



Social Media Evidence: a digital panopticon

Craig Everson SC

Deputy Senior Crown Prosecutor, NSW

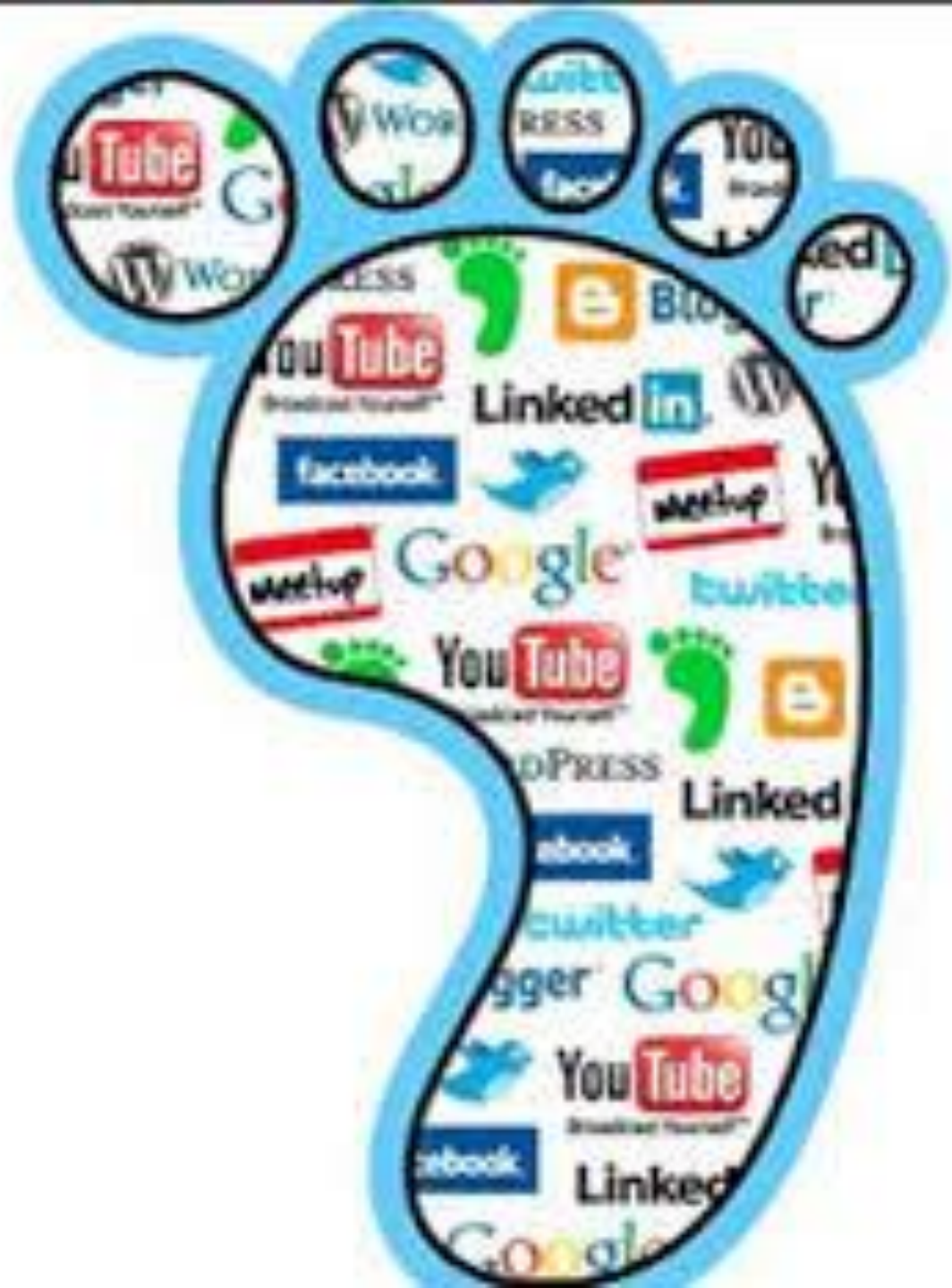
Public Defenders Conference 2022

Am I Being Watched?



“... there was of course no way of knowing whether you were being watched at any given moment ... you had to live ... in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.”

► George Orwell, *Nineteen Eighty-Four*, pp.4-5



**Digital
Footprints**



Calls for TikTok to be banned in Australia over Chinese spying fears

Hamish Goodall • 

Published: 06/07/2020 • Updated: 6 July 2020 7:50 am



Australia could soon move to ban Tik Tok over spying fears
Credit: Getty Images

Share:   

The Australian Government is facing calls to ban social media app TikTok over national security and spying concerns.

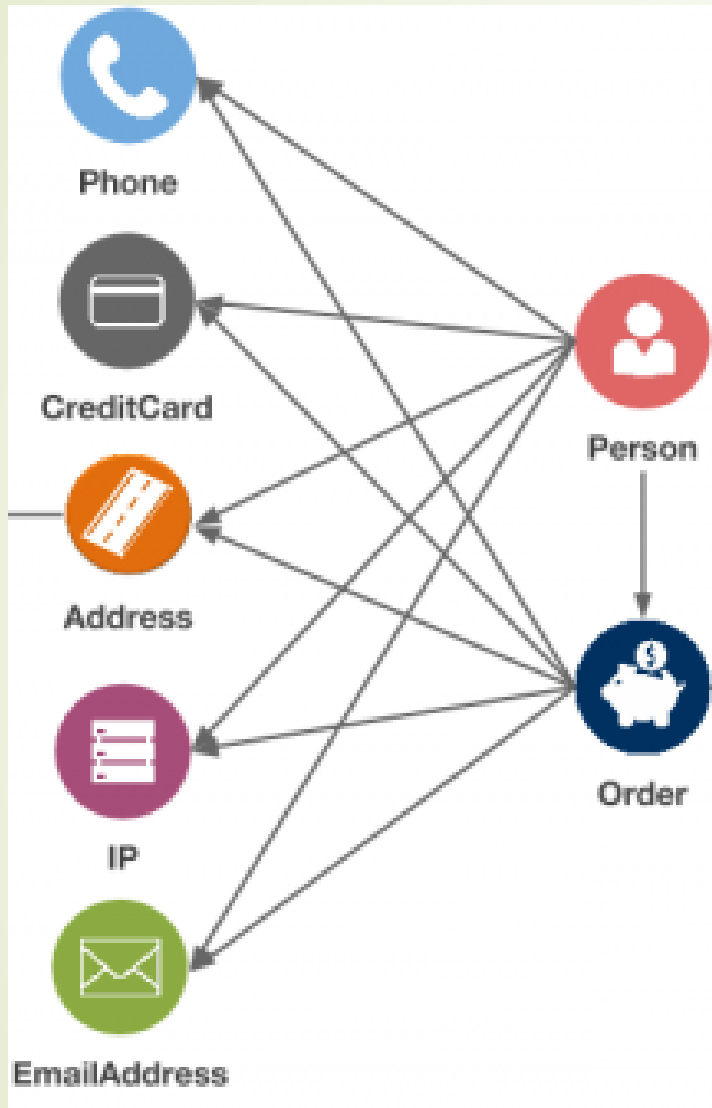
➤ TikTok ban being investigated in Australia over China ...

➤ <https://7news.com.au/sunrise/on-the-show/fresh-calls-for-australian...>

➤ **6 July 2020:** The Australian Government is facing calls to ban social media app TikTok over national security and spying concerns. The *Herald Sun* reports that plans are underway to haul the video-sharing platform before the Foreign Interference through Social Media senate inquiry amid fears the Chinese-owned platform leaks users' information to Beijing.

Palantir is a provider of software applications for integrating, visualizing and analysing information.







Clearview AI
Technology
to help solve
the hardest
crimes



PROCESSING
OF FACE
RECOGNITION

S1 - 528.08; S2 - 833.22; S3 - 944.47
S4 - 922.76; S5 - 334.69; S6 - 432.78
S7 - 899.65; S8 - 209.25; S9 - 798.45
S1 - 528.08; S2 - 833.22; S3 - 798.45
S3 - 944.47; S4 - 922.76; S5 - 387.49
S7 - 899.65; S8 - 209.25; S9 - 449.90
S1 - 528.08; S2 - 833.22; S3 - 944.47
S4 - 922.76; S5 - 334.69; S6 - 432.78
S7 - 899.65; S8 - 209.25; S9 - 528.08
S2 - 833.22; S3 - 798.45; S5 - 387.49
S4 - 922.76; S5 - 387.49; S7 - 899.65
S8 - 209.25; S9 - 449.90; S9 - 798.45


“

*Documents obtained by the ABC reveal how the Australian Federal Police made use of **Clearview AI** — a controversial facial recognition technology that is now the focus of a federal investigation. The AFP acknowledged in April that members of the ACCE had undertaken a free trial of Clearview's facial recognition services, but the extent of its use by officers remained unclear.*

”

– ABC News 13 July 2020

See: <https://www.abc.net.au/news/2020-07-13/afp-use-of-facial-recognition-software-clearview-ai-revealed/12451554>



Facial recognition firm Clearview AI tells investors it's seeking massive expansion beyond law enforcement

– *The Washington Post*,
16 February 2022

By Drew Harwell

The facial recognition company **Clearview AI** is telling investors it is on track to have 100 billion facial photos in its database within a year, enough to ensure “**almost everyone in the world will be identifiable,**” according to a financial presentation from December obtained by *The Washington Post*.

[...]

And the company wants to expand beyond scanning faces for the police, saying in the presentation that it could monitor “gig economy” workers **and is researching** a number of new technologies that could **identify someone based on how they walk, detect their location from a photo or scan their fingerprints from afar.**

Origins of Social Media

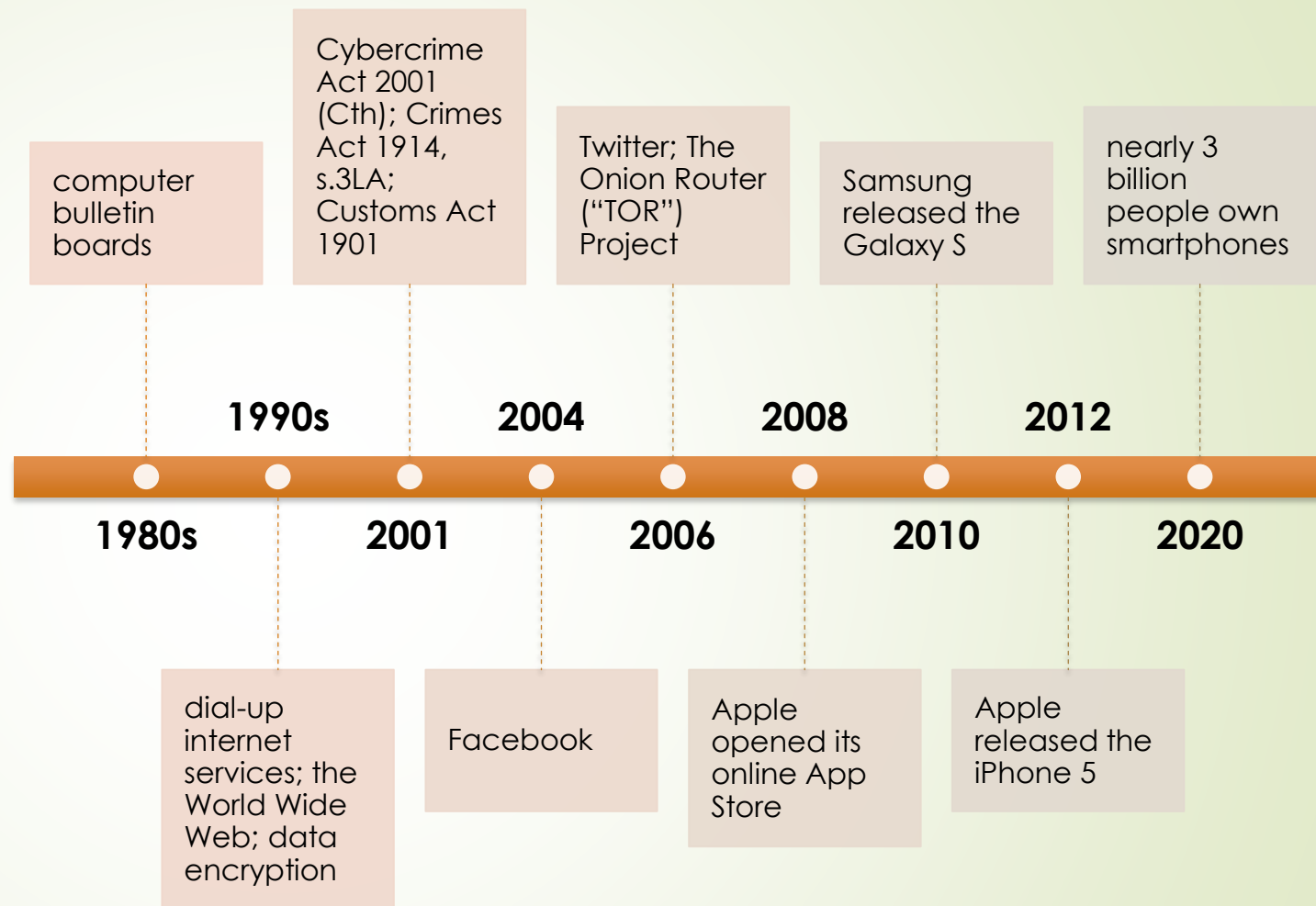
circa 1980:
Computer Bulletin Boards



Privilege Against Self-Incrimination?



Digital Developments



Section 3LA, *Crimes Act 1914* (Cth)

- ***Commissioner of the Australian Federal Police v Luppino*** (2021) 284 FCR 233; [2021] FCAFC 43
- ***Luppino v Fisher (No2)*** [2019] FCA 1100

- ***R v Mohamed, Charani & Moukhaiber (Ruling 2)***
[2019] VSC 72

- ***R v Smith*** [2016] QDC 62





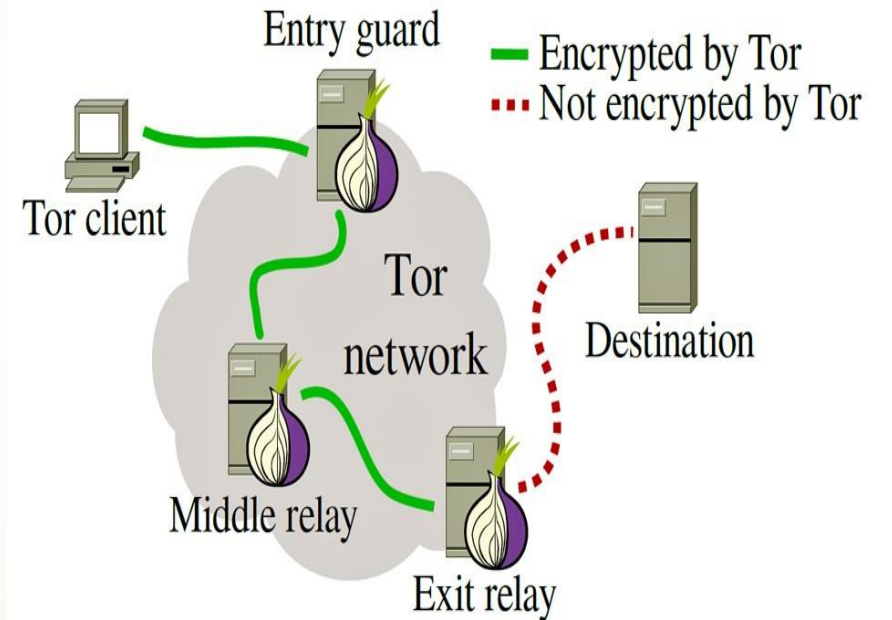
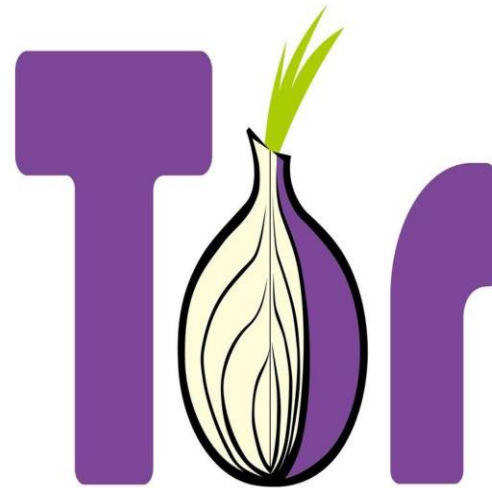
Mutual Assistance in Criminal Matters Act 1987 (Cth).

Used to obtain:

- ➔ **account subscriber details** (the details recorded about the identity of the person who controls the email or social media account) and the IP addresses through which the account was accessed (Internet data); and
- ➔ **the content of accounts** including sent and received emails or messages, postings, commentary, friend lists, contacts, messages, drafts of emails or messages, deleted emails or messages, pictures, videos and links

Encryption and Anonymity

THE ONION ROUTER





Assumed On-Line Identities

- *Crimes Act 1914 (Cth), Part 1AC*
- *Law Enforcement and National Security (Assumed Identities) Act 2010 (NSW)*
- *R v Priest [2011] ACTSC 18*
- *R v Nguyen [2016] NSWDC 395*
- *R v Howe [2017] QCA 7*

Phone Encryption Issues 1

“Two years later, **Brittney Mills** murder case still unsolved after DA hired private company to crack iPhone”

– *The Advocate*, Baton Rouge, Louisiana, USA, 8 May 2017

“... investigators found two smartphones alongside the body of **Ray Owens**. Both devices were passcode protected.

An Illinois state judge issued a warrant ordering Apple and Google to unlock the phones and share with authorities any data therein that could potentially solve the murder. Apple and Google replied, in essence, that they could not — because they did not know the user’s passcode.

The homicide remains unsolved.”

- “When Phone Encryption Blocks Justice,” By Cyrus R. Vance Jr, et al, *New York Times*, 11 August 2015



Phone Encryption Issues 2

- ➔ San Bernadino, USA, December 2015
- ➔ FBI v Apple, February 2016
- ➔ 'Professional Hackers' Crack iPhone, March 2016
- ➔ Cellebrite?

Grayshift's *GrayKey*



*** *Telecommunications and Other Legislation
Amendment (Assistance and Access) Act 2018* (Cth)**





Tuesday 7 July 2020:

“A 40-year-old Sydney man is due to appear before the Central Local Court on child abuse charges following an investigation ... commenced after the AFP-led Australian Centre to Counter Child Exploitation received a report from the United States’ National Centre for Missing and Exploited Children (NCMEC) on 11 March 2020.

[...]

During the search warrant, a number of electronic items were seized for evidentiary purposes and will be subject to forensic examination.”

<https://www.afp.gov.au/news-media/media-releases/sydney-man-face-court-child-abuse-charges>

Child porn blitz nabs state's 'sickest pervs'



NSW Police have arrested 44 men across the country — eight of them in NSW.

AFP Assistant Commissioner Lesa Gale said sites hosting online child sexual abuse material were “crashing due to the increased volume of traffic”.

“During the early stages of COVID-19 (between Feb-April) the AFP witnessed traffic to dark web forums offering child abuse material more than double to the same period in 2019,” she said.

October 2020 - Operation Molto

- FEDERAL police have arrested 44 men across the country — eight of them in NSW.
- AFP Assistant Commissioner Lesa Gale said sites hosting online child sexual abuse material were “crashing due to the increased volume of traffic” .
- “During the early stages of COVID-19 (between Feb-April) the AFP witnessed traffic to dark web forums offering child abuse material more than double to the same period in 2019,” she said.

Media ► News & Press ► UK tip leads to Sydney man charged with possessing child abuse material

UK tip leads to Sydney man charged with possessing child abuse material



Wednesday, 16 February 2022, 9:08pm

Editor's Note: Views of the press and items of the related items are available via <https://www.afp.gov.au/press>


The Australian Federal Police has charged a 43-year-old Sydney man with allegedly possessing child abuse material. He appeared before Sydney Central Local Court today (Wednesday, 16 February 2022).

Investigators from the AFP Eastern Command Child Protection Operations team executed a search warrant at the man's home in Drummoyne this morning.

The operational activity followed a report from the United Kingdom's National Crime Agency to the Australian Centre to Counter Child Exploitation (ACCCE) about a Snapchat user allegedly engaging in sexualised chats and requesting sexualised images and videos of children.

AFP Media Release, 16 Feb 2022:

- The Australian Federal Police has charged a 43-year-old Sydney man with allegedly possessing child abuse material. He appeared before Sydney Central Local Court today (Wednesday, 16 February 2022).
- Investigators from the AFP Eastern Command Child Protection Operations team executed a search warrant at the man's home in Drummoyne this morning.
- The operational activity followed a report from the United Kingdom's National Crime Agency to the **Australian Centre to Counter Child Exploitation (ACCCE)** about a Snapchat user allegedly engaging in sexualised chats and requesting sexualised images and videos of children.



“... allow law enforcement and national security agencies in each participating country to issue orders, through a competent authority, for the production of data directed to communications and technology companies in the other country’s jurisdiction.”

Telecommunications Legislation Amendment (International Production Orders) Bill 2020

Crims cop new data laws

CHARLES MIRANDA

POLICE will have powers to intercept live stream video phone conversations and data of targeted criminals overseas, regardless of their encrypted device, under unprecedented new powers that even took federal parliament by surprise.

Critically, the move will also block Facebook stalkers.

There is evidence that prosecutions were being dropped because the social network giant was stalling on handing over evidence to police for up to five years.

In what is being hailed as a game changer for Australian law enforcement, including police and ASIO spies, agencies under strict protocols will be allowed to tap into encryp-

ted services such as Google, Apple cloud, WhatsApp, Viber and Facebook Messenger.

Australia has never had the ability to access, in real time, overseas service providers, a majority of which are based in the United States.

But amendments to the laws are set to allow that.

The parliamentary joint committee on intelligence and

security had been looking at proposed amendments believing they were just for overseas stored data and expressed shock when it was realised they extended to live-stream interceptions.

“This is something that the committee has just uncovered today in terms of the bill itself.”

The parliamentary joint committee deputy chair Anthony Byrne said.

If approved later this year, major fraud, transnational drug smuggling, terrorism and child exploitation will be some of the categories for which authorities will be allowed to tap offshore service providers, including live-stream interception and stored cloud data.

NSW Police Assistant Commissioner and Commander, Forensic Evidence

and Technical Services Command Michael Fitzgerald said the bill, if passed, would give authorities “unprecedented but necessary” capacity to expedite investigations.

He said his officers had been hampered by current laws, which the committee heard were outdated for the digital era and often took years to attain evidence under.

Telecommunications Legislation Amendment (International Production Orders) Act 2021, No. 78, 2021

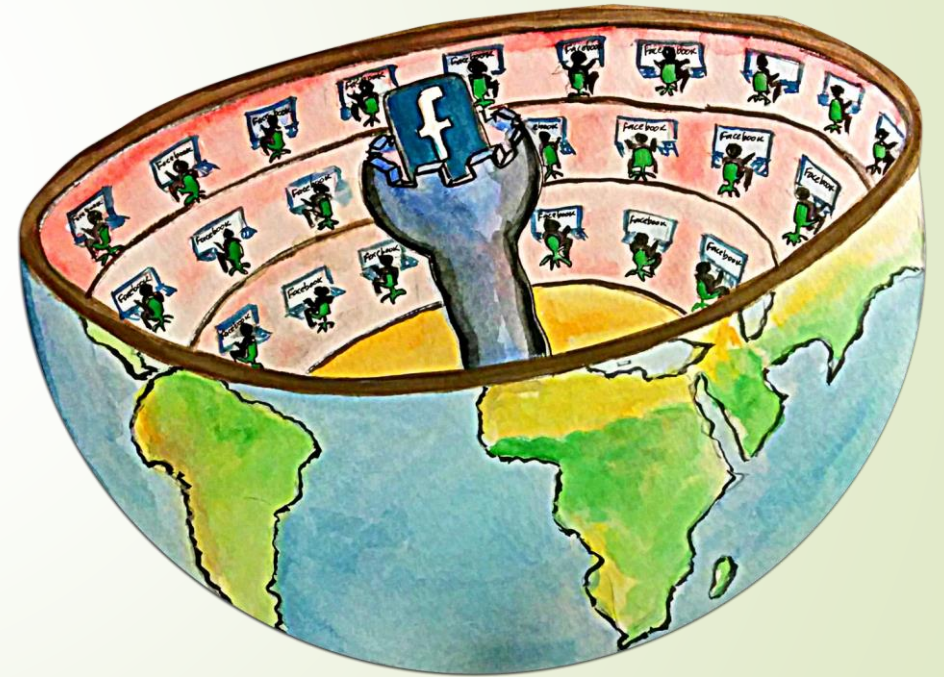
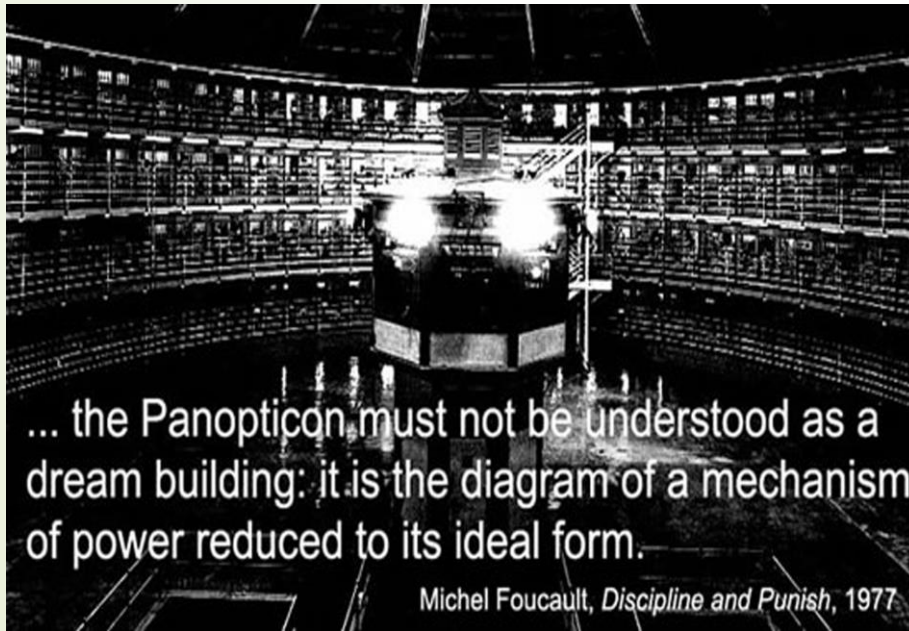
An Act to amend the *Telecommunications (Interception and Access) Act 1979*, and for other purposes

On 23 July 2021, the ***Telecommunications Legislation Amendment (International Production Orders) Act 2021*** received Royal Assent.

- Subject to reciprocal international agreements, the *International Production Orders Act* enables Australian Government agencies to obtain "International Production Orders" (IPOs) issued directly to foreign "prescribed communications providers", in respect of information stored overseas.
- Likewise, Australian-based prescribed communications providers will be subject to compliance with incoming IPOs issued by international authorities.
- The law is a precondition to Australia entering into a bilateral agreement with the United States under its "**Clarifying the Lawful Overseas Use of Data Act**" – the CLOUD Act.



Food for Thought





Yes.
We are being watched.