The Snoopers Charter
and what you can do about it

What is privacy?

Personal Information

- Name
- Address
- Email
- Username
- Payment information

Personal Information

- **IP address**
- **Communications data**
- Location
- MAC address
- Cookies
- Digital fingerprint

Why should we care?

Identity Theft

We don’t want everyone to know

Can be used against us

Snoopers Charter

Investigatory Powers Bill

Investigatory Powers Act 2016

- “Communication service providers”
- Anyone handling the users data

Investigatory Powers Act 2016

- “Communication service providers” legally obligated to:
  - Collect metadata
  - Assist with investigations
  - Never tell anyone about any request
  - Keep the data for 12 months

Investigatory Powers Act 2016

- Police power increased
  - Read your internet records
  - Hack into your computer/devices
- Prevent information about MP’s, journalists, lawyers and doctors being kept

Log Access

- Police
- MOD
- GCHQ
- Intelligence Services
- Home Office
- HMRC
- Department of Transport
- Department of Work & Pensions
- NHS Trusts & Foundations
- Competition and markets authority
- Financial Conduct Authority
- Food standards
- Gambling commission
- Health and safety executive
- Fire & Rescue services
- Ambulance services

The Five Eyes

- United Kingdom
- United States
- Australia
- Canada
- New Zealand

Nine Eyes

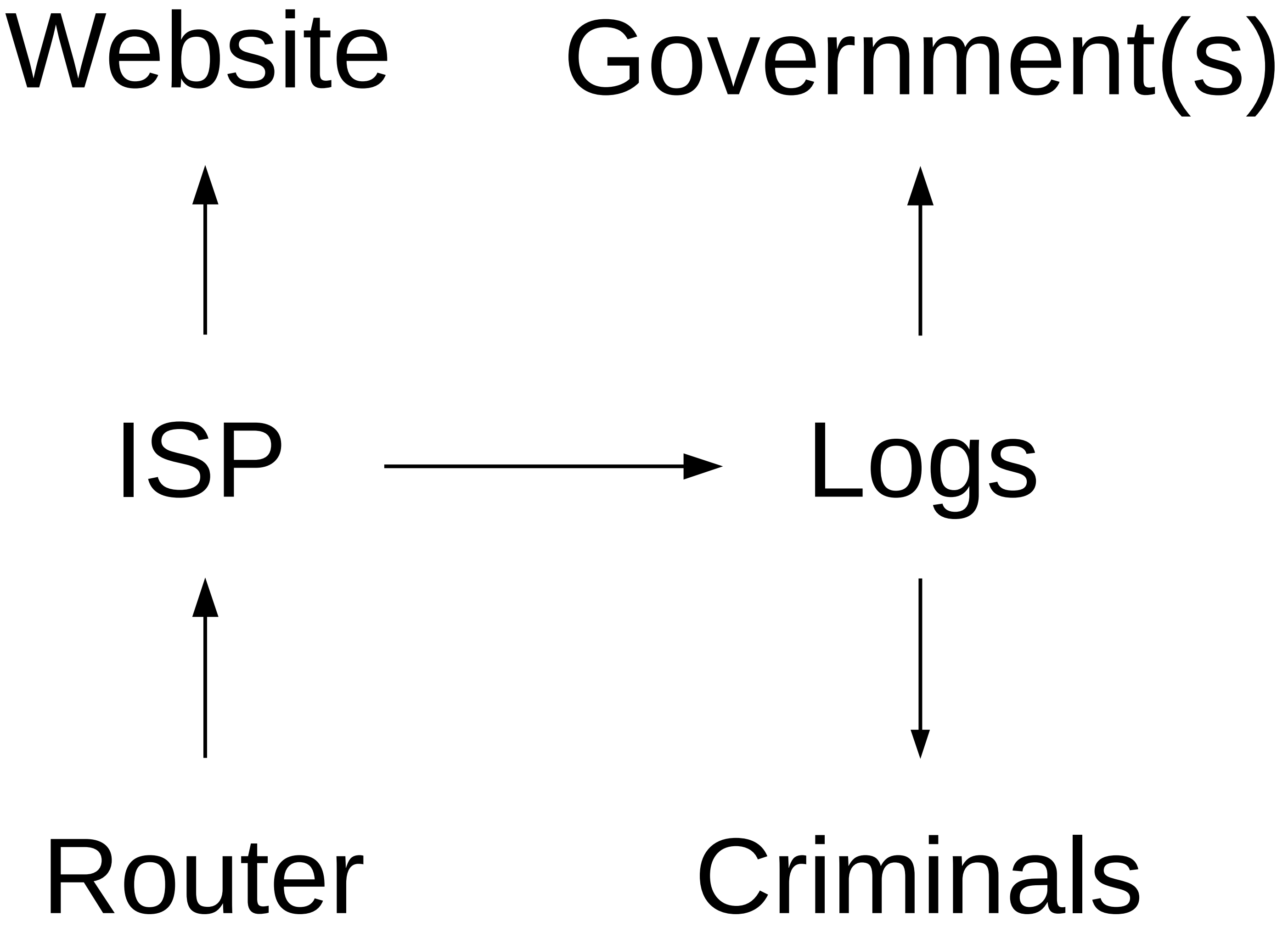
- Five eyes
  - United Kingdom
  - United States
  - Australia
  - Canada
  - New Zealand
- Denmark
- France
- Netherlands
- Norway

Fourteen Eyes

- Nine eyes
  - United Kingdom
  - United States
  - Australia
  - Canada
  - New Zealand
  - Denmark
  - France
  - Netherlands
  - Norway

- Belgium
- Germany
- Italy
- Spain
- Sweden

Issues with keeping logs



Website

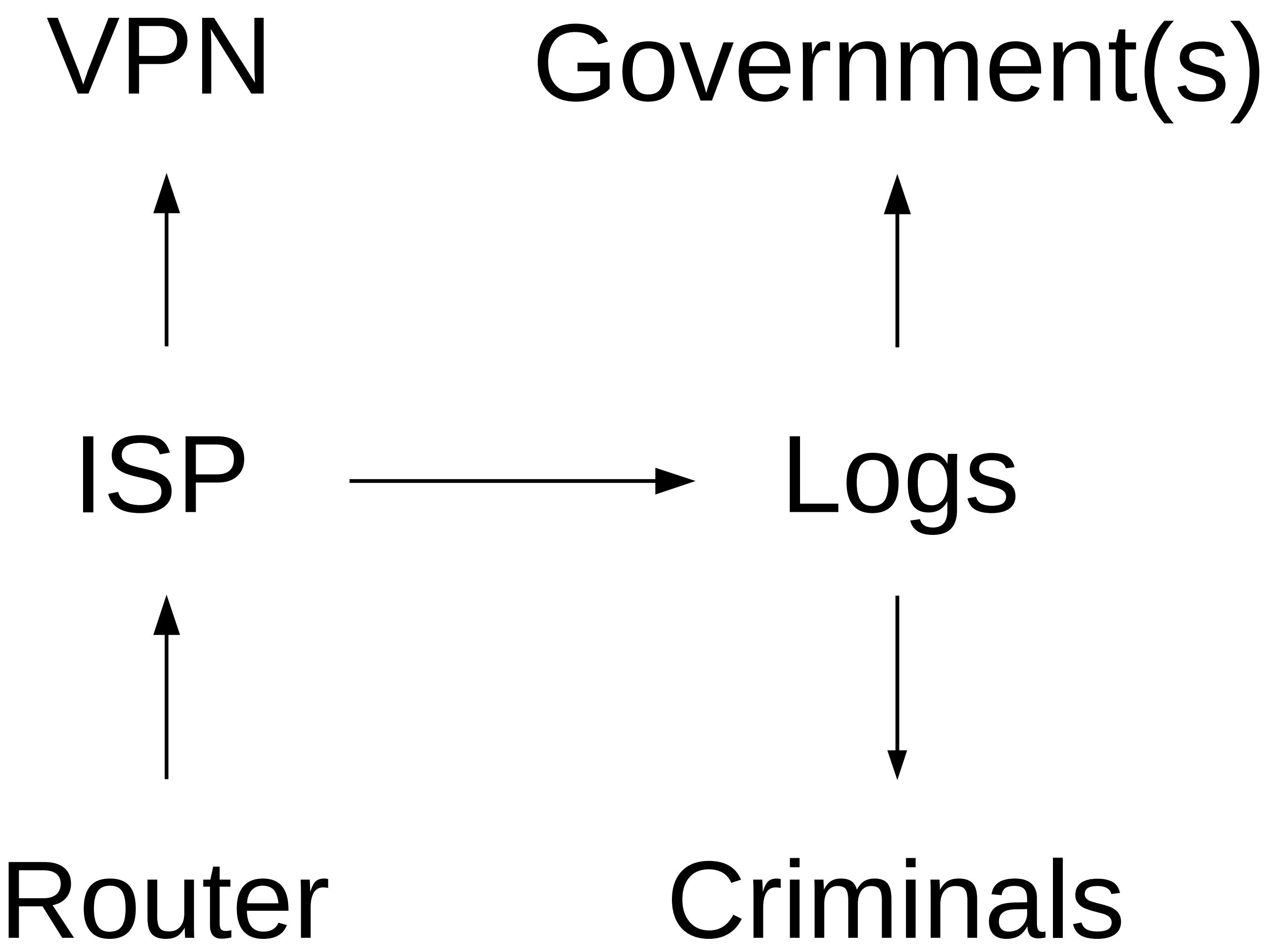
Government(s)

ISP

Logs

Router

Criminals



VPN

Government(s)

ISP

Logs

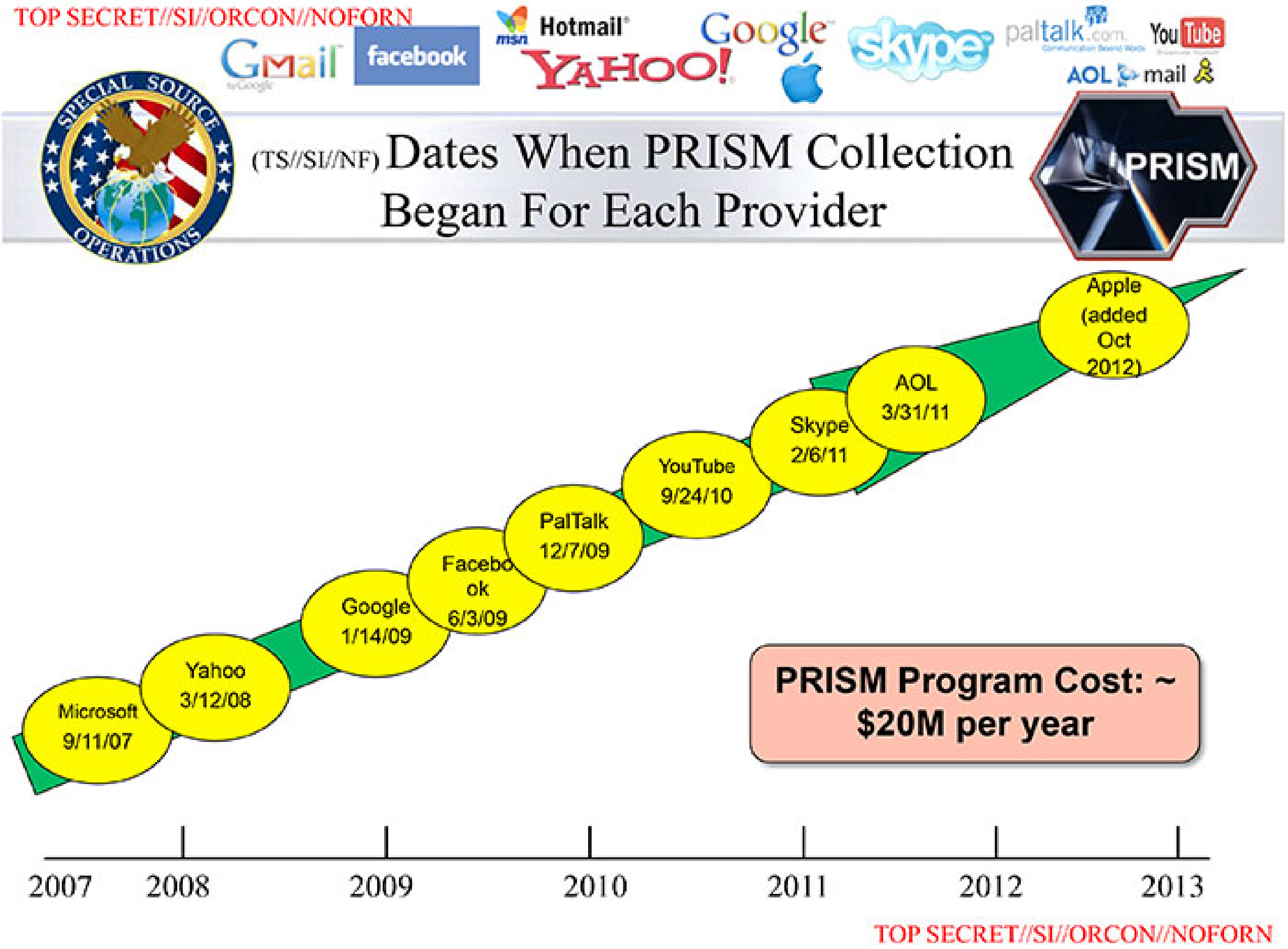
Router

Criminals

Options

- As is
- Proxies
- Virtual Private Networks
- TOR

Consider your threat model



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

Microsoft 9/11/07

Yahoo 3/12/08

Google 1/14/09

Facebook 6/3/09

PalTalk 12/7/09

YouTube 9/24/10

Skype 2/6/11

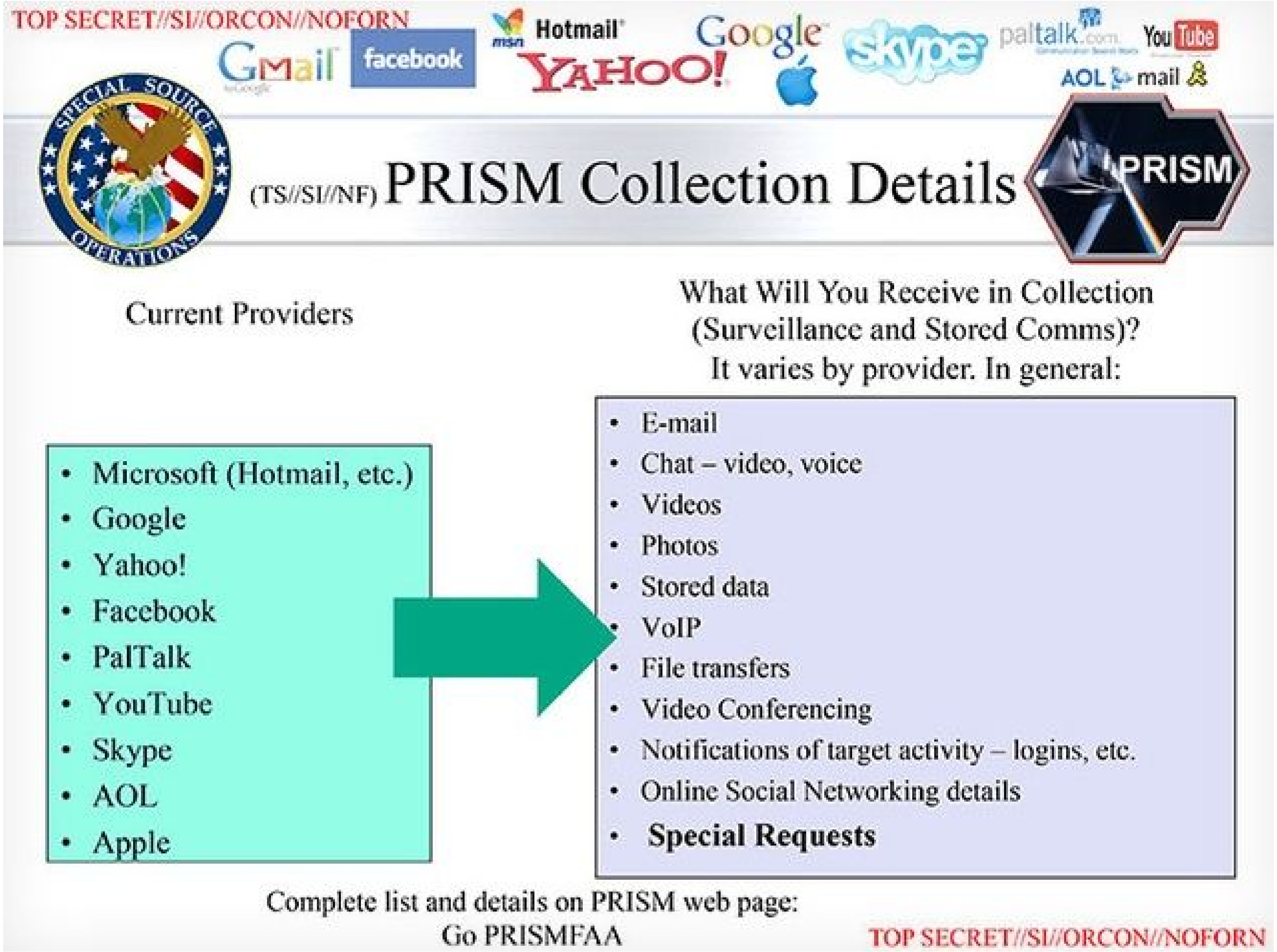
AOL 3/31/11

Apple (added Oct 2012)

PRISM Program Cost: ~ $20M per year

TOP SECRET//SI//ORCON//NOFORN

speakerdeck.com/jamiecruwys/snoopers-charter



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

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection
(Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

speakerdeck.com/jamiecruwys/snoopers-charter

Benefits of a VPN

- ISP can only log your connection to the VPN
- Prevents snooping the traffic in transit
- Masks IP address
- Bypasses network filters

Issues

- DNS leaks
- WebRTC flaw
- Unencrypted traffic from the VPN
- Latency / Speed
- Websites block access via VPN
  - Netflix
  - PayPal

Choosing a VPN

- Company incorporated location
- VPN server locations & laws
- Logging policies
- TOR / BitTorrent policies
- Kill switch functionality
- Payment methods
- Clients
- Control over servers

Roll your own?

- Streisand
  - https://github.com/jlund/streisand
- Algo
  - https://github.com/trailofbits/algo

VPN Protocols

- PPTP
- L2TP
- OpenVPN
- SSTP
- IKEv2

Point-to-Point Tunnelling Profile

- Created by a consortium funded by Microsoft
- Previously been hacked in 2 days
- Known to be insecure
- Microsoft now recommend you use L2TP/IPSec

Layer 2 Transport Protocol

- Provides no encryption or confidentiality on its own
- Usually paired with IPSec for tunnelling and encryption
- Known as L2TP/IPsec
- May require port forwarding
- Faster than OpenVPN
- Possibly compromised/weakened by the NSA

OpenVPN

- Uses OpenSSL / SSLv3 / TLSv1
- Very configurable
- Can be made to look like normal HTTPS/SSL traffic
- Slower than using L2TP/IPSec
- More secure (especially with Perfect Forward Secrecy)
- Needs 3rd party software

Secure Socket Tunnelling Protocol

- Propriety standard owned by Microsoft
- Mainly used on Windows machines
- Similar advantages to OpenVPN

Internet Key Exchange v2

- Developed by Microsoft & CISCO
- At least as good as L2TP/IPsec
- Mainly used on Windows machines
- Similar advantages to OpenVPN

Actions

- Compare VPN’s
  - https://thatoneprivacysite.net/vpn-comparison-chart/
- If using a VPN
  - Check for DNS leaks
  - Disable WebRTC
- Disk encryption
- HTTPS everywhere
- PGP
- OTR
- Signal / Telegram

Sources

- Surveillance Self Defence by the EFF
  - https://ssd.eff.org/
- privacytools.io
  - https://privacytools.io
- Chris Yui’s list of organisations with access:
  - https://yiu.co.uk/blog/who-can-view-my-internet-history/
- TorrentFreak’s VPN guide
  - https://torrentfreak.com/vpn-anonymous-review-160220/

Sources

- Microsoft Advises not to use PPTP
  - https://technet.microsoft.com/library/security/2743314
- That One Privacy Guy’s Guide To Choosing The Best VPN
  - https://www.reddit.com/r/VPN/comments/4iho8e/that_one_privacy_guys_guide_to_choosing_the_best/

The Snoopers Charter and what you can do about it