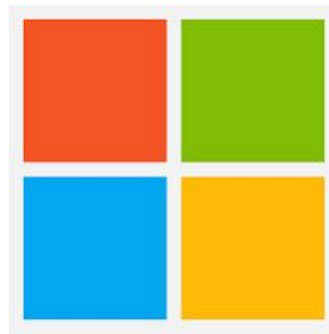




Who controls the internet?





I do not speak on
behalf of anyone,
least of all the
Dutch government.



POWERDNS 



[@bert_hu_bert](https://berthub.eu)



ITNOG EXISTS
BUT HAS NO
LOGO!





“Good Job”



Comcast, one of America's largest broadband providers, has now deployed RPKI on its network to defend against BGP route hijacks and leaks.

BGP route hijacks is a networking problem that occurs when a particular network on the internet falsely advertises that it supports certain routes or prefixes that it, in fact, does not.

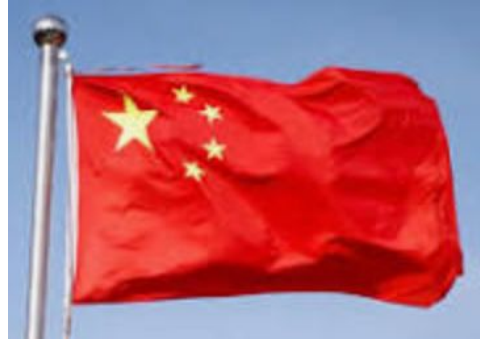
ROUTINATOR

Routinator 3000 is free, open source RPKI Relying Party software written in the Rust programming language. The application is designed to be secure and have great portability. It is a lightweight implementation that can run effortlessly on almost any operating system using minimalist hardware.

Routinator is a full-featured RPKI Relying Party software package that runs as a service which periodically downloads and verifies RPKI data. Routers can connect to Routinator to fetch verified data via the RPKI-to-Router (RTR) protocol. The built-in HTTP server offers a user interface and API endpoints for the various file formats, as well as logging, status and Prometheus metrics.



China



- Massive control (“Chinnet”)
 - But also self-sufficient
 - Parallel infrastructure, very advanced
 - Not just blocks, also “slowdowns” or errors
- China could disconnect itself from the worldwide Internet
- Willing to let certain groups have more access
 - Many Chinese companies are on Twitter, Facebook
 - Specific people also get permission somehow
 - Such freedom may come with enhanced monitoring
- **We should know _far more_ about how this works**
 - **“Cone of silence”**
- Periodically launch technical efforts to create an Internet more along their lines for the rest of the world as well
 - Many companies also work like that

Russia



- ROSKOMNADZOR
 - Federal Service for Supervision of Communications, Information Technology and Mass Media (Russian: Роскомнадзор)
- Blocked PowerDNS.COM for ages and ages
- ROSKOMNADZOR has tried real real hard to block certain services. To do so, it blocked wide swathes of AWS, Digital Ocean etc
 - Including PowerDNS
- Reportedly, this started to hurt the economy too much, so they relented
- Unlike China, Russia does not (yet?) have enough home grown capabilities to seriously cut off the internet
 - They are working on it though, including by building independent payment systems

The European Union



- Love regulation. Came up with the GDPR that we now all have to deal with
 - Unless you have a litigation budget in the billions of euros of course
- A new idea is the NIS2 directive which, in its original design, attempts to regulate the reliability and availability of all root servers
 - Even if not in the EU!
 - This idea has been removed in the EU parliament version, but.. work in progress
- Digital Markets Act / Digital Services Act
- Various European countries at times implement blocks of domain names and IP addresses, usually after a long legal struggle
- In Germany, the rights industry scans for bittorrent & other file sharing, and get court orders so ISPs must cough up user details. You then receive scary letters asking for 1000 euros.
- In general, blocking happens somewhat frequently, easier in some member states than others.
 - Not very effective



The United States of America

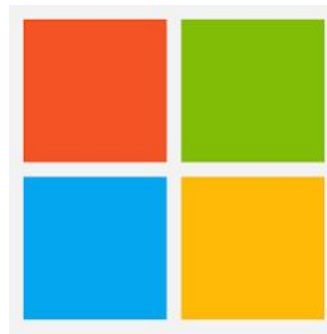
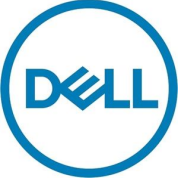


- FIRST AMENDMENT!
- And indeed, government ordered actual blocking never happens at the ISP level as far as I know
 - Well done
- So is it all good?
- US wages war on (international) content via other means:
 - DMCA
 - Exclusion from international payment systems
 - National security sanction legislation
 - **Impounding your domain name if it is in .COM, .NET or .ORG**



Turkey, Indonesia, Iran..

- It turns out that effectively blocking the internet is hard work
 - It is not easy to get technical people to work on this kind of infrastructure
 - Also expensive
- Many countries only succeed half-heartedly, perhaps by design:
 - DNS based blocks
 - Trying to block third party DNS, VPNs
 - Some IP blocking, some BGP hijacks
 - Some SNI blocking
- “Before the block in April 2017, the number of Turkish articles in Wikipedia was 289,314. By the time of the Constitutional Court's decision in January 2020, it had reached 338,882 articles”
- For a period, Internet without VPN in Iran was just too slow.

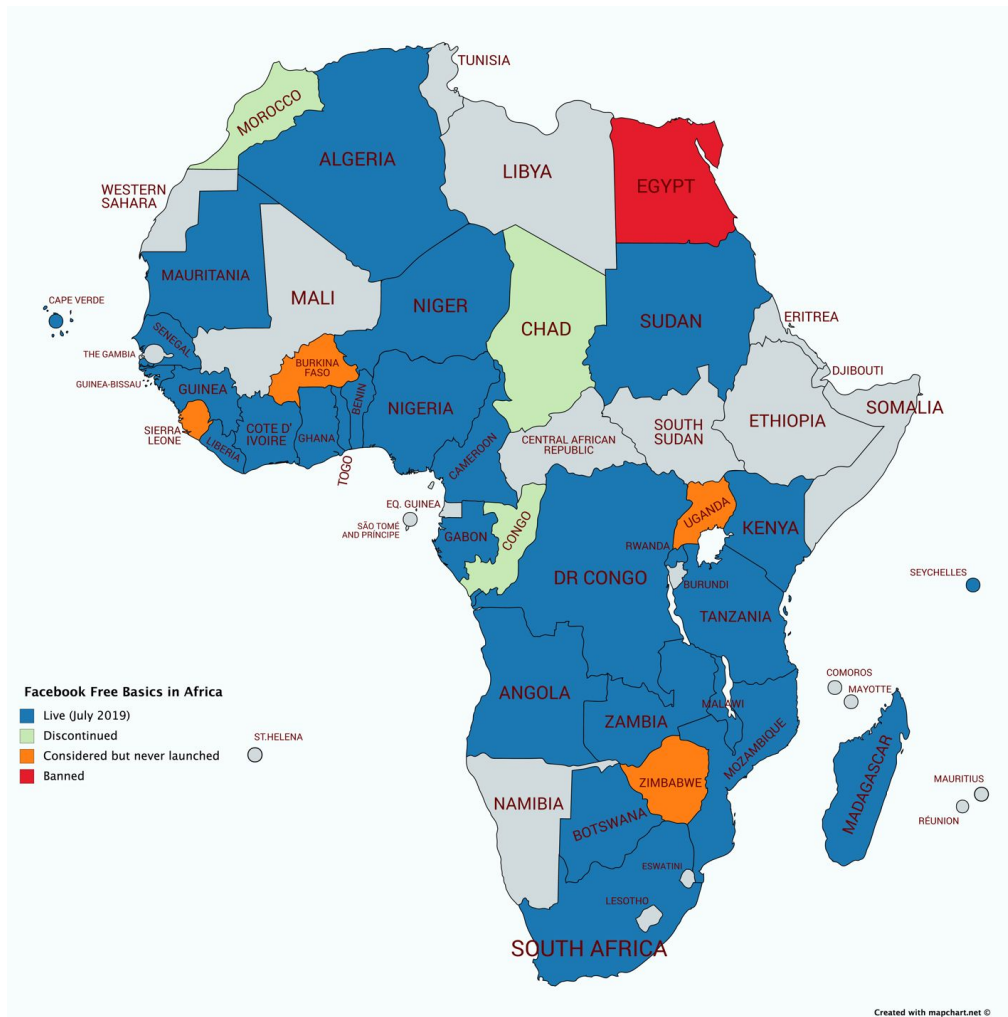


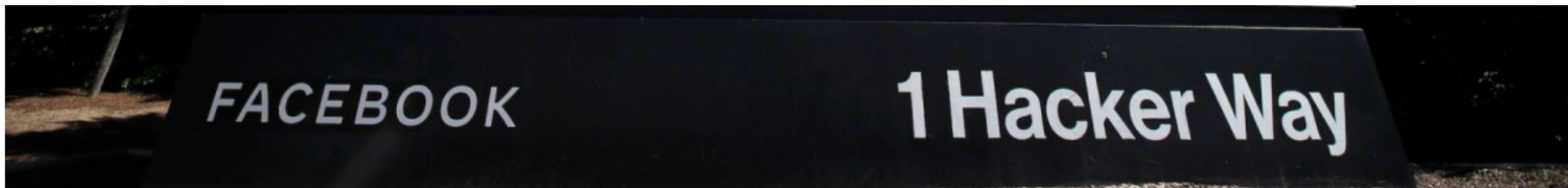


Big tech efforts

- Behind the scenes, 'big tech' effectively controls the internet
 - Spoiler
- For example:
 - I can't send email to Hotmail or KPN users
 - Email is no longer open or reliable
 - Need to pay to get out of the GMail promotions tab
 - Each and every website you visit gets checked against the Google Safe Browsing list. For all browsers.
 - Apple and Google take 30% of your revenues on their phones, plus decide if you get access at all
 - Facebook is the only internet in large parts of the world, and they kick you off randomly (or disappear you)

Facebook Basics in July 2019





AP

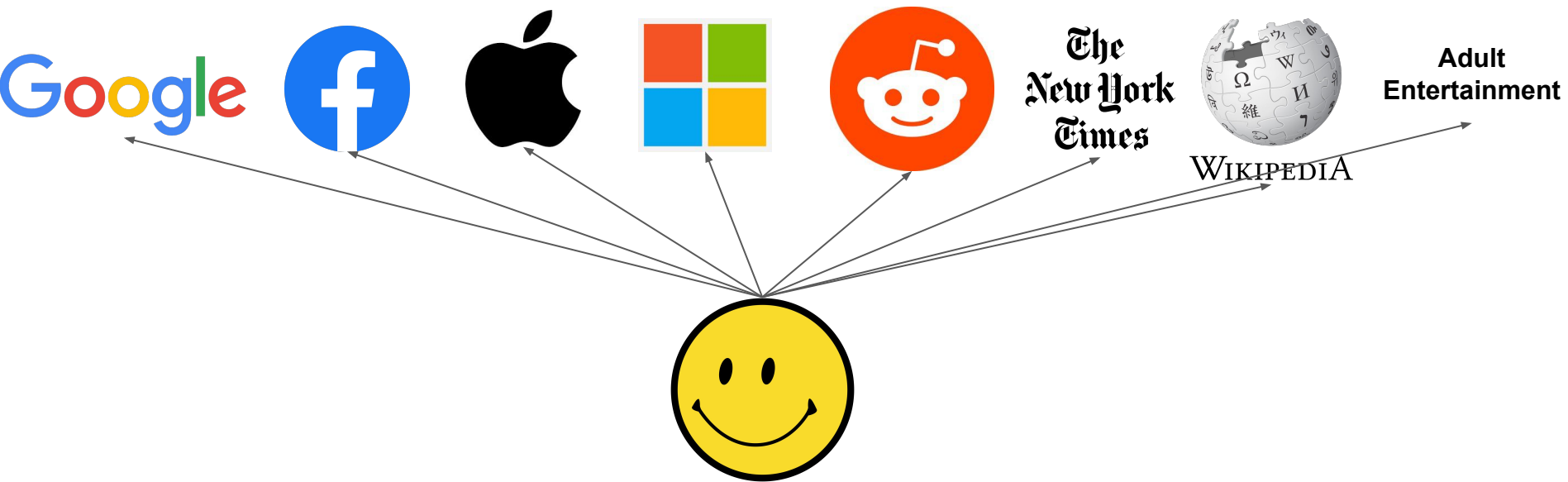
Mark Zuckerberg in 2020 bowed to demands from Vietnam's government to censor posts with anti-state language rather than risk losing an estimated \$1 billion in annual revenue from the country, *The Washington Post* reported on **Monday**.

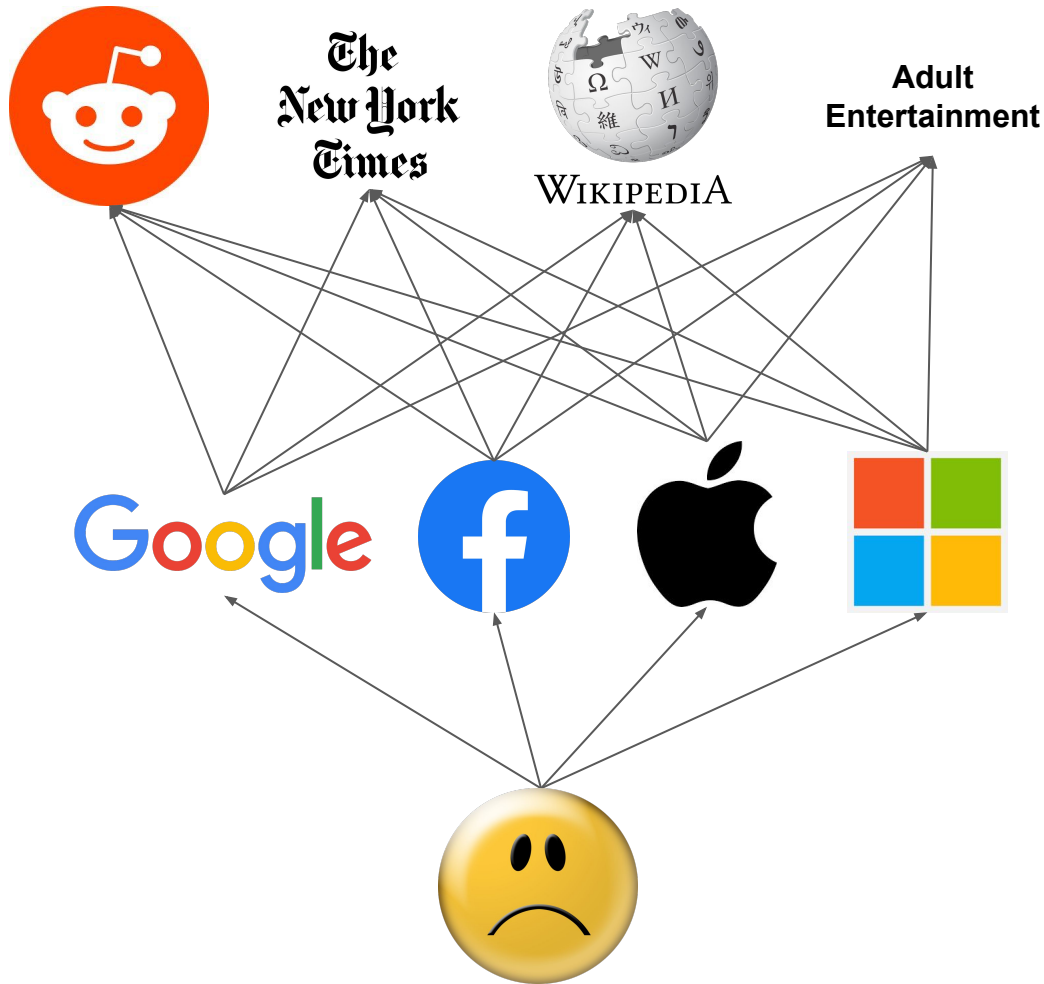
The decision to side with Vietnam's government led to a significant increase in censorship of posts in the country, according to the *Post*, which spoke with three people familiar with the decision in addition to local activists and free speech advocates. **Facebook's** own **transparency report** shows that the company more than doubled the number of posts it blocked in the country — from 834 in the first half of 2020 to more than 2,200 posts in the second half of the year.

Big tech efforts

- Google, Youtube, Facebook, Microsoft, Apple, Twitter all run private tribunals on who gets to be on the internet, send email or who gets to make money
- Much like with authoritarian governments, the choices of these tribunals:
 - Are arbitrary
 - Can't be appealed (elsewhere)
 - Do not adhere to any published procedures
 - Are often enforced without warning
 - Can be so harsh you can't even communicate with the company anymore
- Consequences are dire and far reaching
 - If "Google Safe Browsing" hates your content, you are *gone*
 - Losing access to Facebook or WhatsApp can kill a company
- **Processes are so arbitrary even senior staff can't help you**

“A kangaroo court is a court that ignores recognized standards of law or justice, carries little or no official standing in the territory within which it resides, and is typically convened ad hoc. A kangaroo court may ignore due process and come to a predetermined conclusion.” - Wikipedia





It may help your privacy, but this presentation is about who **controls** the Internet

- VPN by Google One (US only)
- (Facebook Onavo)
- **Apple Private Relay**
- Microsoft Edge Secure Network



So what will it be?



You can be important in all three places



But whatever you do, think about it.



Who controls the internet?

