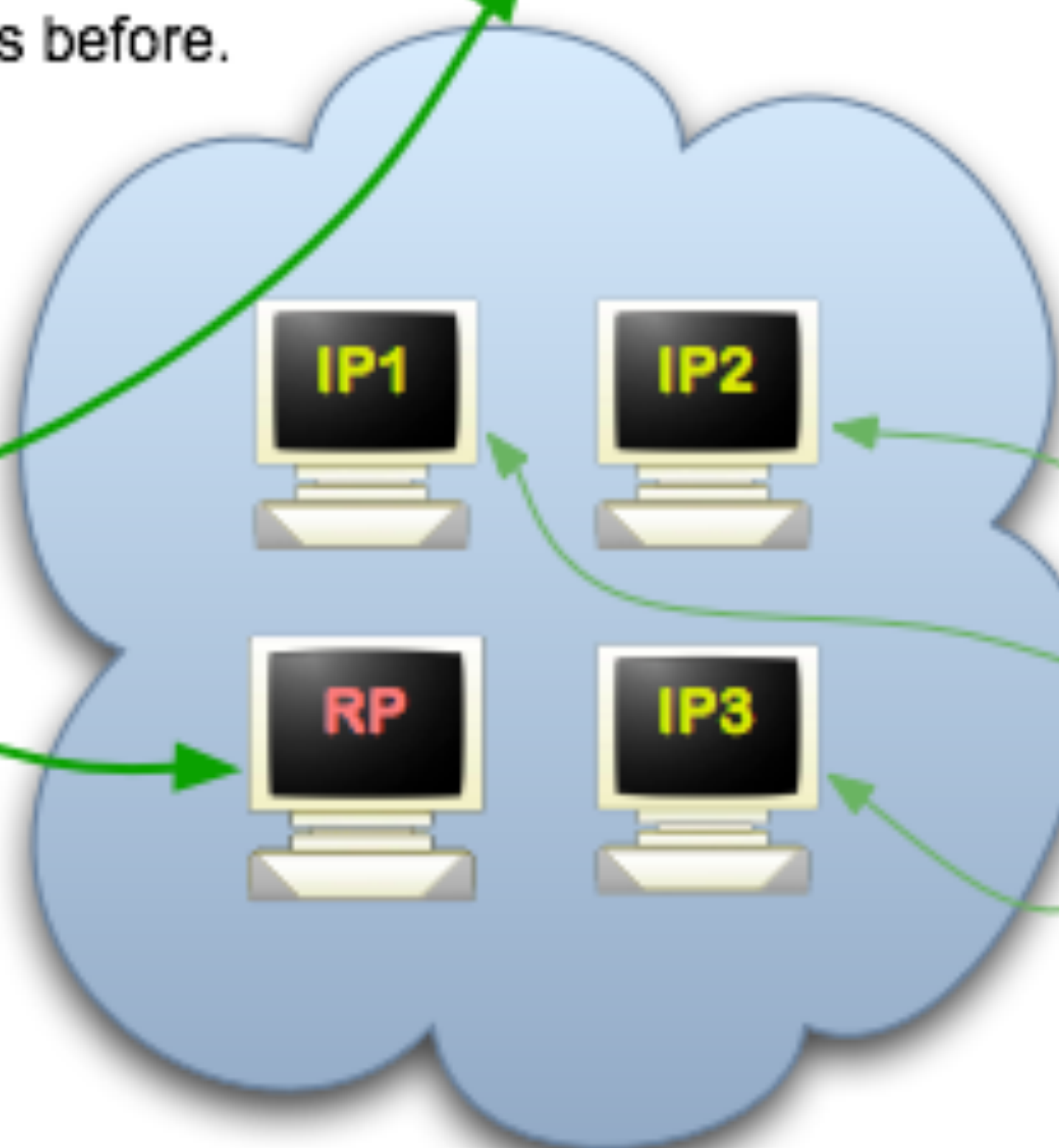
-  Tor cloud
-  Tor circuit
-  Introduction points
-  Public key
-  One-time secret
-  Rendezvous point

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.



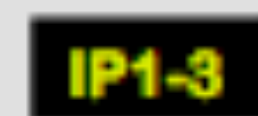
Alice



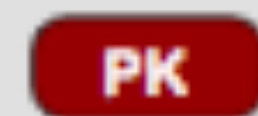
Tor cloud



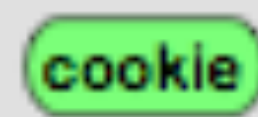
Tor circuit



IP1-3 Introduction points



PK Public key



cookie One-time secret



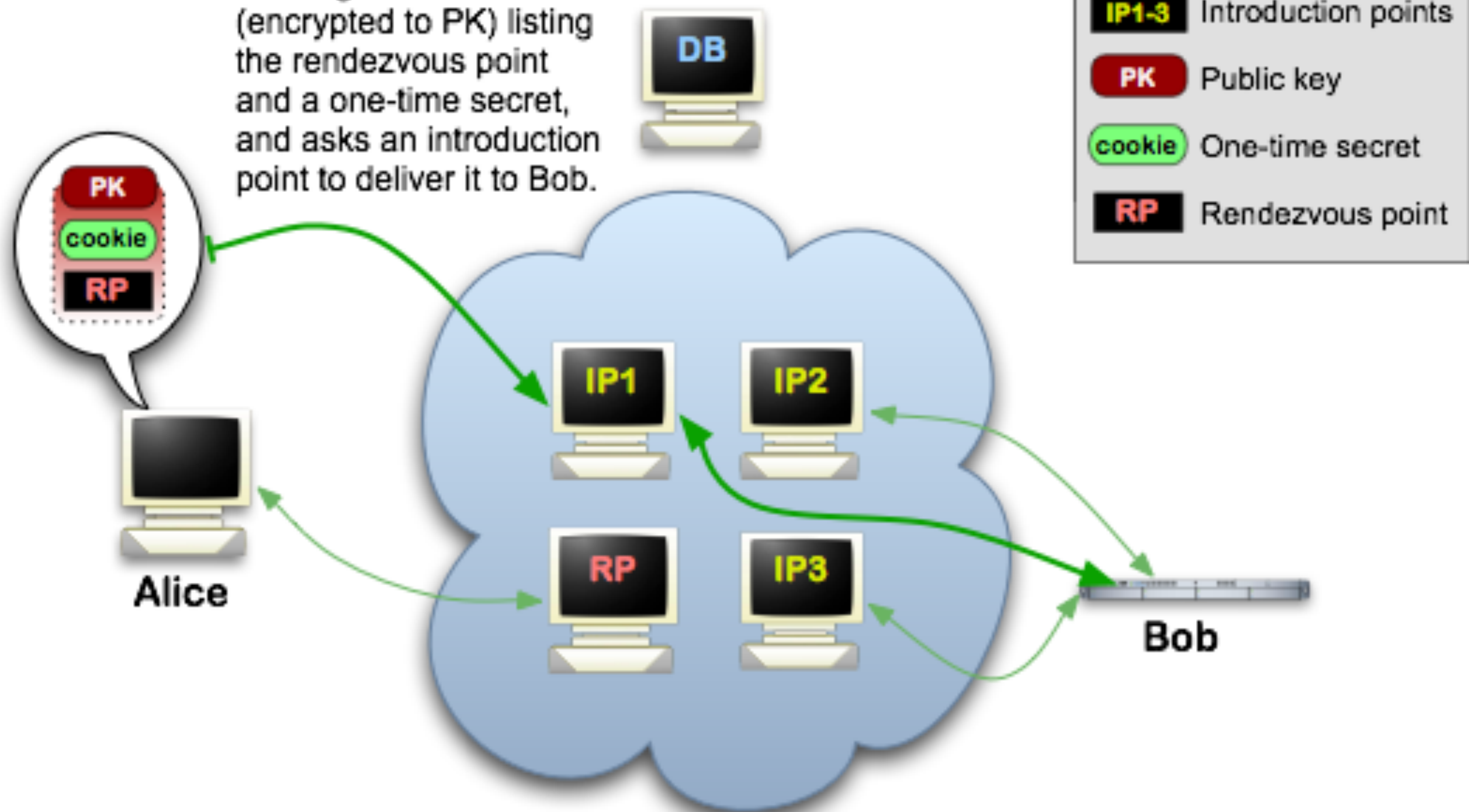
RP Rendezvous point



Bob

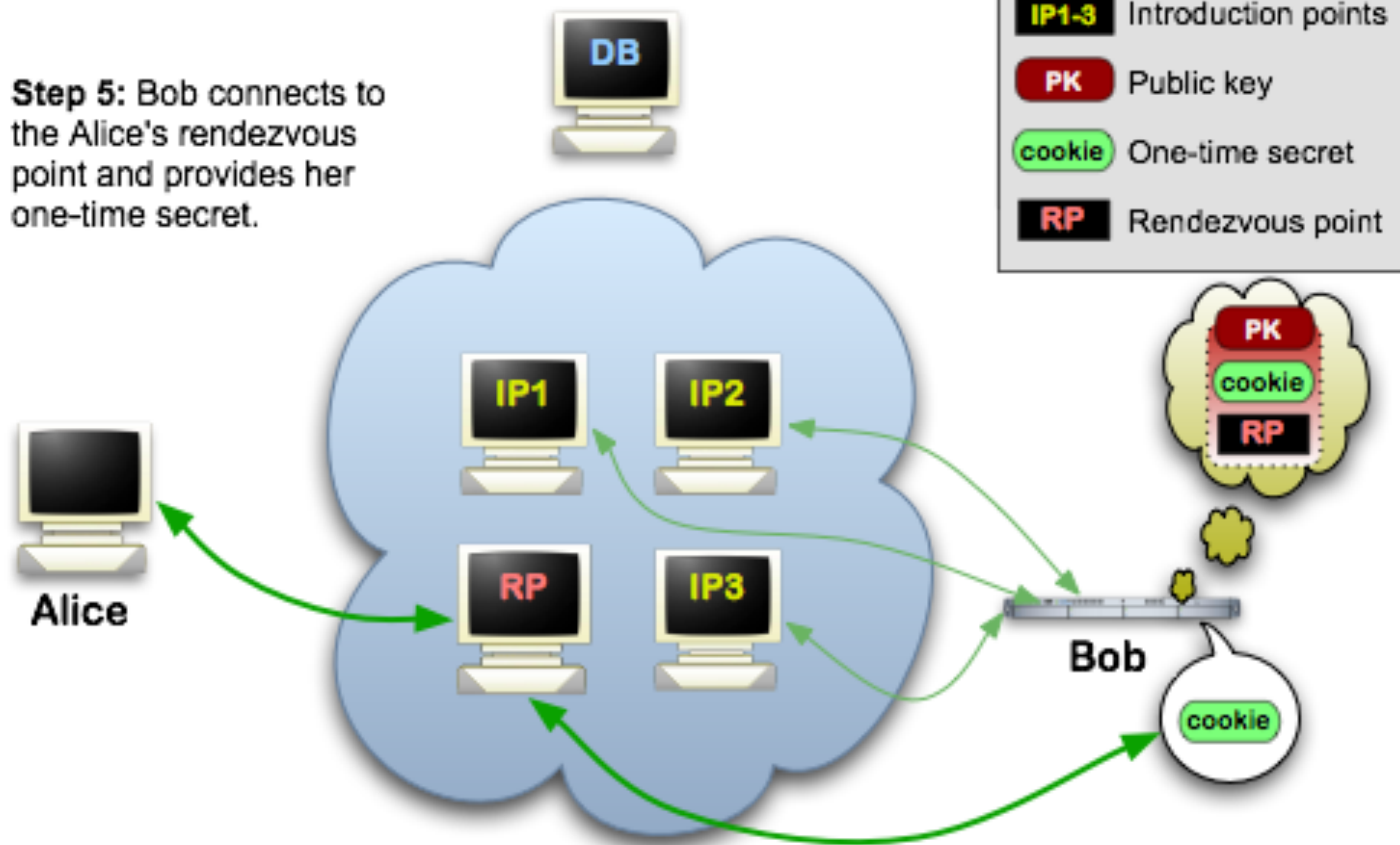
Tor Hidden Services: 4

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

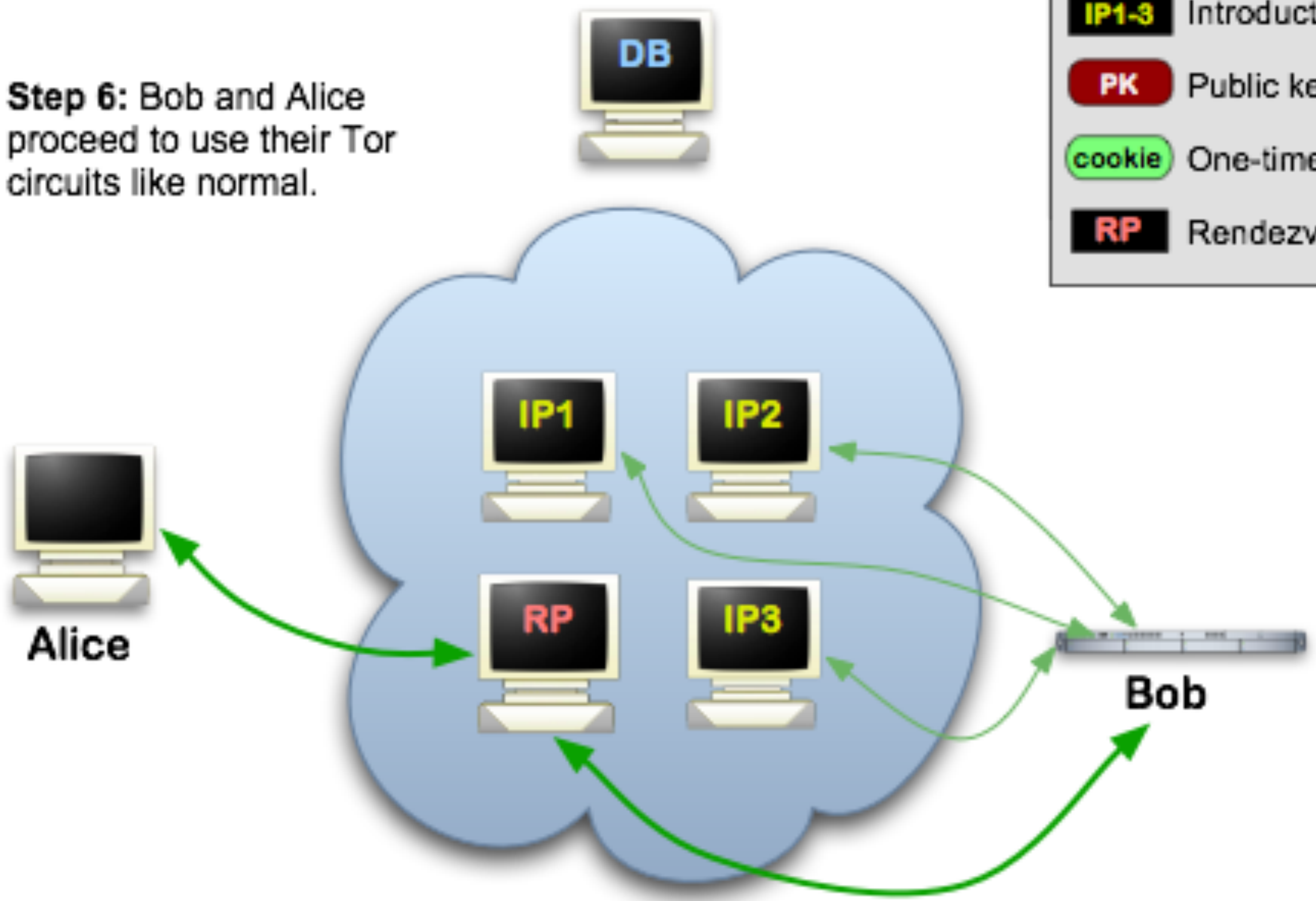
Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.



Tor Hidden Services: 6

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

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



Shop by category:

- Drugs(752)
 - Cannabis(280)
 - Ecstasy(35)
 - Dissociatives(11)
 - Psychedelics(84)
 - Opioids(62)
 - Stimulants(53)
 - Other(107)
 - Benzos(70)
- Lab Supplies(6)
- Digital goods(98)
- Services(48)
- Money(55)
- Weaponry(15)
- Home & Garden(14)
- Food(4)
- Electronics(5)
- Books(49)
- Drug paraphernalia(28)
- XXX(30)
- Medical(3)
- Computer equipment(4)
- Apparel(4)
- Musical instruments(2)
- Tickets(1)
- Forgeries(13)



5 Marijuana Butter
Chocolate Chip...
฿8.53



4mg. TIZANIDINE
(zanaflex) x25
฿2.09



US customers only
Express...
฿2.79



4 x 20MG Original Lily
Cialis
฿7.85



(1g) High-grade Crystal
Meth
฿11.95



MindFood - Protect your
brain!...
฿3.69



to US 1/4 lb (qp) BC
Master Kush...
฿121.37



How to Grow Mushrooms
฿0.14



Mushroom Indoor
Growing - Easy...
฿0.29

News:

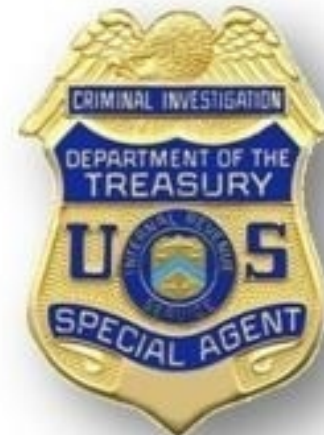
- Escrow hedging **update**
- New feature to help protect **sellers**
- We are **hiring!** Get paid for a referral, too...
- Reclaim lost coins from **MyBitcoin.com**
- Seller ranking and feedback **overhaul**
- Change your Mt. Gox **password**

Silk Road Marketplace



THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York



Who uses anonymity systems?

“If you’re not doing anything wrong, you shouldn’t have anything to hide.”

- Implies that anonymous communication is for criminals

The truth: who uses Tor?

- Journalists, Law Enforcement, Human Rights Activists, Business Executives, Intelligence/Military, Normal People

Internet Censorship

Government censors

Block websites containing “offensive” content
Commonly employ blacklist approach

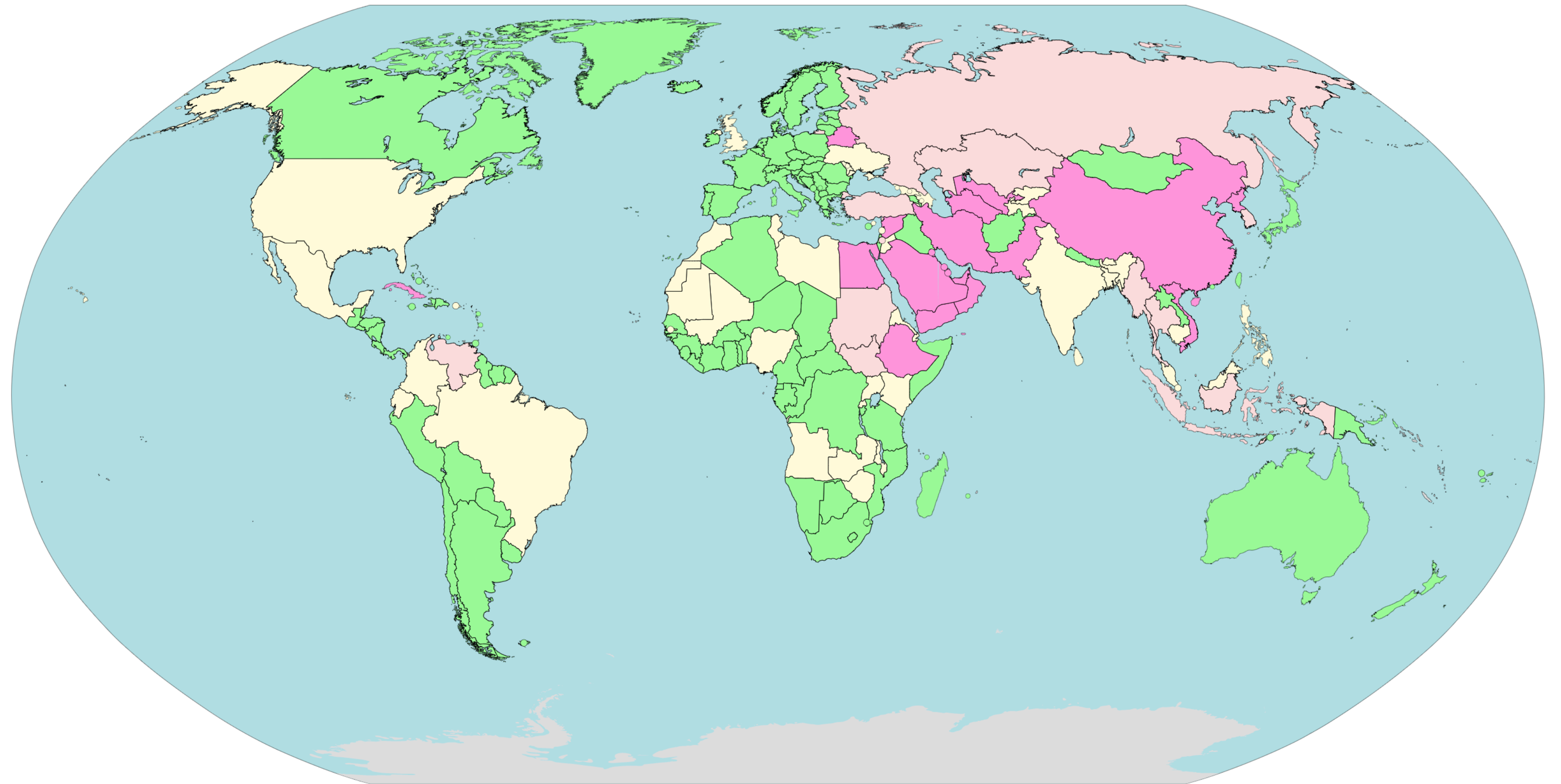
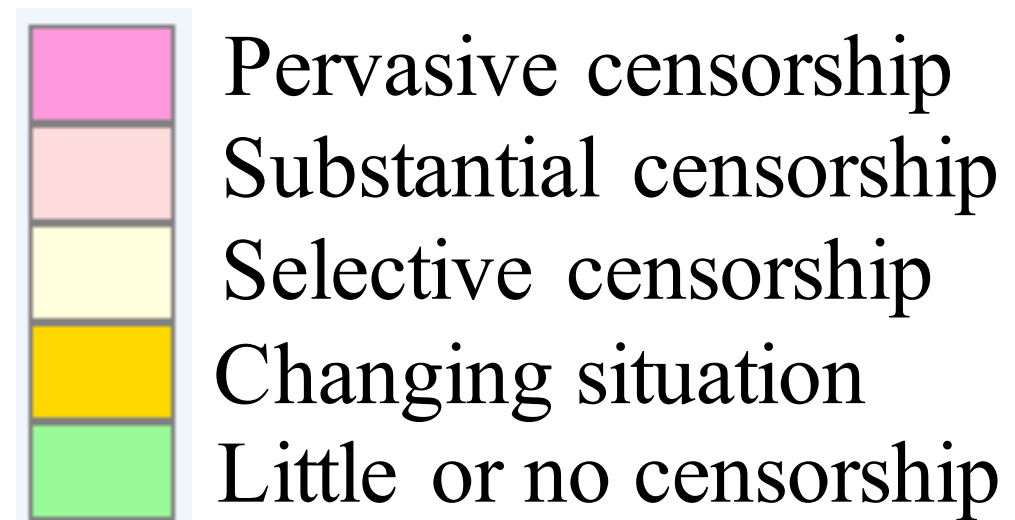
Observed techniques

IP blocking, DNS blackholes, forged RST packets

Popular countermeasures

Mostly proxy based — Tor, Freenet, Ultrasurf, ...
Problem: Cat-and-mouse game

Internet Censorship



Tor Bridges

Anyone can look up the IP addresses of Tor relays

- Public information in the consensus file

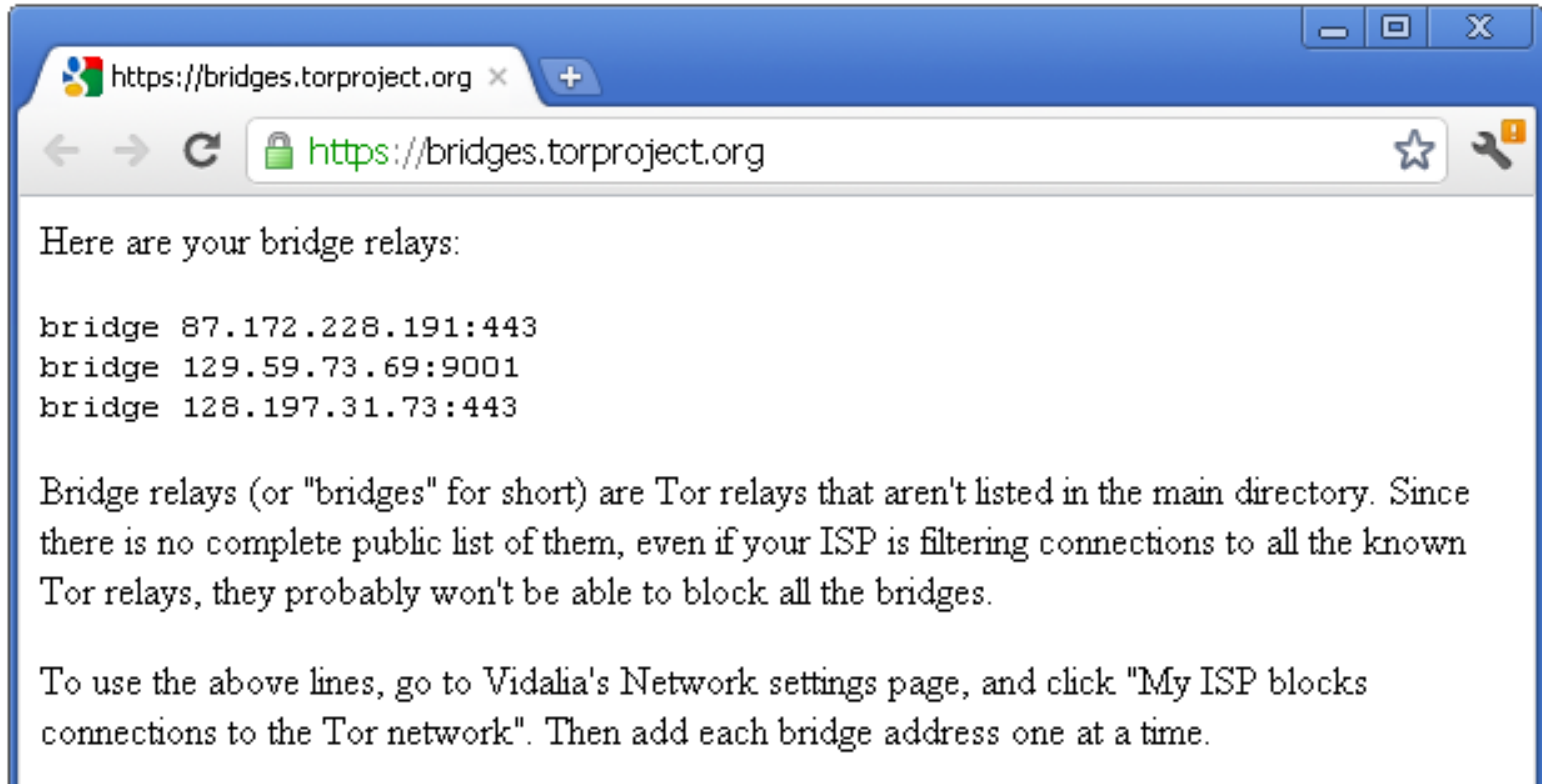
Many countries block traffic to these IPs

- Essentially a denial-of-service against Tor

Solution: Tor Bridges

- Tor proxies that are not publicly known

Tor Bridges



The image shows a screenshot of a web browser window. The address bar displays the URL `https://bridges.torproject.org`. The page content includes the heading "Here are your bridge relays:" followed by three lines of bridge addresses: `bridge 87.172.228.191:443`, `bridge 129.59.73.69:9001`, and `bridge 128.197.31.73:443`. Below this, there is a paragraph explaining that bridge relays are Tor relays not in the main directory and that they can bypass ISP filtering. A final paragraph provides instructions on how to use these addresses in Vidalia's Network settings.

Here are your bridge relays:

```
bridge 87.172.228.191:443  
bridge 129.59.73.69:9001  
bridge 128.197.31.73:443
```

Bridge relays (or "bridges" for short) are Tor relays that aren't listed in the main directory. Since there is no complete public list of them, even if your ISP is filtering connections to all the known Tor relays, they probably won't be able to block all the bridges.

To use the above lines, go to Vidalia's Network settings page, and click "My ISP blocks connections to the Tor network". Then add each bridge address one at a time.

Obfuscating Tor Traffic

Bridges alone may be insufficient to get around all types of censorship

- DPI can be used to locate and drop Tor frames

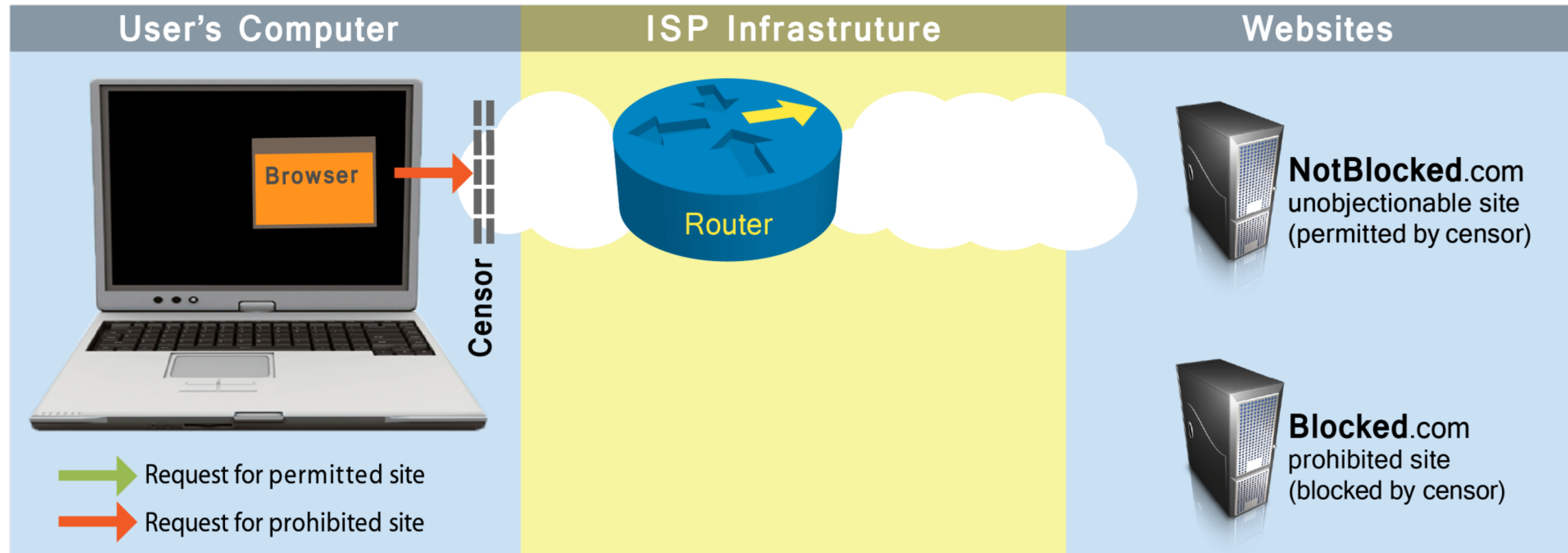
Countries would passively detect and block bridges

- Single use bridges

Tor adopts a pluggable transport design

- Tor traffic is forwarded to an obfuscation program
- Obfuscator transforms the Tor traffic to look like some other protocol
 - BitTorrent, Skype, HTTP, streaming audio, etc.

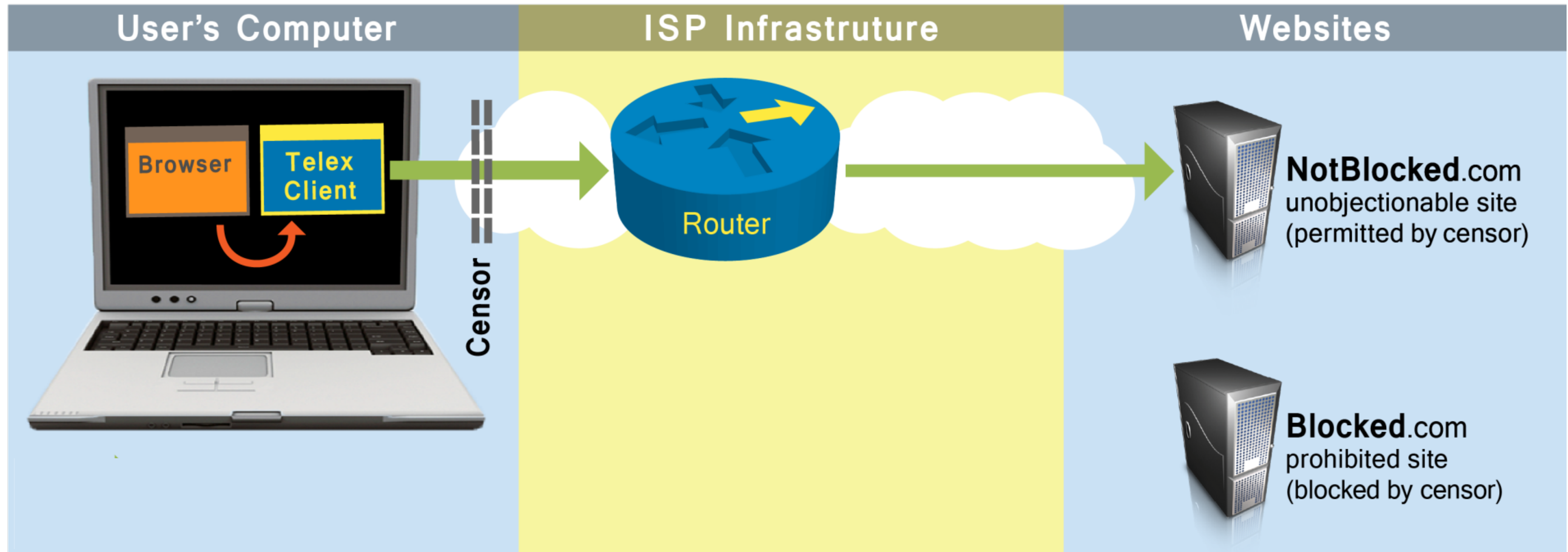
Decoy Routing (Telex)



→ Request for **permitted** site

→ Request for **prohibited** site

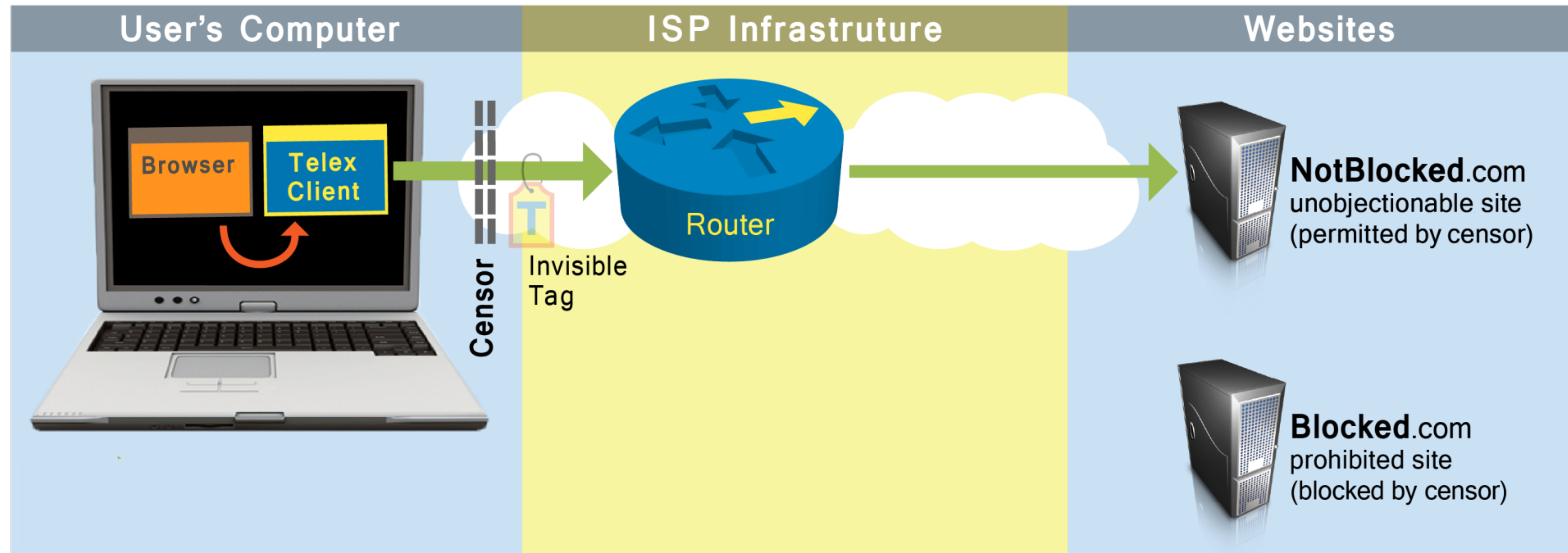
Decoy Routing (Telex)



→ Request for **permitted** site

→ Request for **prohibited** site

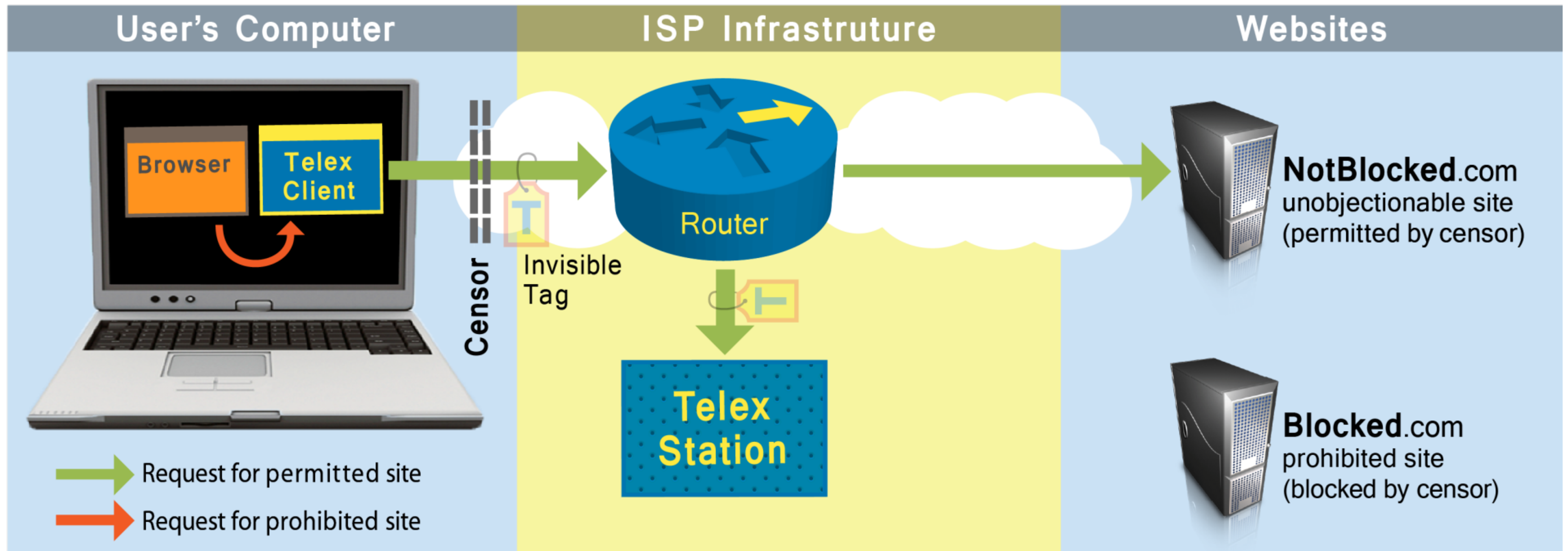
Decoy Routing (Telex)



➡ Request for **permitted** site

➡ Request for **prohibited** site

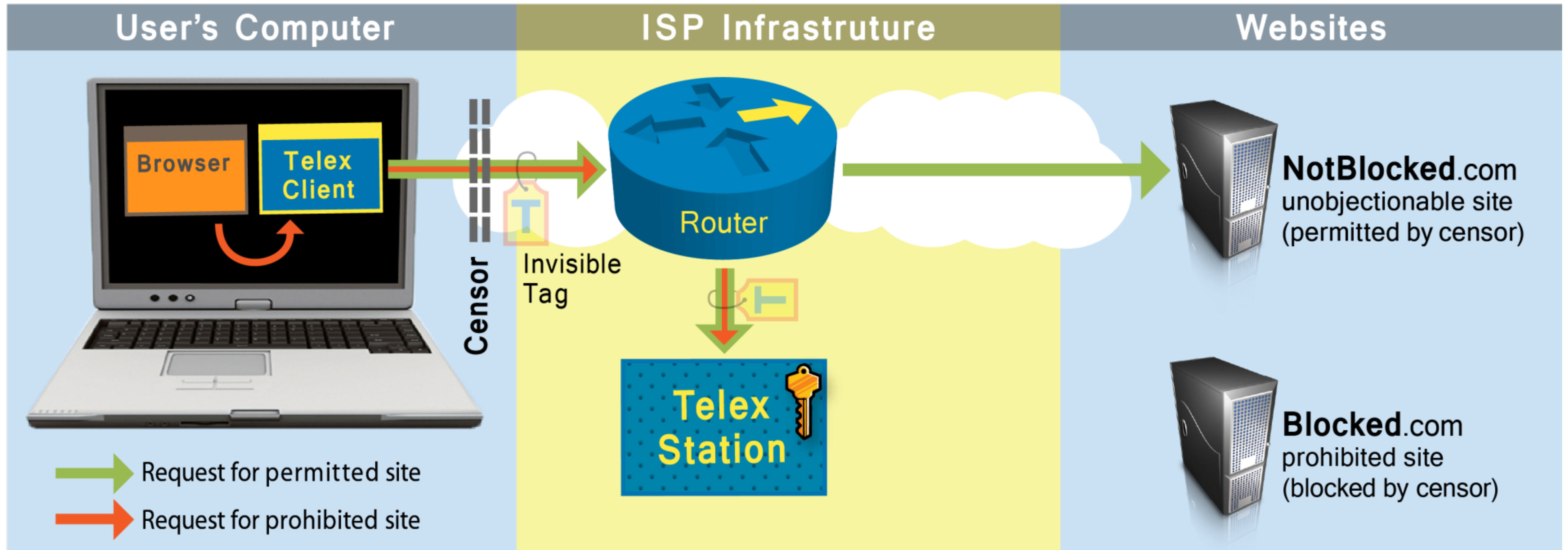
Decoy Routing (Telex)



Green arrow: Request for **permitted** site

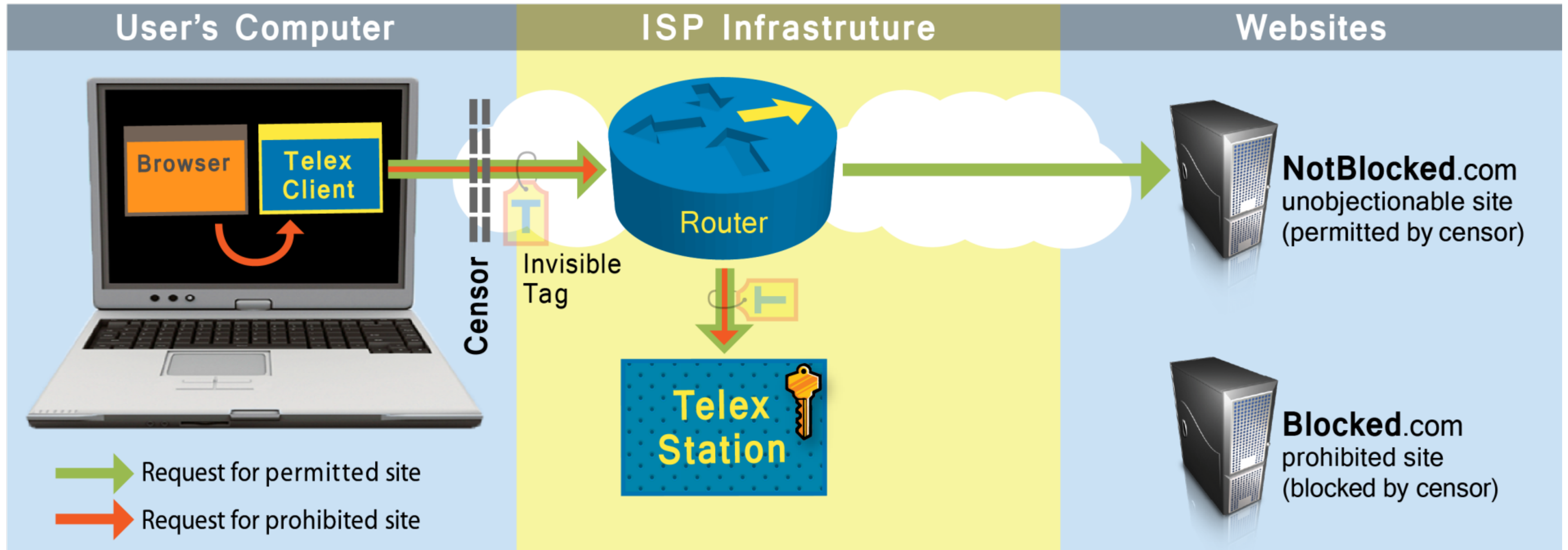
Orange arrow: Request for **prohibited** site

Decoy Routing (Telex)



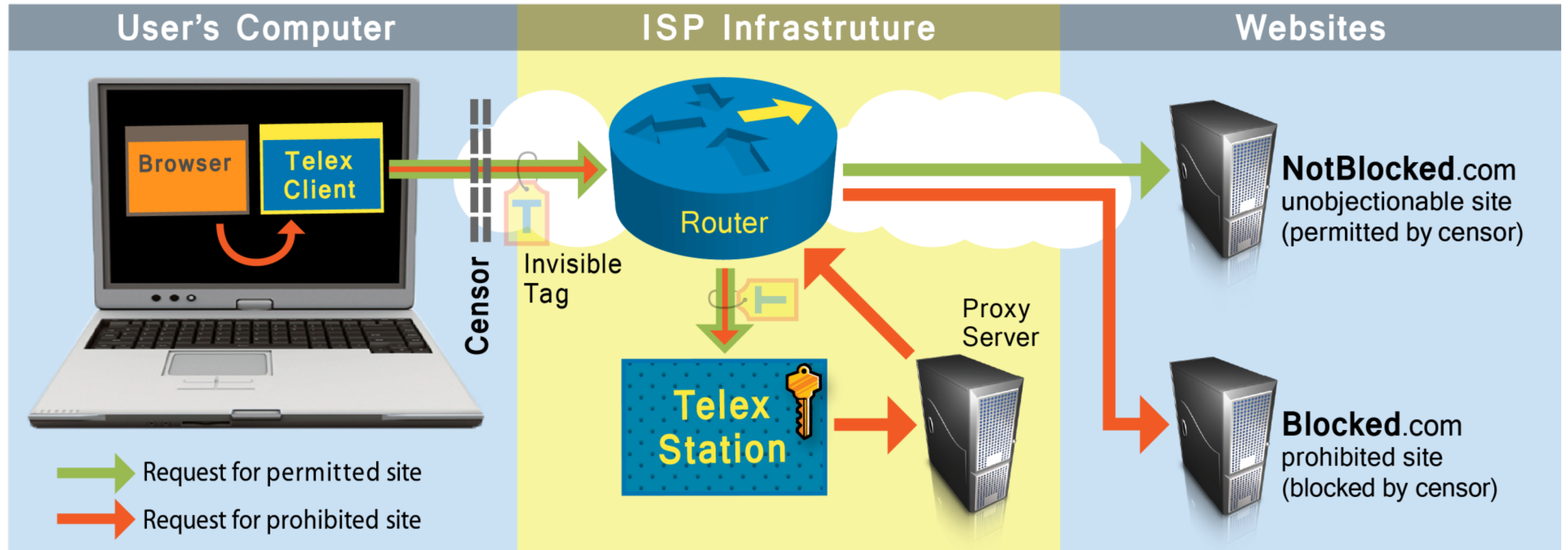
➡ Request for **permitted** site ➡ Request for **prohibited** site

Decoy Routing (Telex)



Green arrow: Request for **permitted** site Red arrow: Request for **prohibited** site

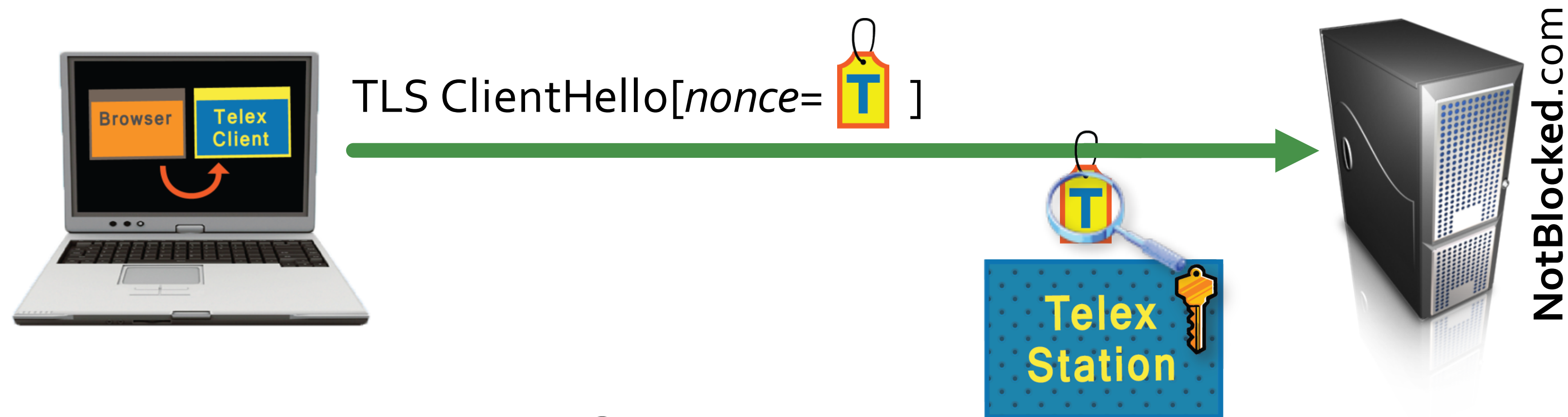
Decoy Routing (Telex)



→ Request for **permitted** site → Request for **prohibited** site

Decoy Routing (Telex)

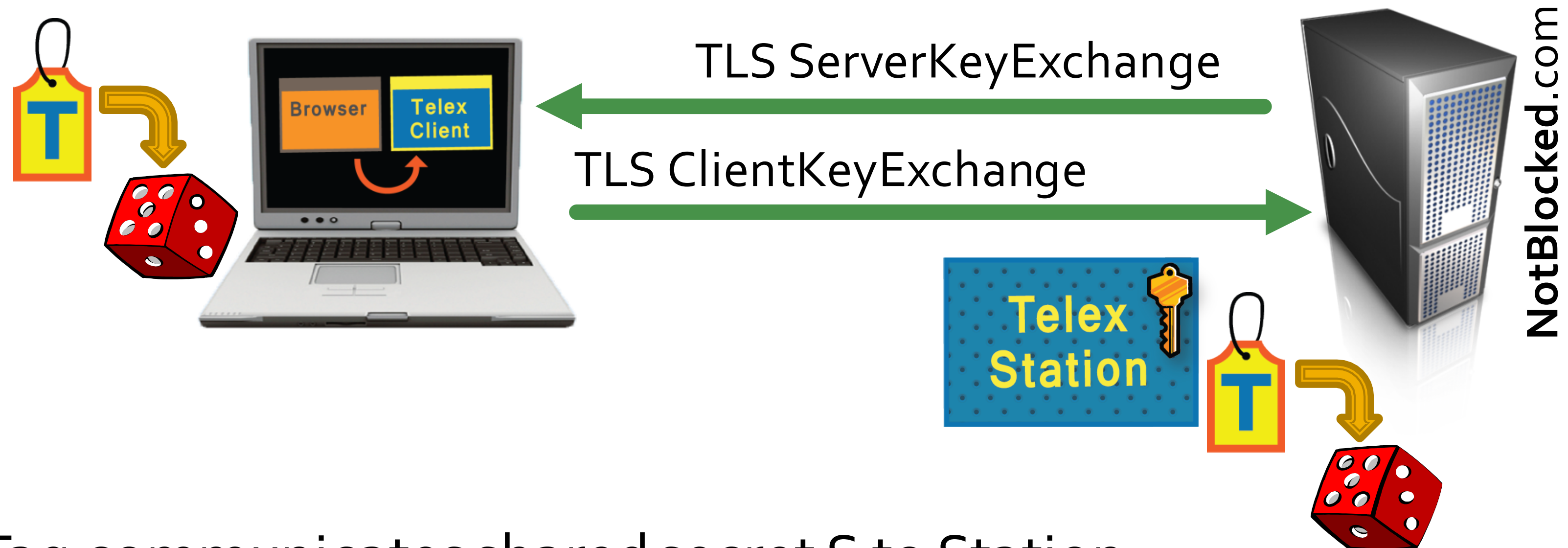
1. **Client** starts TLS connection to **NotBlocked.com**



2. **Station** recognizes **T** using private key,
but **Censor** can't tell from normal random nonce
Constructed using *public key steganography*.

Decoy Routing (Telex)

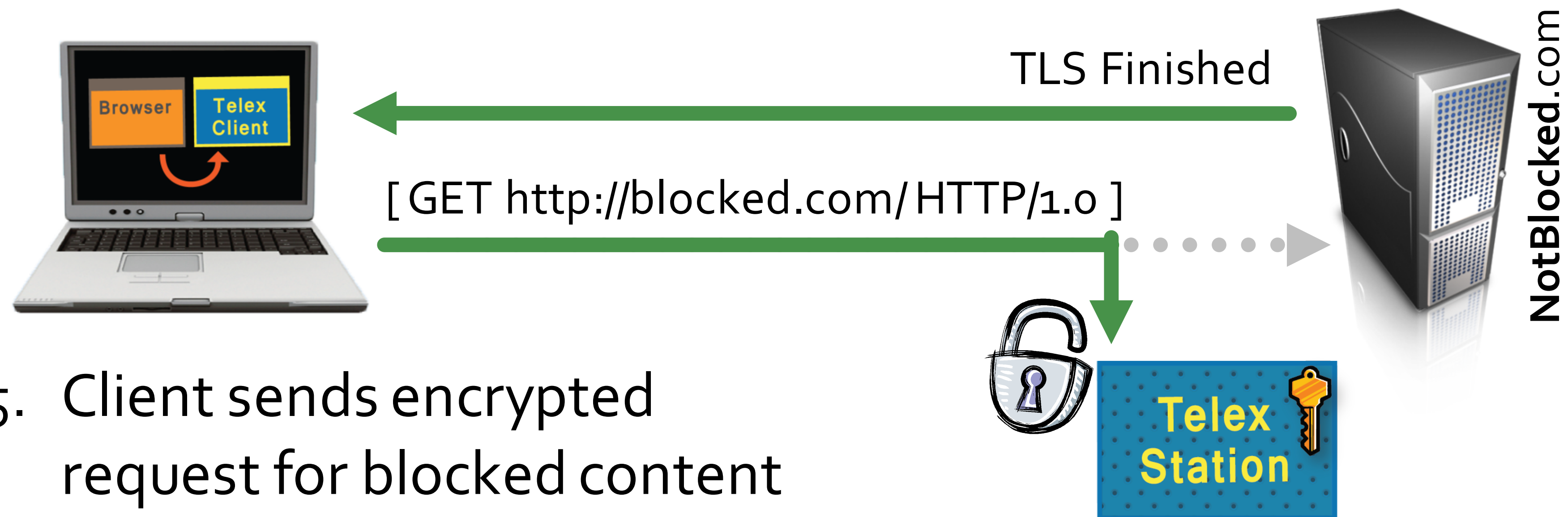
3. Client negotiates TLS session key with NotBlocked and leaks it to Station



- Tag communicates shared secret S to Station
- Client uses S in place of random coins for key generation
- Station simulates Client, derives same TLS key

Decoy Routing (Telex)

4. Station verifies Finished message from NotBlocked, switches from observer to MITM



5. Client sends encrypted request for blocked content
6. Station intercepts, decrypts, and proxies request

Email Protection

Your email provider may be required to turn over your (securely stored) email

- Warrant (for content)

Metadata

- National Security Letter (NSL), Court Order

What if you want to protect email content?

PGP

Modern implementations: GnuPG, Keybase

Each user has:

- A public encryption key, paired with a private decryption key
- A private signature key, paired with a public verification key

How does sending/receiving work?

How do you find out someone's public key?

PGP Operations

To send a message:

Sign with your signature key

Encrypt message and signature with recipient's public encryption key

To receive a message:

Decrypt with your private key to get message and signature

Use sender's public verification key to check sig

PGP Public Keys

How do you obtain Bob's public key?

Get it from Bob's website? (🙄)

Get it from Bob's website, verify using out-of-band communication

Keys are unwieldy **fingerprints**

A fingerprint is a cryptographic hash of a key

What if you don't personally know Bob?

Web of Trust (WoT)

Social Network (Keybase)

Lost PGP Key

What if Bob's machine compromised?

His key material becomes known

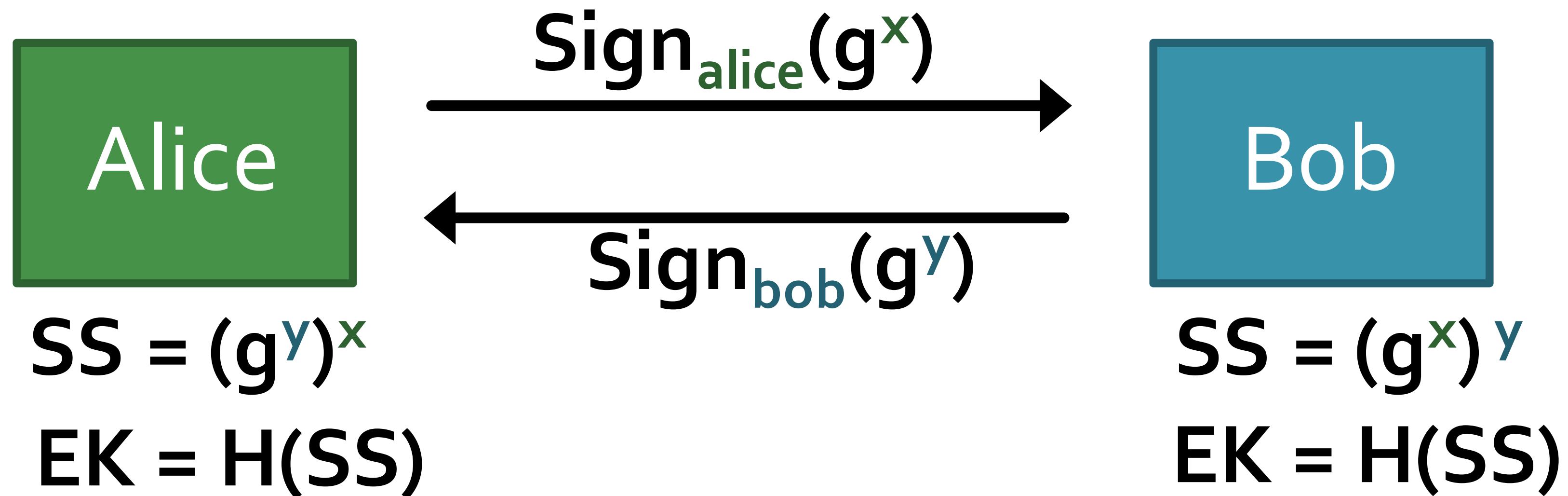
Past messages can be decrypted and read

You also have **sender's signature** on messages sent, so you can prove identity of sender

Sender must trust recipient's ability/desire to keep her statements private

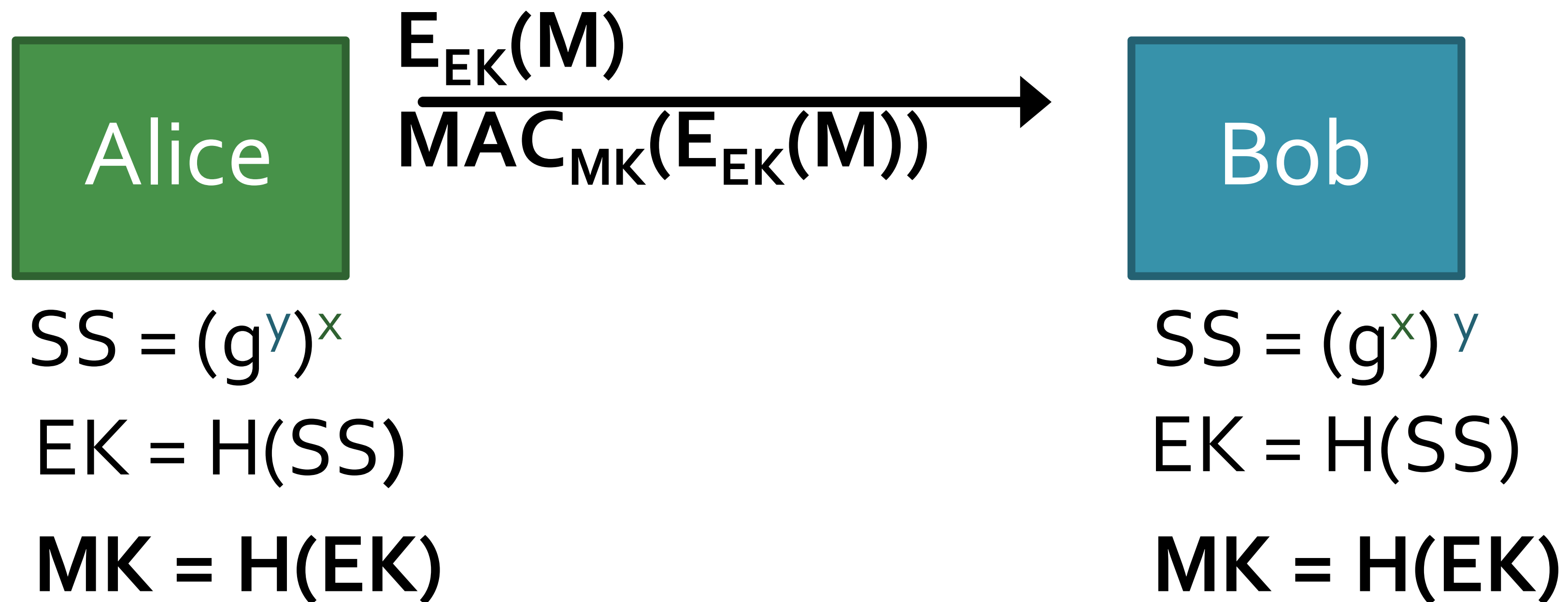
OTR: Off the Record Chat

1. Use authenticated Diffie-Hellman to establish a (short-lived) **session key EK**



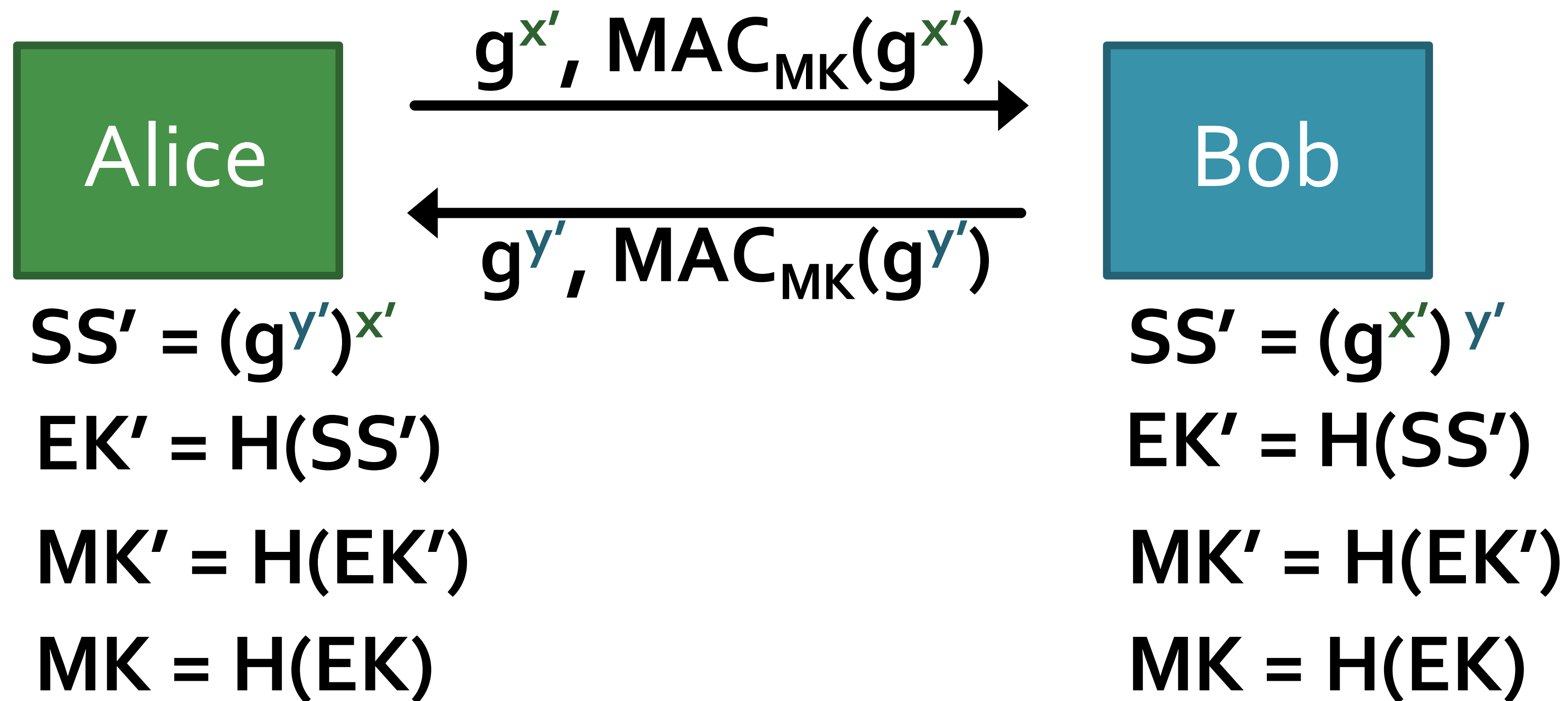
OTR: Off the Record Chat

2. Then use symmetric encryption on message M ... and authenticate using a MAC



OTR: Off the Record Chat

3. Re-key using Diffie-Hellman



OTR: Off the Record Chat

4. Publish old MK

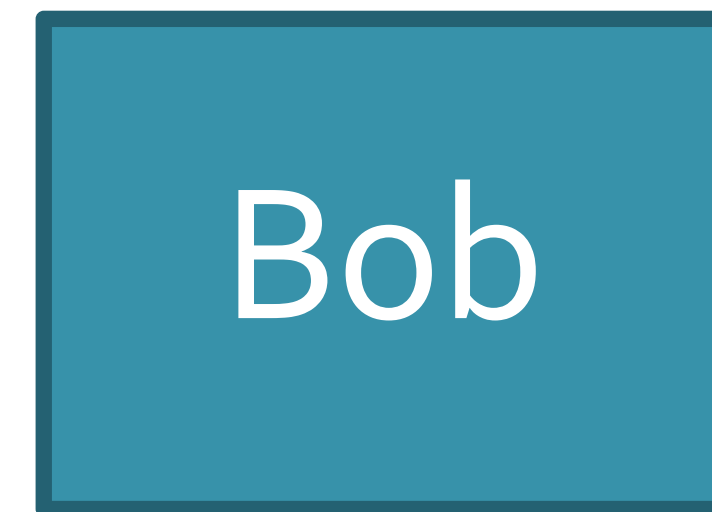


$$SS' = (g^{y'})^{x'}$$

$$EK' = H(SS')$$

$$MK' = H(EK')$$

~~$$MK = H(EK)$$~~



$$SS' = (g^{x'})^{y'}$$

$$EK' = H(SS')$$

$$MK' = H(EK')$$

~~$$MK = H(EK)$$~~

"Deniability"

Signal/Whatsapp

Note this is suited to interactive communication, not so much email.

But, OTR provides

- message confidentiality
- authentication
- perfect forward secrecy
- deniability

OTR has since lost popularity. Signal Protocol now de facto standard.