

---

---

# Ctrl+Alt+Activism

— safeguard ur online-self —

---

---



It's not just to regulate a system, it can be to develop systems, a legal system, or even a system of government. Remember, a system is just a bunch of parts that function together as a whole.

It's one of the great stumbling facts of working with systems, that the point of a system that malfunctioned is almost never the point which you make the malfunction. To find what caused the system to collapse, you have to start from the point where you spotted the problem, and trace it backward through all of the system's components.

# Edward Snowden

former NSA contractor

leaked NSA docs in 2013

- mass data collection programs like PRISM, XKeyscore, Tempora, etc...
- Documents on Foreign Leaders, Five Eyes Alliance

# Edward Snowden

The U.S.A in response...

- revoked his passport, stranding him at Moscow airport
- brought him up on charges relating to the Espionage Act
- ...

excerpts are part of the documentary War for the Web



# Aaron Swartz



# Aaron Swartz

- Hacktivist and Reddit Co-founder
- Arrested for downloading millions of academic articles from JSTOR
- Faced a potential 35-year prison sentence and a \$1 million fine
- Two years into the legal battle, Swartz was found dead in his Brooklyn apartment
- JSTOR, the provider of academic articles, did not seek a lawsuit against Swartz

image of "we dont like cops"

# Canadian Government Censorship

# Canadian Government Censorship

Project Cleanfeed Canada

- Major Canadian ISPs voluntary effort to block websites hosting CSAM (child sexual abuse material)

**Bell**

**MTS**allstream

**Shaw)**

**SaskTel** 



**VIDÉOTRON**

 **ROGERS**<sup>TM</sup>

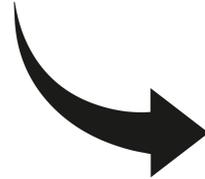
 **TELUS**

# Canadian Government Censorship



Fairplay Canada

- Coalition of telecom and media giants. Proposed blocking copyright-infringing sites to CRTC.
- No judicial oversight planned.
- Potential Charter rights violation.
- CRTC ignored the move due to lack of jurisdiction.
- biggest target/victim was a pirate IPTV service



# Canadian Government Censorship



Front de libération du Québec crisis

- 1970 Canada event.
- FLQ kidnapped Laporte, Cross.
- PM P. Trudeau invokes War Measures Act.
- Lacroix blamed journalists for death.
- War Measures Act invoked.
- CBC restricted news coverage.

# Canadian Government Censorship

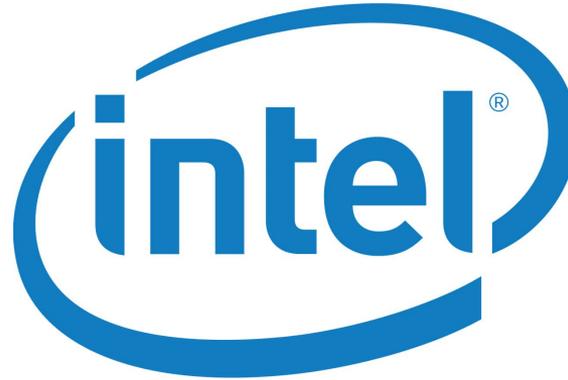


Canada Truckers convoy protest

- J. Trudeau involved.
- Protestors' bank accounts frozen.
- Judge: Federal Emergencies Act use unreasonable.

**More specific to cs and programming:**

# NSA & Intel



- NSA built a backdoor into Intel CPUs (supposedly)
- through Intel Management Engine

# NSA & Intel

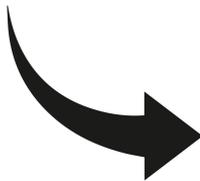
What is Intel Management Engine?

- Separate CPU in Intel chipsets post-2008.
- Controls primary CPU, with elevated privileges.
- Full network, memory access; independent of BIOS, CPU, OS.
- Operates even when PC is off, with power.
- Runs closed-source MINIX software.

# NSA & Intel

What Intel ME can do:

- Bypass firewall rules
- see all data passing through CPU and RAM
- Obviously, huge security risk, which has been exploited before



The screenshot shows a support article on the Intel website. The header is purple with the word 'Support' in white. The article title is 'Intel Management Engine Critical Firmware Update (Intel-SA-00086)'. The main text describes security vulnerabilities in Intel Management Engine (ME) and Trusted Execution Engine (TXE) firmware. A 'Note' box highlights that the article does not contain information about Meltdown/Spectre vulnerabilities. The article includes a list of affected products: Intel Management Engine (ME), Intel Trusted Execution Engine (TXE), and Intel Server Platform Services (SPS). On the right side, there are icons for email and print, and a sidebar with 'Documentation', 'Content Type Troubleshooting', 'Article ID 000025619', and 'Last Reviewed 11/13/2023'.

# NSA & Intel

- US government requested Intel chips without ME, under secret deal.
- AMD has similar system, AMD Platform Security Processor (PSP).
- PSP grants similar access and vulnerabilities.
- Solutions: Install LibreBoot/CoreBoot, use TempleOS/TailOS, or System76 laptops with disabled ME.

# NSA & Intel

- Conspiracy theories say that NSA had access to these backdoors, and would often exploit them.
- these r just theories and tbh they lack sustenance and proof, but they're fun to think abt.

# Expert claims NSA has backdoors in Intel, AMD processors

by [PETER SCOTT](#)

on 31 JULY 2013

[TWEET](#)

FONT SIZE

[PRINT](#)[EMAIL](#)[HOME](#)[HOME](#)[NEWS](#)[REVIEWS](#)[ABOUT](#)

## Paranoid tin foil hat wearers were right all along?

We're not fans of conspiracy theories and we can never be. They don't stand up to scientific scrutiny and as a geek site we have a soft spot for science, tech and logic. Well, at least science and tech, logic is overrated.

Silicon Valley security expert Steve Blank now says there is a very good chance that AMD and Intel processors ship with a very nice feature for totalitarian regimes. They might have a backdoor that allows spooks to access and control computers. Furthermore security expert Jonathan Brossard recently told the Financial Review that CPU backdoors are attractive attack vectors.

Blank said the NSA has already secured pre-encryption access to Microsoft's email services and that this could be why the Kremlin is bringing back electric typewriters, which we find very cool as they remind us of the Cold War.

He pointed out that hacking computers was a lot better for the NSA than cracking codes. Why would they bother with decryption when they could tap processors directly, via a backdoor? Blank said chip companies started integrating automatic software patching in the nineties, in an effort to resolve small bugs without recalling the processors.

The NSA could have used the same avenue to do its shady job.

"Perhaps they are the only good guys," he said. "Or perhaps the NSA – legally compelling the chip vendors and/or Microsoft, or working outside of them – have compromised the microcode updates that affect most computers."

# Intel chips could let US spies inside: expert

PUBLISHED: 30 JUL 2013 00:05:47 | UPDATED: 30 JUL 2013 12:39:54

SHARE LINKS:   Share  Recommend  417

  Reprints & permissions



A spokesperson for Intel says there's "no basis for these highly speculative claims" that the US National Security Agency may embed "back doors" inside chips produced by Intel and AMD. Photo: Andrew De La Rue

**CHRISTOPHER JOYE AND PAUL SMITH**

One of Silicon Valley's most respected technology experts, [Steve Blank](#), says he would be "surprised" if the US National Security Agency was not embedding "back doors" inside chips produced by Intel and AMD, two of the world's largest semiconductor firms, giving them the possibility to access and control machines.

Internationally renowned security research engineer [Jonathan Brossard](#), who unveiled what *Forbes* described as an “[undetectable and incurable](#)” permanent back door at last year’s prestigious Black Hat conference, told the *Financial Review* that he had independently concluded that CPU back doors are “attractive attack vectors”.

# Big Tech's wrongdoings

# FAAN(G)

one of the big business strategies of these companies is providing exceptional service for free.

you use free services like all the time

If you are not  
paying for the  
product,  
then you are the  
product

Baidu 百度

salesforce



ByteDance

NVIDIA



dji



Tencent 腾讯

ORACLE

intel.

# FAAN(G)

we've heard of the pretty loud and blatant cases (i.e google selling ur data, etc etc)

 **Signal**  @signalapp · 3h ⋮

With the May 15th WhatsApp Terms of Service acceptance deadline fast approaching, Mark leads by example:



Leaked phone number of Mark Zuckerberg reveals he is on Signal  
Zuckerberg's phone number was among the leaked data of 533 million Facebook users. A security researcher confirmed that Zuckerberg uses ...  
[indiatoday.in](https://indiatoday.in)

101 1.6K 4.5K

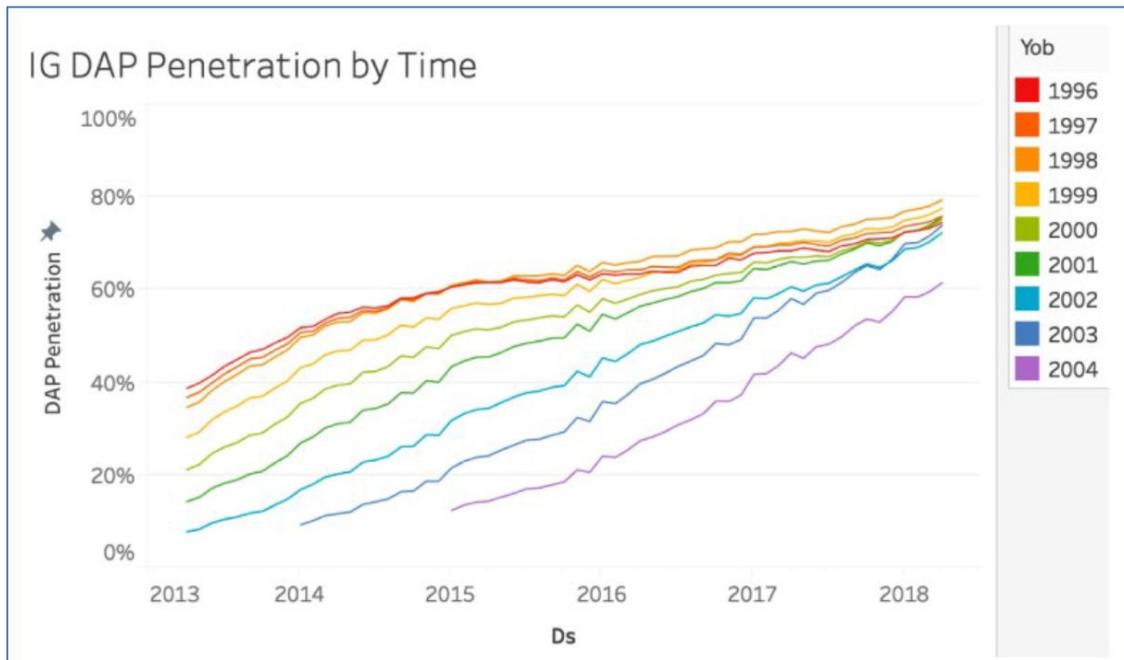
**Meta/Facebook**

# FAAN(G)

Meta (formerly Facebook) aware of large underage presence.

- Actively pursued under 13-year-old group.
- Monthly Active People Penetration (MAP) tracked.
- 20-60% of 11-13 year olds using Instagram monthly.
- Meta saw this as successful market reach, not a problem.
- Exploiting children for monetary gain.





- "The chart reveals that in 2016, approximately 20% of users from the 2004 birth year cohort (i.e., Instagram users who were 12 years old at that time) used Instagram on at least a daily basis." (652)

◆ WSJ NEWS EXCLUSIVE

## Instagram Connects Vast Pedophile Network

The Meta unit's systems for fostering communities have guided users to child-sex content; company says it is improving internal controls



LIONEL BONAVENTURE/AFP/GETTY IMAGES

By [Jeff Horwitz](#)

and [Katherine Blunt](#)

June 7, 2023 7:05 am ET

# FAAN(g)

Should 100% be prosecuted & sanctioned but according to opensecrets.com...

## Meta

*Top Affiliates: Facebook Reality Labs · Facebook Technologies · Instagram*

Cycle: 2024

DONATE

### CONTRIBUTIONS

Ranks 209 of 26,562

\$835,469

### LOBBYING

Ranks 9 of 9,458 in 2024

\$19,300,000 in 2023

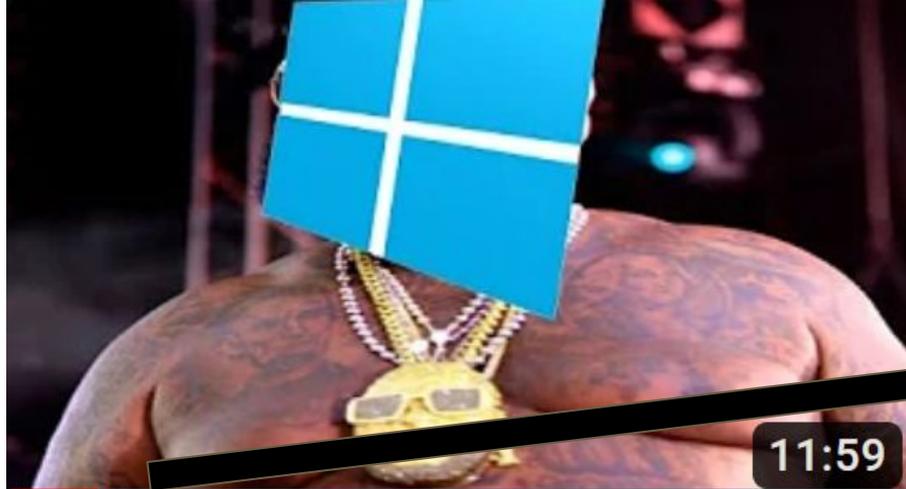
### OUTSIDE SPENDING

\$0

**Microsoft**

# FAAN(G)

- Windows: Loaded with bloatware.
- Windows 10 and 11: Telemetry invasion



# FAAN(G)

- Windows telemetry: Data uploaded by Connected User Experience and Telemetry component (UTC).
- Microsoft collects from Windows 10 and 11, uploads to their and 3rd party servers.
- The PC Security Channel did an insight:



# FAAN(G)

- Windows telemetry includes advertising and marketing data.
- Baseline telemetry occurs even with minimum settings.
- Data sent to Microsoft and third-party servers.
- Telemetry starts before internet connection, app usage.
- Users pay for Windows 10/11 (cost included in PC price).