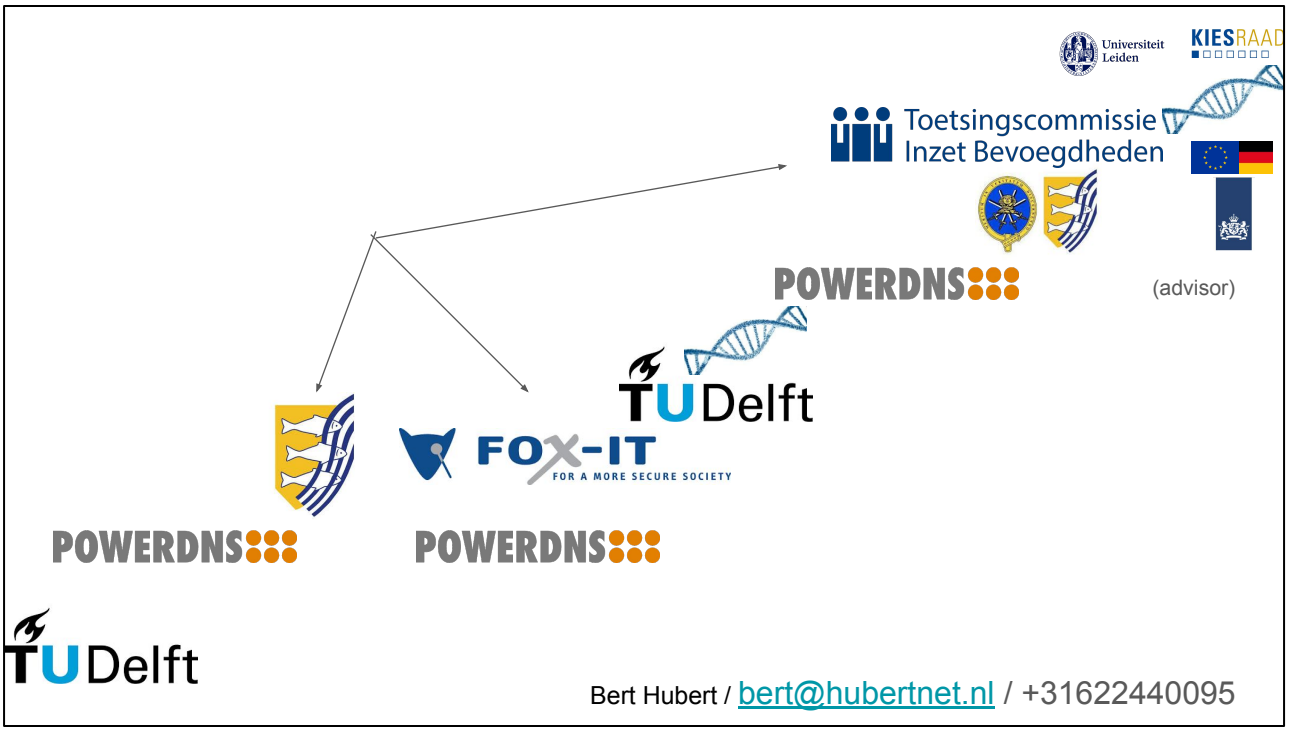
Sovereignty & global surveillance

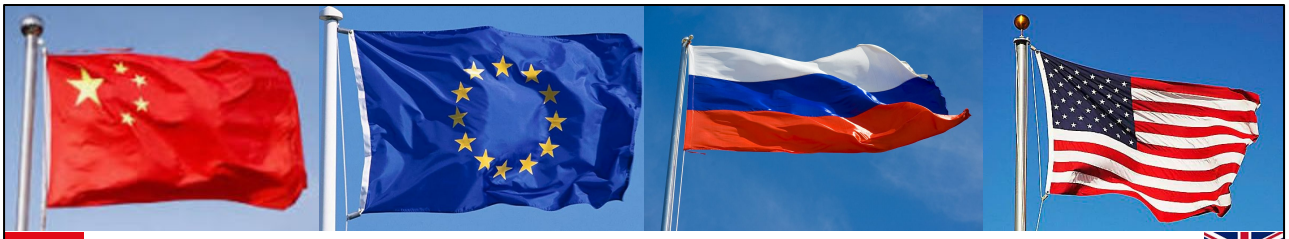
https://berthub.eu/dis



I have worked for government, been a government buyer, a government supplier and a government regulator, current advisor. But I do not speak for the Dutch government!

I was part of the panel that ruled on lawful intercept/hacking for the Dutch intelligence/security agencies.


POWERDNS
1999 - 2020
T-Mobile
kpn
AT&T
orange™
BT
TIM
LIBERTY GLOBAL
verizon
Telia
vodafone
اتصالات
etisalat
Telefónica



Who controls the internet?

RIPE

IETF

ICANN

ARIN
American Registry for Internet Numbers

APNIC

ITU

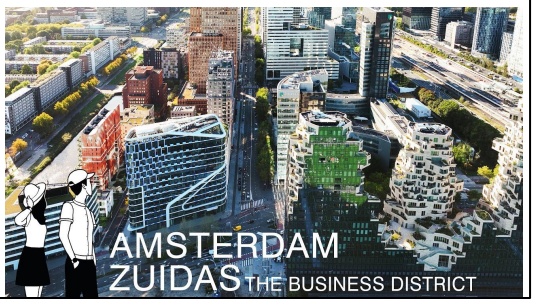
Google

Meta

Ja dit is niet best, alle clouds komen dus van buiten Europa. Tot nu toe hebben mensen wel door dat je je overheid of andere belangrijke processen niet op de Alibaba Cloud moet draaien, maar dat komt vermoedelijk niet omdat mensen nadenken over de ‘soevereiniteit’. Het lijkt erop dat Europa z’n overheden nog op Noord Koreaanse servers zou draaien als de gebruikersinterface een beetje aantrekkelijk was.

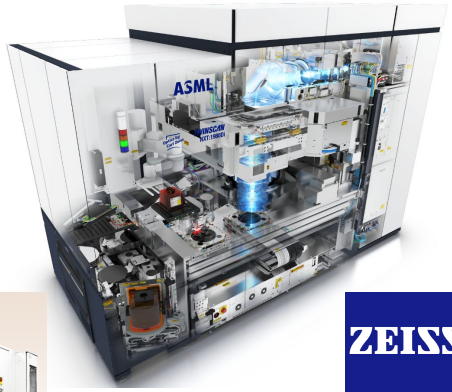
De Europese en Amerikaanse cloudproviders. Niet echt op schaal, maar het schetst een beeld. Kijk goed onder de ‘e’ van Google. OCI is Oracle

100 times smaller



At least we still have this going for us!

imec



ZEISS

TRUMPF

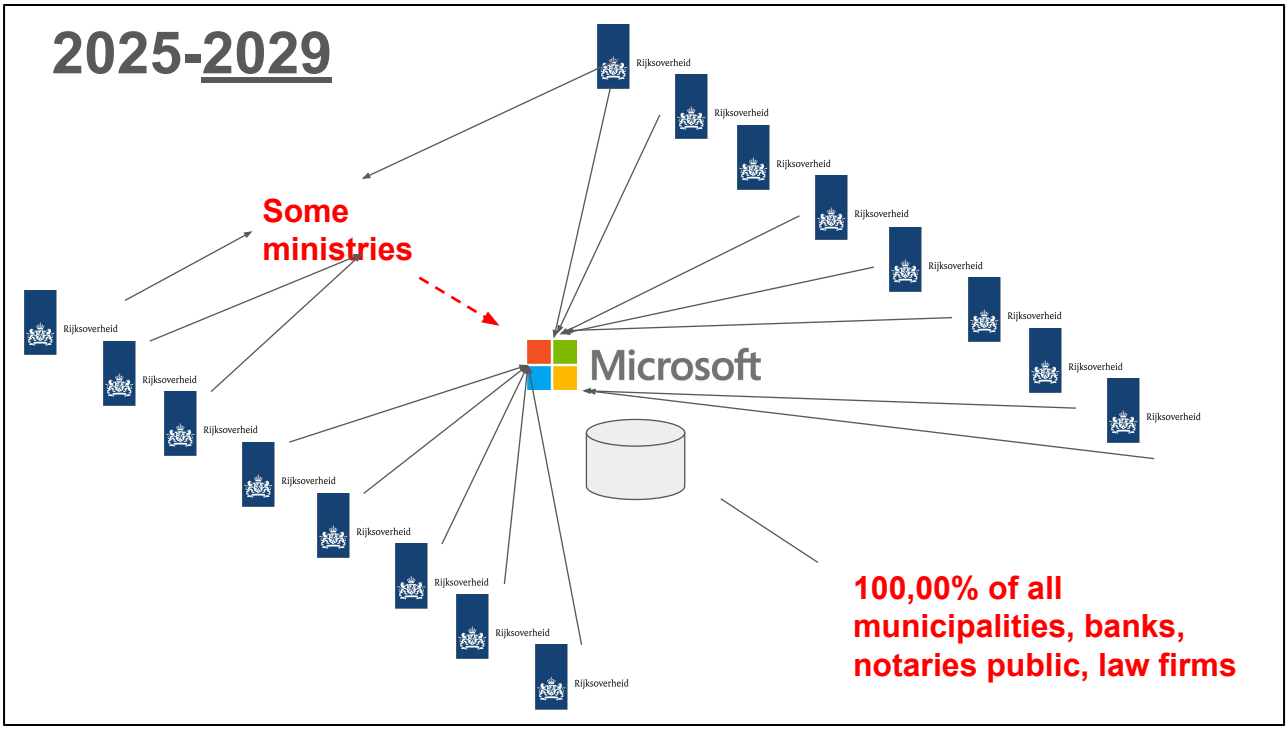
"That cloud and AI of yours come out of our machines exclusively"

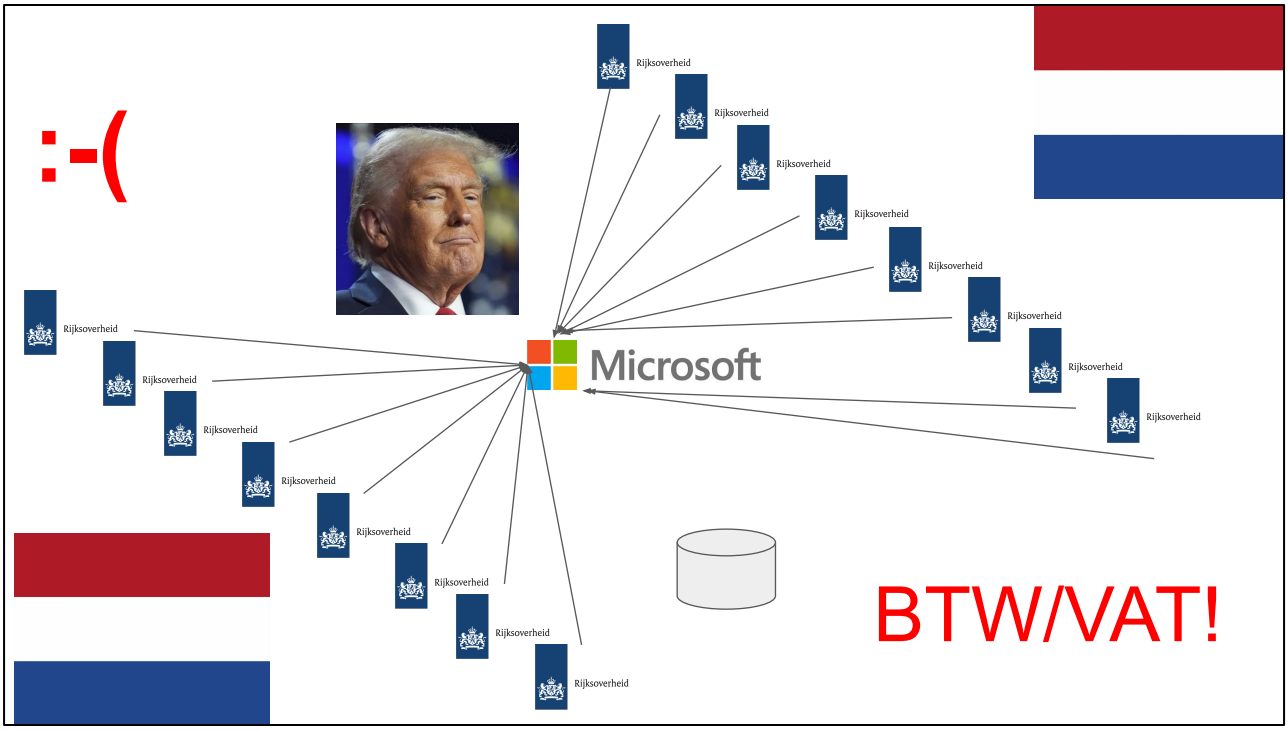
Nice.

Then senior scientist at the US NSA Bob Morris on how to decrypt data:

"First look for **cleartext**. You'll usually find it."

https://federate.social/@mattblaze/115339234462315512


2025-2029
Some ministries
Rijksoverheid
Microsoft
100,00% of all municipalities, banks, notaries public, law firms



That gets you this

Your Word documents will be saved to the cloud automatically on Windows going forward

MARTIN BRINKMANN Aug 27, 2025 Windows 10, Windows 11 News

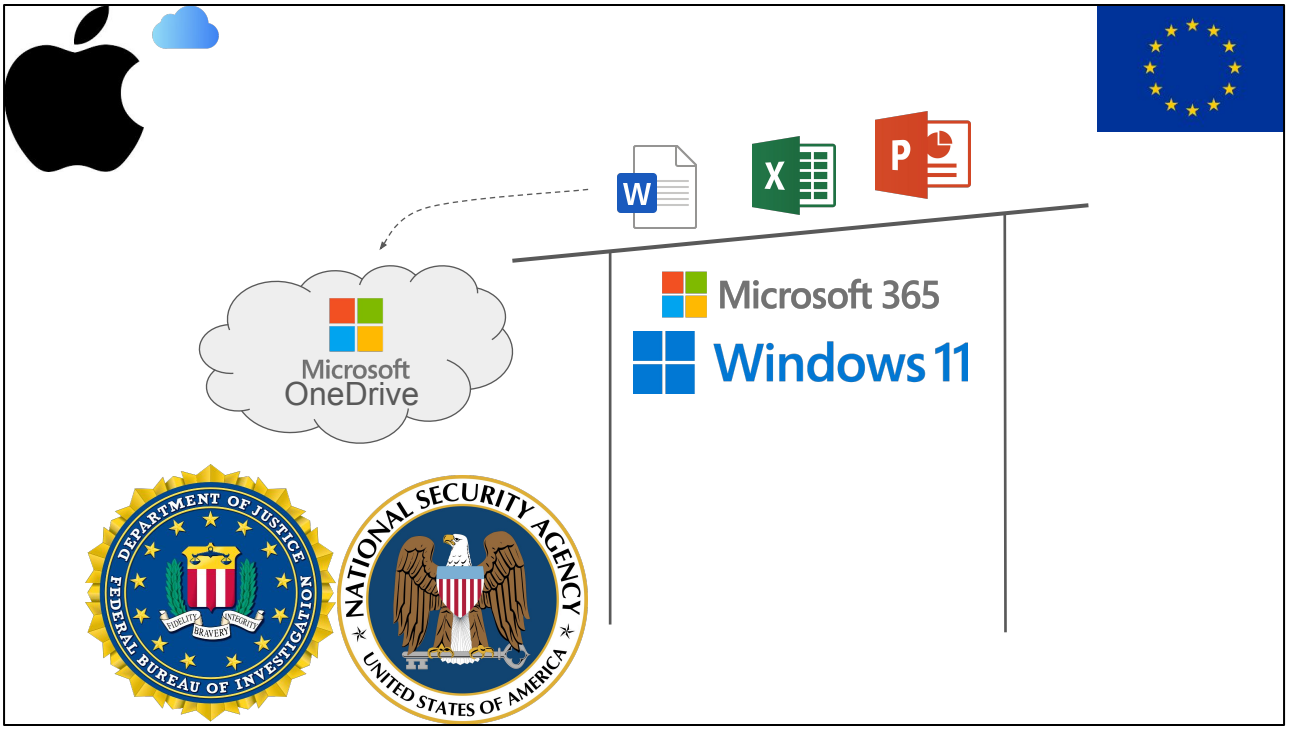
This really is weird

Lawfirms have to host their lawsuits against Microsoft on Microsoft servers

Governments make policy on US, on US servers

A whole continent that is unable to store its own data

https://www.ghacks.net/2025/08/27/your-word-documents-will-be-saved-to-the-cloud-automatically-on-windows-going-forward/



It is what it is.

2 MIN • INFRASTRUCTURE

Microsoft hinders Amsterdam Trade Bank's bankruptcy case

GEERT VAN DER KLUGT
10 aug 2022, 12:44 CEST

The Court of Amsterdam took a swing at Microsoft in a ruling on the bankruptcy of the Amsterdam Trade Bank. According to the court, Microsoft hindered the the case by preventing trustees from accessing important information and thwarting a subpoena.

EDITOR PICKS

Dutch Authority: Data theft via ransomware doubles in one year

In 2024, cybercriminals stole personal data almost twice as often as ...

The International Criminal Court deplores new sanctions from the US administration against ICC Officials

r/sysadmin • 4 maanden geleden
stupidic

This Microsoft Entra ID Vulnerability Could Have Been Catastrophic

Security researcher Dirk-jan Mollema discovered two vulnerabilities in Microsoft's Entra ID identity platform that could have granted attackers administrative access to virtually all Azure customer accounts worldwide. The flaws involved legacy authentication systems – Actor Tokens issued by Azure's Access Control Service and a validation failure in the retiring Azure Active Directory Graph API.

Mollema reported the vulnerabilities to Microsoft on July 14. Microsoft released a global fix three days later and found no evidence of exploitation. The vulnerabilities would have allowed attackers to impersonate any user across any Azure tenant and access all Microsoft services using Entra ID authentication. Microsoft confirmed the fixes were fully implemented by July 23 and added additional security measures in August as part of its Secure Future Initiative. The company issued a CVE on September 4.

https://doublepulsar.com/citrix-forgot-to-tell-you-cve-2025-6543-has-been-used-as-a-zero-day-since-may-2025-d76574e2dd2c

This is all **UNACCEPTABLE**.

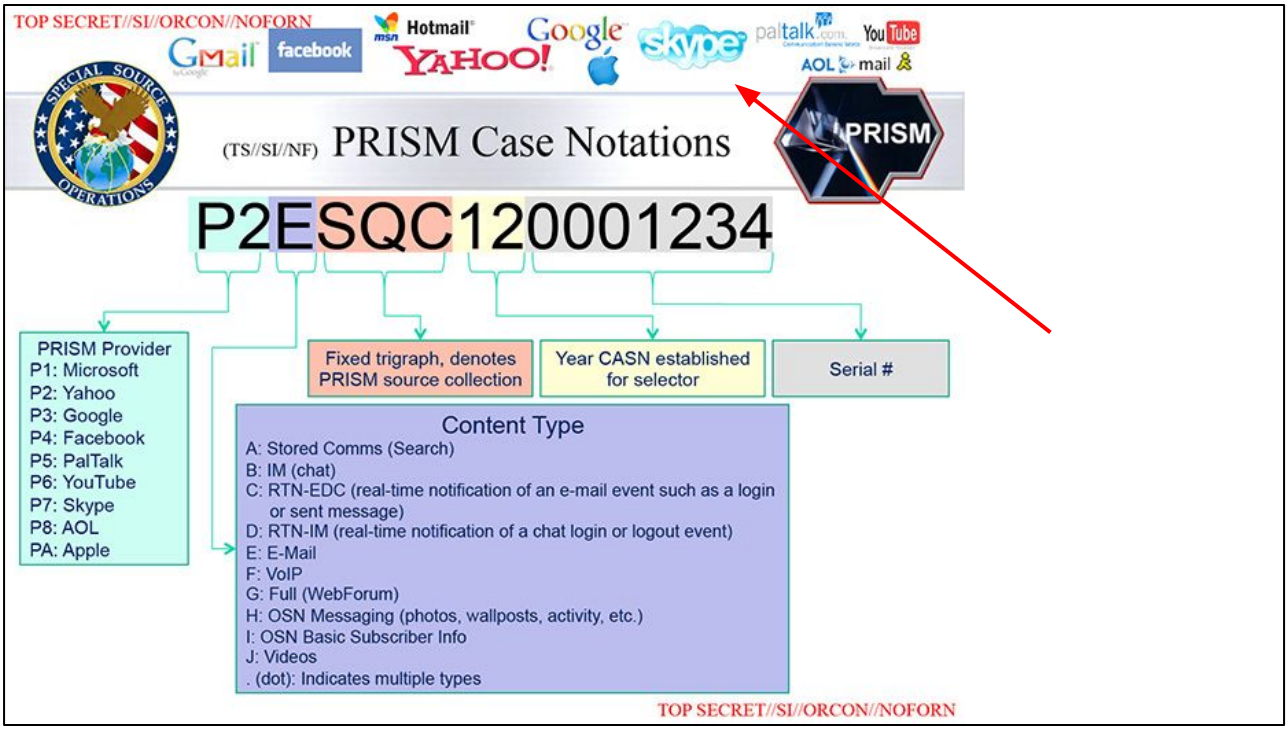
Literally a risk that can not be “accepted” © NCSC Webinar, 2026-03-30

Encryption that was strong… but not TOO strong

Berlin was surrounded by the enemy. “The West” wanted secure phones, secure enough so the soviets could not listen in to Berlin. But the west also wanted to be able to break in when needed. They succeeded.

"Skype was created by Niklas Zennström, Janus Friis, and four Estonian developers, and first released in August 2003. In September 2005, **eBay** acquired it for $2.6 billion"

One of the weirdest acquisitions ever

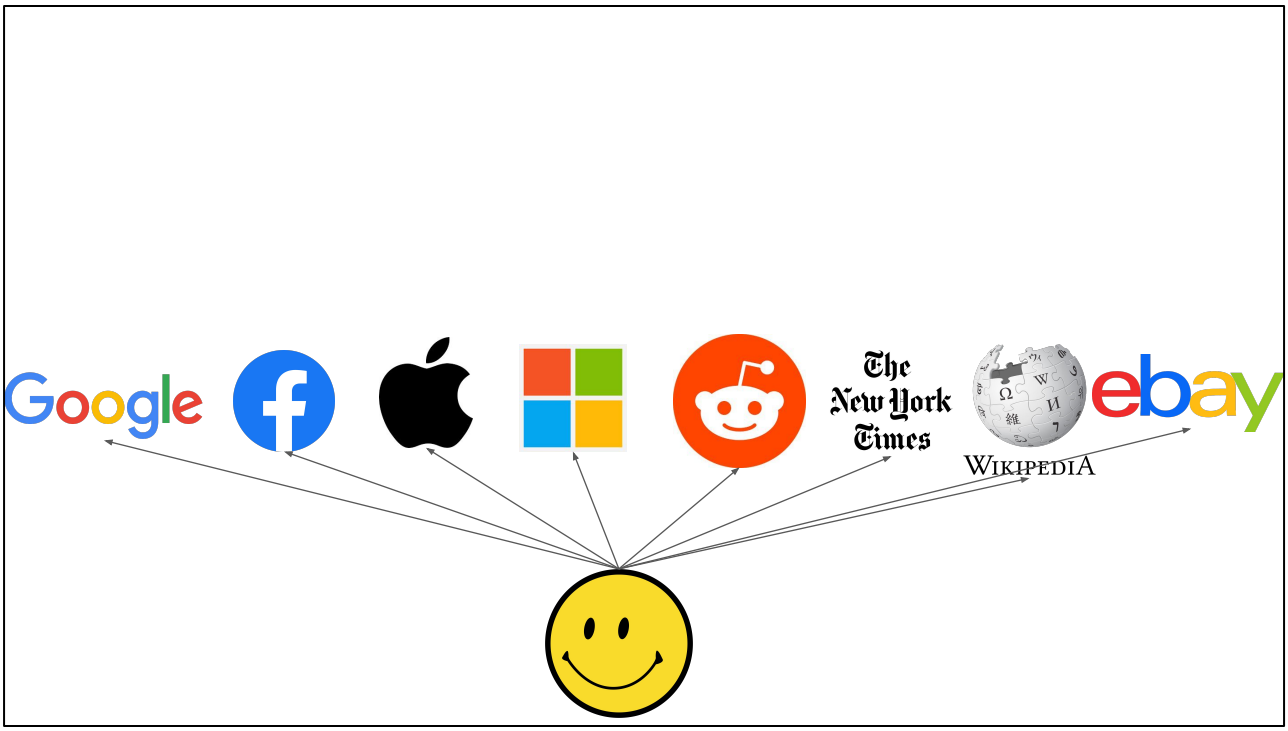


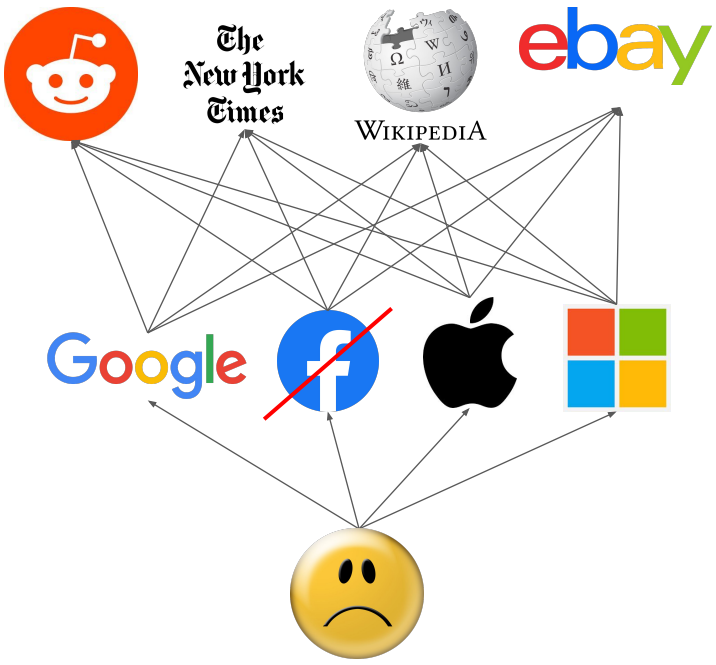
Edward Snowden leaks showing Skype participating in the NSA spying program (2011 data likely)

“Weapons from a more civilized time”

- DES
- GSM
- TETRA/ETSI
- Crypto AG
- Philips Crypto
- Dual_EC_DRBG
  - TLS “extended random”
- "Bullrun"
- NIST curves?
  - Perhaps not

- https://blog.cryptographyengineering.com/2017/12/
- https://en.wikipedia.org/wiki/Dual_EC_DRBG


Google
The New York Times
WIKIPEDIA
ebay

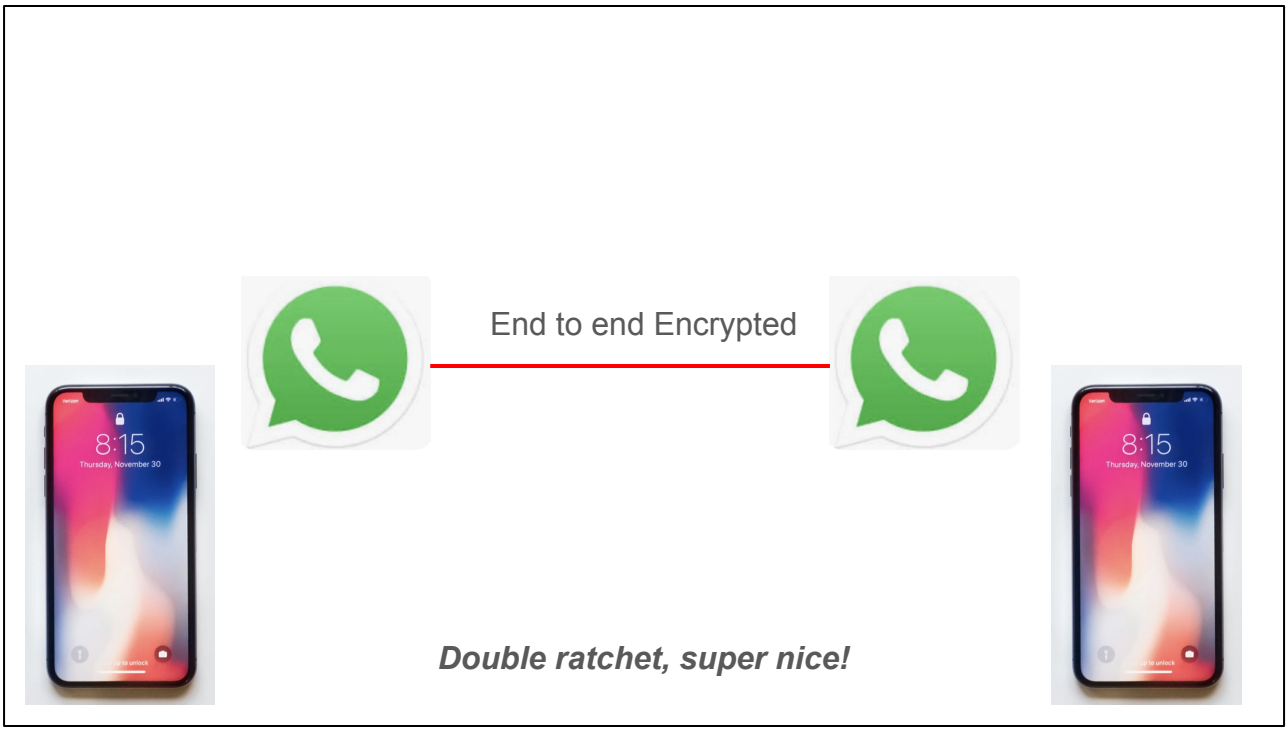


Makes investigations real hard…

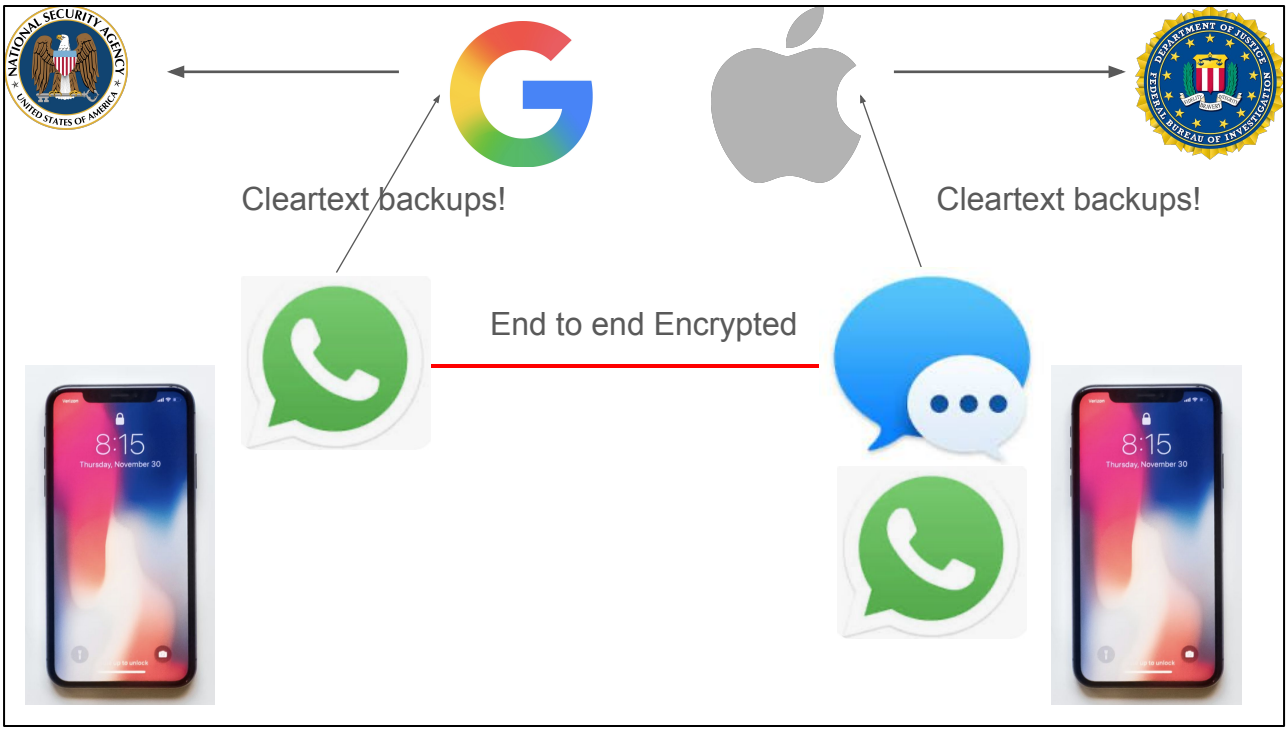
- VPN Pixel by Google
- (~~Facebook Onavo~~)
- **Apple Private Relay**
- Microsoft Edge Secure Network VPN

“But we aren’t telecommunication companies”

https://store.google.com/intl/en/ideas/articles/pixel-vpn/



This is what we are all talking about in effect. We can’t intercept WhatsApp here in Europe, because it is (supposedly) end to end encrypted



Both iphones and android phones URGE you to turn on backups for your most secret communications. Both dissuade you from turning on encrypted backups.

Commercial surveillance
“We’re lovin’ it”

The bulk of websites and apps snitch on everyone all the time

Overview

You must use the AppTrackingTransparency framework if your app collects data about end users and shares it with other companies for purposes of tracking across apps and web sites. The AppTrackingTransparency framework presents an app-tracking authorization request to the user and provides the tracking authorization status.

(“ATT”)

15 MAY 2026

I broke AppLovin's mediation cipher protocol.

I broke the cipher AppLovin wraps around its ad-mediation traffic and decrypted several thousand real requests captured on my consented mobile-traffic research panel. The conclusion is straightforward: The encrypted bid request carries enough device data to deterministically re-identify the same iPhone across apps from different publishers, even when user denies ATT. That payload reaches AppLovin plus around 12 downstream ad networks on every banner load, every ~30 seconds, for as long as the user is playing. The assumption that ATT is the only way to deterministically identify a user is wrong. Fingerprinting the device works just as well.

https://www.buchodi.com/i-broke-applovins-mediation-cipher-protocol/

The mini-envelopes

A typical publisher app has ~18 demand-partner SDKs compiled in: Meta, Google, Mintegral, Vungle, ironSource, Unity, InMobi, BidMachine, Fyber, Moloco, TikTok, Pangle, Chartboost, Verve, MobileFuse, Bigo, Yandex, plus AppLovin's own. When a banner needs filling, the AppLovin SDK calls each of those locally, and asks "prepare a bid signal." Each demand SDK independently constructs an opaque token containing whatever device data its publisher backend wants. The AppLovin SDK bundles them all into `signal_data[]` and ships the whole thing inside its encrypted envelope. AppLovin's server then forwards each token to that bidder's bid server via server-to-server OpenRTB.

Is it encrypted? And well?

The device makes one outgoing network call. The data reaches a dozen separate ad-tech companies.

The OpenRTB spec still "recommends" against use of HTTPS (2.2 Security)

https://blog.bidswitch.com/openrtb-3.0-what-is-it-and-why-is-almost-nobody-using-it-yet

Microsoft handed over keys to BitLocker-encrypted data stored on its servers during an FBI probe last year, granting access to data on three separate laptops.

BitLocker, a built-in data protection feature for Windows, is used by millions of users worldwide to encrypt data on their devices, and has come preinstalled on many Windows devices since Windows 11. Users can choose to store keys locally on a device, such as a USB drive, or on one of Microsoft's servers.

Forbes reports that Microsoft handed the keys over in early 2025, following an FBI request during an investigation into alleged unemployment fraud on the Pacific island of Guam. The case is still ongoing, and about seven people have been charged so far, according to local media.

https://www.pcmag.com/news/report-microsoft-hands-over-keys-for-bitlocker-encrypted-data-to-fbi

By Adam Conway — Published May 13, 2026, 10:53 AM EDT

I'm Adam Conway, an Irish technology fanatic with a BSc in Computer Science and I'm XDA's Lead Technical Editor. My Bachelor's thesis was conducted on the viability of benchmarking the non-functional elements of Android apps and smartphones such as performance, and I've been…

Trending Now

https://www.xda-developers.com/new-windows-11-bitlocker-bypass-needs-usb-stick-researcher-backdoor/

Apple–FBI encryption dispute

From Wikipedia, the free encyclopedia

The **Apple–FBI encryption dispute** concerns whether and to what extent courts in the United States can compel manufacturers to assist in unlocking cell phones whose data are cryptographically protected.[1] There is much debate over public access to strong encryption.[2]

In 2015 and 2016, Apple Inc. received and objected to or challenged at least 11 orders issued by United States district courts under the All Writs Act of 1789. Most of these seek to compel Apple "to use its existing capabilities to extract data like contacts, photos and calls from locked iPhones running on operating systems iOS 7 and older" in order to assist in criminal investigations and prosecutions. A few requests, however, involve phones with more extensive security protections, which Apple has no current ability to break. These orders would compel Apple to write new software that would let the government bypass these devices' security and unlock the phones.[3]

The most well-known instance of the latter category was a February 2016 court case in the United States District Court for the Central District of California. The Federal Bureau of Investigation (FBI) wanted Apple to create and electronically sign new software that would enable the FBI to unlock a work-issued iPhone 5C it recovered from one of the shooters who, in a December 2015 terrorist attack in San Bernardino, California, killed 14 people and injured

An iPhone 5C (color), the model used by one of the perpetrators of the 2015 San Bernardino attack

Apple pulls data protection tool after UK government security row

22 February 2025

Share Save

Zoe Kleinman
Technology editor • @zsk

Apple is taking the unprecedented step of removing its highest level data security tool from customers in the UK, after the government demanded access to user data.

Advanced Data Protection (ADP) means only account holders can view items such as photos or documents they have stored online through a process known as end-to-end encryption.

NSO GROUP

Why did Apple continue to do zero-click display of images and PDFs from untrusted sources? Including a whole font rendering language?
Outside the sandbox?

Google

https://www.upwind.io/feed/webp-zero-day-everything-you-need-to-know-about-libwebp
https://projectzero.google/2021/12/a-deep-dive-into-nso-zero-click.html

“The stalemate”
(maintaining US access to most data)

Why do we allow this to happen?

Historical Reasons, not just laziness

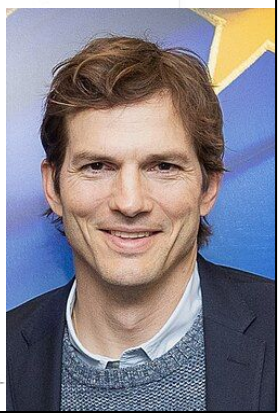
“Get Meta to scan Europe’s deepest secrets & report us to local police. SOME politicians & government people get an exemption”

EUROPEAN COMMISSION

Brussels, 11.5.2022

COM(2022) 209 final

2022/0155(COD)



Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down rules to prevent and combat child sexual abuse

(Text with EEA relevance)

{SEC(2022) 209 final} - {SWD(2022) 209 final} - {SWD(2022) 210 final}

NEWS ARTICLE | 24 June 2025 | Directorate-General for Migration and Home Affairs | 2 min read

Commission presents Roadmap for effective and lawful access to data for law enforcement

Register of Commission Expert Groups and Other Similar Entities

GROUP | E04005

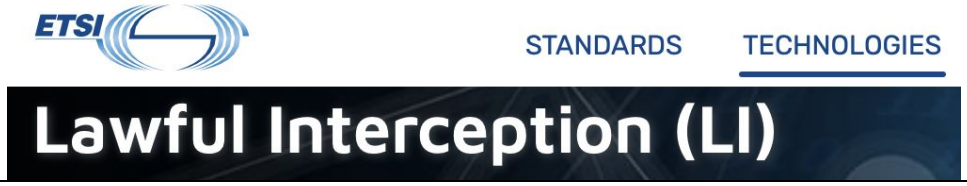
Expert Group for a Technology Roadmap on Encryption (E04005)

ACTIVE

The US has ample access to “encrypted” data. They do not have our problem. **They could already help us also**. They have data on all Europeans

It is theoretically possible to **standardize** and **legislate** access to supposedly end-to-end encrypted data.

However, will take >5 years of **transatlantic cooperative** standard setting and **political** negotiations



But are they any good at it in the US?

The Chinese state-sponsored advanced persistent threat (APT) known as Salt Typhoon appears to have accessed major US broadband provider networks by hacking into the systems that law-enforcement agencies use for court-authorized wiretapping.

According to unnamed sources speaking to the Wall Street Journal, the affected providers include major national players like AT&T and Verizon Communications, along with enterprise-specific service providers like Lumen Technologies.

In addition to the wiretapping connections, the sources said Salt Typhoon also had access to more general Internet traffic flowing through the provider networks, and that the cyberattackers went after a handful of targets outside the US as well. The APT could have had access for months, they added.

“Salt Typhoon”

https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF

DUAL_EC_DRBG & RSA BSAFE was a disgrace

Summarizing

- It is effectively impossible for “normals” to communicate/author documents without their data ending up in (effective) plaintext on US controlled servers
  - Try it!
- This is maintained through an ongoing evolving stalemate between USGOV and large communication providers (Apple, Google, Microsoft, Meta etc)
- Encryption is mostly between users and the servers accessible to the US government. Postquantum straight to the NSA!
- Advertising networks feed into this network too
- US appears however to be that great at execution anymore
- EU has some feeble efforts going

Sovereignty & global surveillance

https://berthub.eu/dis