

AI and Privacy: Back to the Future

Privacy Week 2025

Dr Andrew Chen and James Ting-Edwards

13 May 2025

Speakers

Dr Andrew Chen

Chief Advisor: Technology Assurance
New Zealand Police

Trained in technology,
picked up ethics along the way

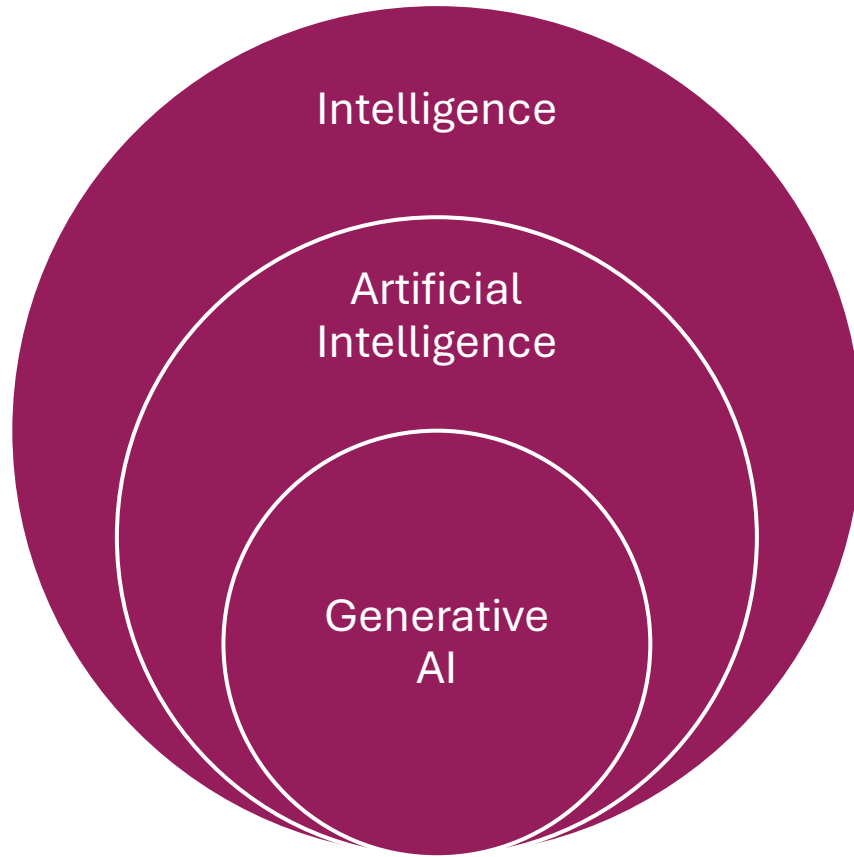
James Ting-Edwards

Senior Policy Advisor
Office of the Privacy Commissioner

Trained in law and philosophy,
picked up technology along the way



The views and opinions expressed in this presentation are solely those of the presenter(s) and do not necessarily reflect the official policy or position of New Zealand Police, the Office of the Privacy Commissioner, or the government.



The ability to derive information, learn from experience, and correctly utilise thought and reason

Intelligence, but simulated using algorithms and data to give the impression of thinking

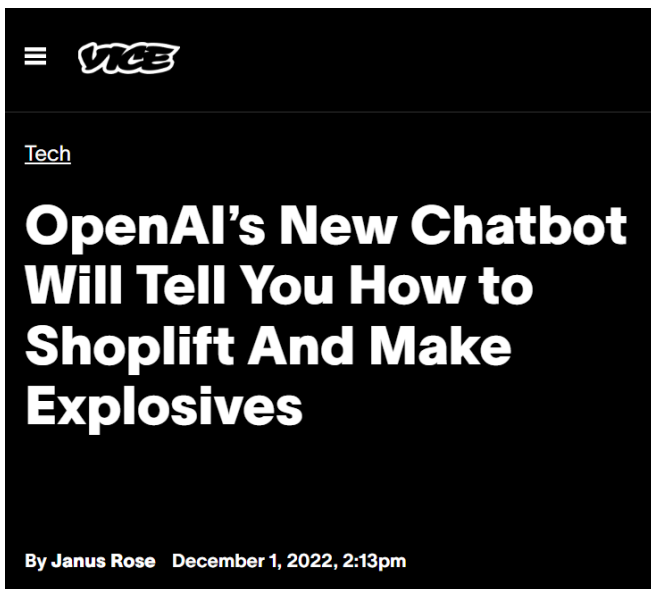
Artificial Intelligence, but people think it's cool towards creating new content (text, audio, image/video)

OpenAI debuts ChatGPT and GPT-3.5 series as GPT-4 rumors fly

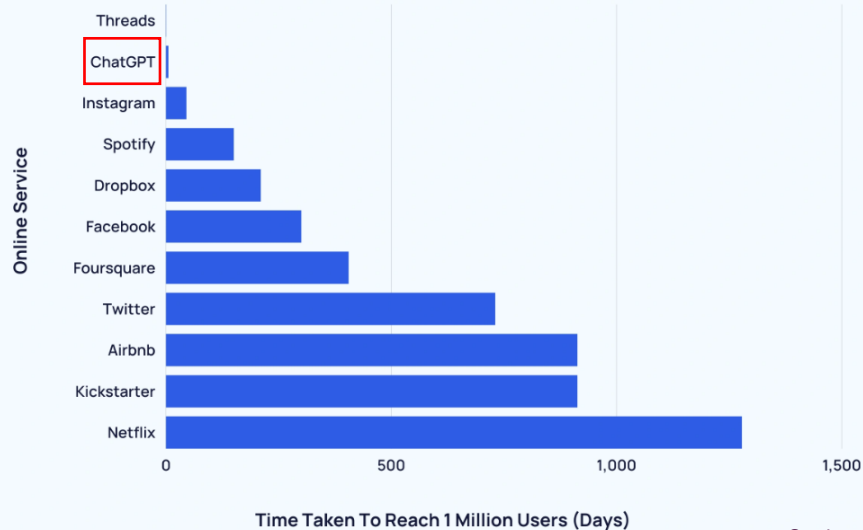
Sharon Goldman

@sharongoldman

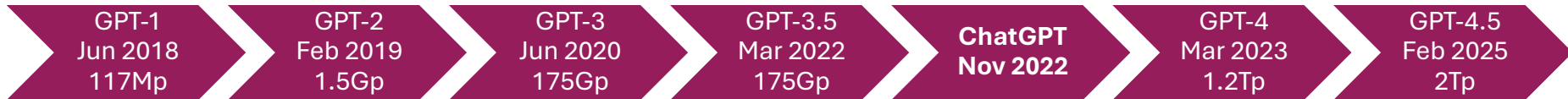
November 30, 2022 1:34 PM



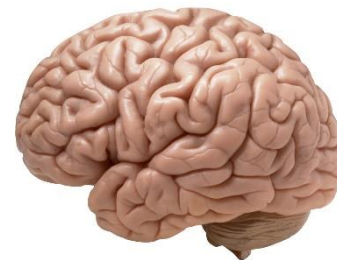
Time taken to reach 1 million users



Statista



VS



~100 trillion parameters
~20W energy consumption
\$12.5M (NZTA valuation)

On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?

Emily M. Bender*
ebender@uw.edu
University of Washington
Seattle, WA, USA

Angelina McMillan-Major
aymm@uw.edu
University of Washington
Seattle, WA, USA

Timnit Gebru*
timnit@blackinai.org
Black in AI
Palo Alto, CA, USA

Shmargaret Shmitchell
shmargaret.shmitchell@gmail.com
The Aether

ABSTRACT

The past 3 years of work in NLP have been characterized by the development and deployment of ever larger language models, especially for English. BERT, its variants, GPT-2/3, and others, most recently Switch-C, have pushed the boundaries of the possible both through architectural innovations and through sheer size. Using

alone, we have seen the emergence of BERT and its variants [39, 70, 74, 113, 146], GPT-2 [106], T-NLG [112], GPT-3 [25], and most recently Switch-C [43], with institutions seemingly competing to produce ever larger LMs. While investigating properties of LMs and how they change with size holds scientific interest, and large LMs have shown improvements on various tasks (§2), we ask whether



DECEMBER 19, 20

AI

 Reuters

New York Times fake ChatGPT

By Sara Merken

June 26, 2023 8:28 PM



Home > Tech

Air Canada loses court case after fake policies to a customer

The airline argued that the chatbot

By [Chase DiBenedetto](#)

BBC

Glue pizza and eat rocks: Google AI search errors go viral

25 May 2024

Liv McMahon
Technology reporter

Zoe Kleinman
Technology editor



Privacy Commissioner
Te Mana Mātāpono Matatapu

AI and Privacy: Back to the Future
13 May 2025

PG 8

Inc.

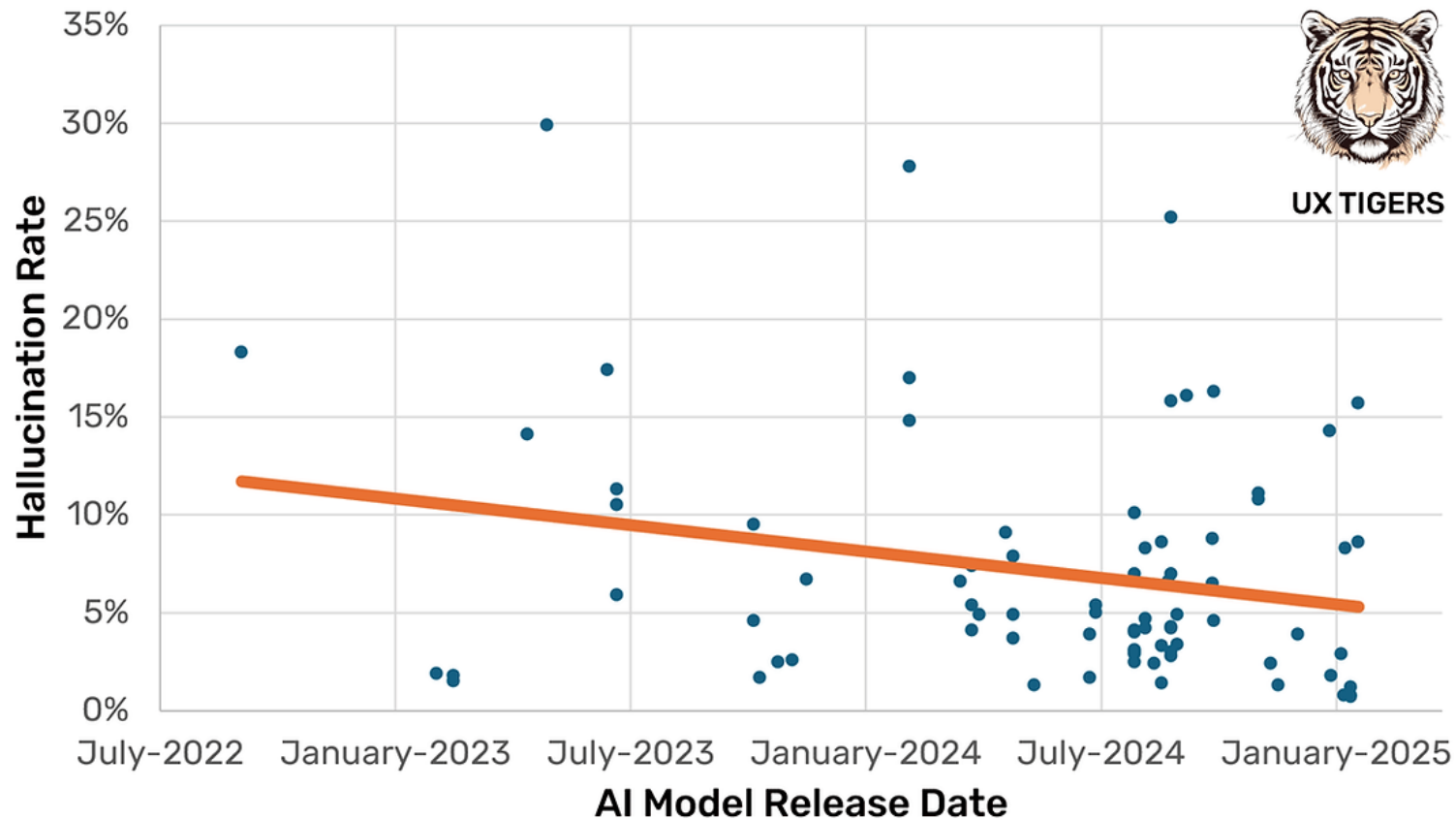
TECHNOLOGY

How Many R's in 'Strawberry'? This AI Doesn't Know

Though this very powerful technology remains full of promise, a recently discovered glitch shows AI is imperfect, so keep double-checking its results.

BY KIT EATON @KITEATON

AUG 28, 2024



Knowledge

Futurism

PANTS ON FIRE

MAR 1, 9:00 AM EST by NOOR AL-SIBAI

OpenAI Admits That Its New Model Still Hallucinates More Than a Third of the Time

Why is a company whose products can't tell the truth valued at
hundreds of billions of dollars?

/ Artificial Intelligence / AI Hallucinations / Gpt45 / Lims

Rease



Man files complaint after ChatGPT said he killed his children

22 March 2025

Imran Rahman-Jones
Technology reporter

penalty in
complexities involved in family



AI and automation |

57% of enterprise employees input confidential data into AI tools, survey reveals

A TELUS Digital Experience survey found 68% of employees use personal AI accounts for work instead of company-approved platforms.

Swagath Bandhakavi February 27, 2025

2024 Edelman Trust Barometer:

“52% of New Zealanders reject AI as a significant innovation”

KPMG 2025 Survey:

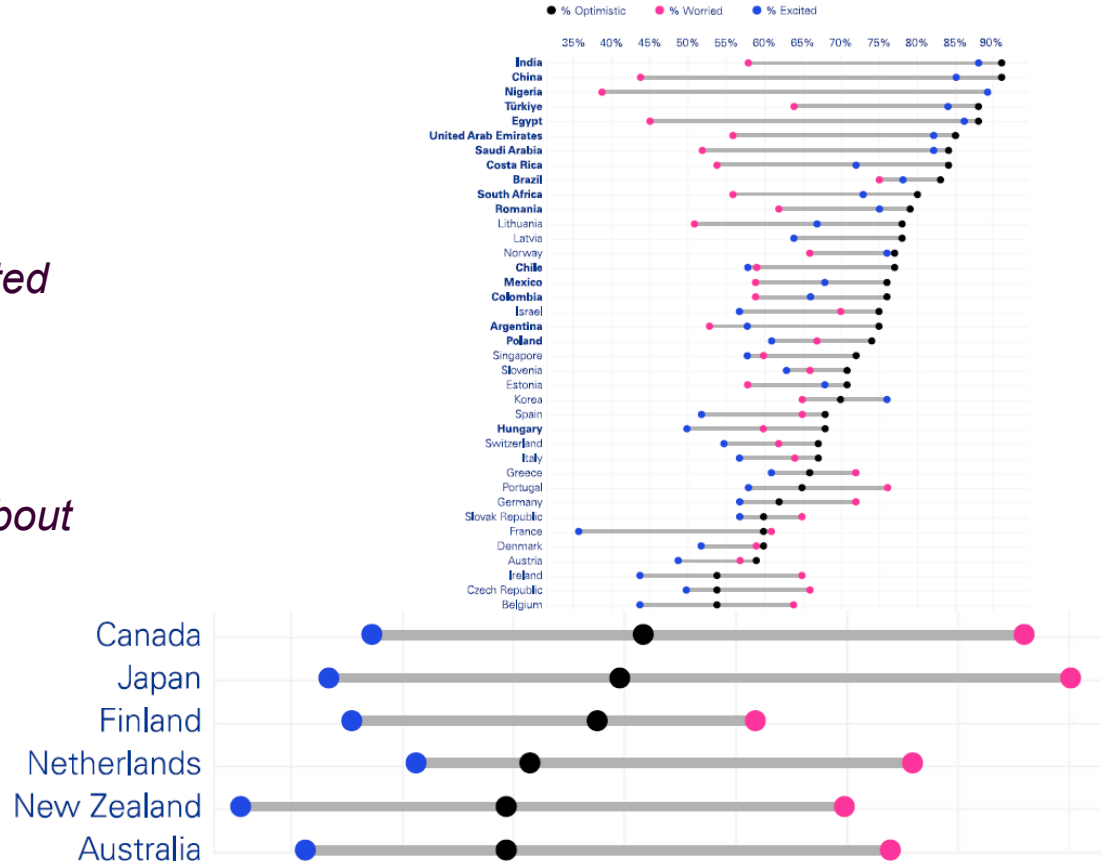
“Only 34% of New Zealanders are excited about AI, while 60% are worried”

InternetNZ 2025 Survey:

“68% of New Zealanders are worried about the malicious use of AI and the lack of regulation surrounding it”

“a light-touch, proportionate and risk-based approach to AI regulation”

Figure 15: Emotions toward AI across countries



Thinking about privacy when **building and using** AI tools

Artificial intelligence and the Information Privacy Principles

September 2023

**The Privacy Act
still applies!**

Legal requirements
are tech neutral...

...but understanding
privacy and the tech
helps with both!

AI tools and privacy

Input

What goes in?

Training data

???

(Can processing be understood / audited?)

(Can we access or correct info about us?)

Output

What comes out?

Text, images, voice

Categories (target ads)

AI



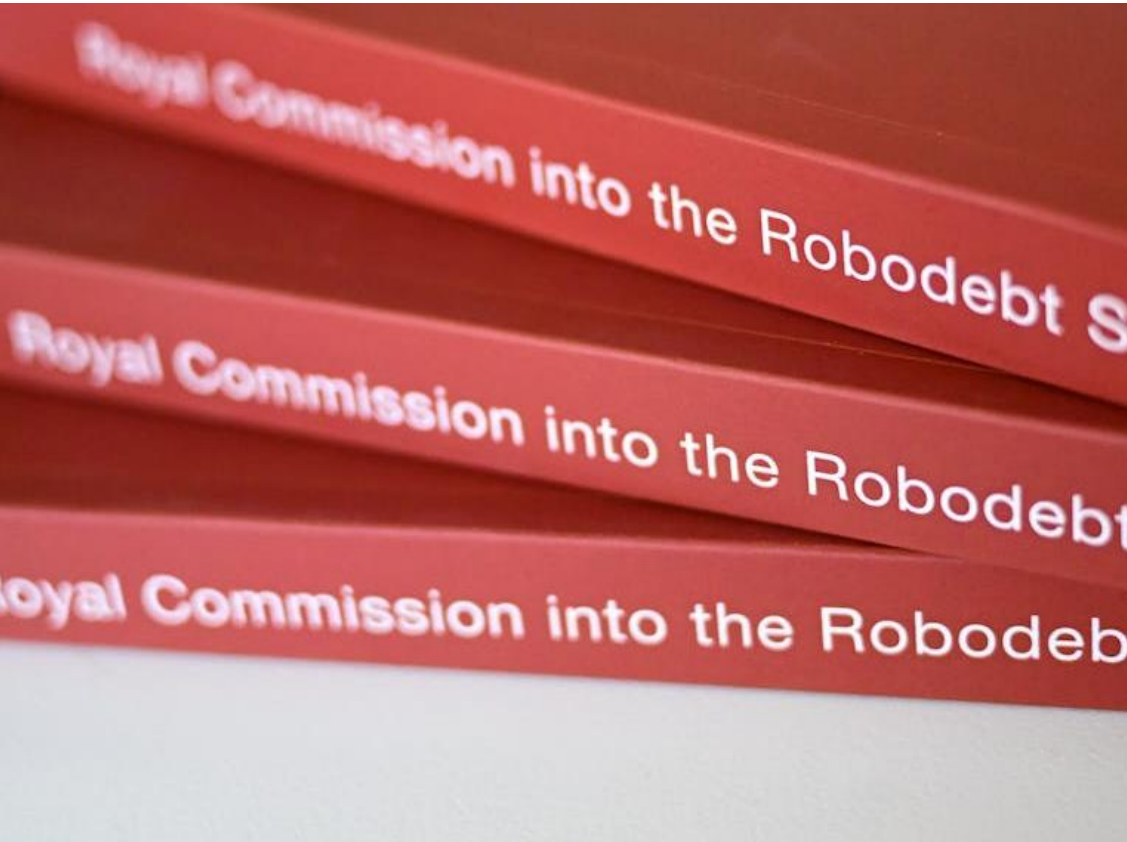
Assess Impact



Quebec Bridge 1907



Robodebt (AU)



Horizon (UK)



HORIZON SCANDAL INQUIRY

Fujitsu boss: We knew right from start about Post Office IT problem

Astonishing admission from top executive that firm was aware of 'bugs, errors and defects' for nearly two decades – but evidence was withheld during prosecutions of postmasters

ZOE GRUNEWALD

Fujitsu knew of defects in the

bugs and errors in the faulty accounting system were known about "right from the

false accounting – which he described as "shameful" and "appalling". Fujitsu now faces

A COMPUTER

CAN NEVER BE HELD ACCOUNTABLE

THEREFORE A COMPUTER MUST NEVER

MAKE A MANAGEMENT DECISION

AI tools and privacy

Automation

Computers controlling stuff (eg thermostat)

“Computer says no”

Algorithms

Computers putting stuff in categories

“Computer says I know your type”

“Generative AI” tools

Computers with output that feels meaningful (eg text, images, voice)

“Computer talks too much!”

Big focus on chatbots

Welcome to

EEEEEE	LL	IIII	ZZZZZZ	AAAAA
EE	LL	II	ZZ	AA AA
EEEEEE	LL	II	ZZZ	AAAAAAA
EE	LL	II	ZZ	AA AA
EEEEEE	LLLLLL	IIII	ZZZZZZ	AA AA

Eliza is a mock Rogerian psychotherapist.

The original program was described by Joseph Weizenbaum in 1966.

This implementation by Norbert Landsteiner 2005.

ELIZA: Is something troubling you ?

YOU: Men are all alike.

ELIZA: What is the connection, do you suppose ?

YOU: They're always bugging us about something or other.

ELIZA: Can you think of a specific example ?

YOU: Well, my boyfriend made me come here.

ELIZA: Is it important to you that your boyfriend made you come here ?

YOU: He says I'm depressed much of the time.

ELIZA: I am sorry to hear that you are depressed.

YOU: It's true. I am unhappy.

ELIZA: Can you explain what made you unhappy ?

YOU:

Privacy Act 2020: some key ideas

Agency

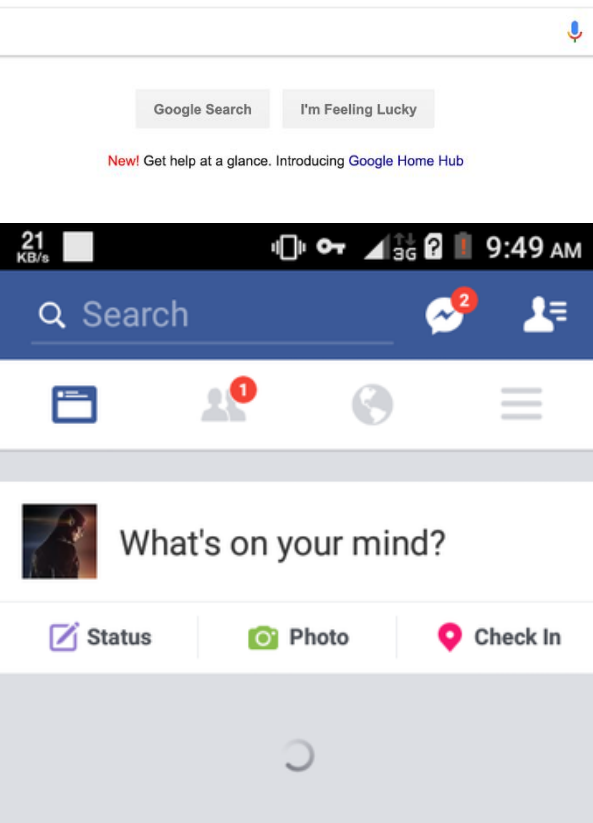
The organisation or person holding info

Personal Information

Information about an identifiable individual

Purpose

Why you collect it!



Algorithms

Big data: combining and reusing data (what **purpose** allows for this?)

Processing: is it fair and accurate???

Outputs: linking of data may lead to new info about people (and leaks)



Information Privacy Principles

IPP 1 – purpose for collection

IPP 2 – source

IPP 3 – transparency (IPP3A)

IPP 4 – fair and reasonable collection

IPP 5 – security

IPP 6 – access

IPP 7 – correction

IPP 8 – accuracy

IPP 9 – retention

IPP 10 – use

IPP 11 – disclosure

IPP 12 – overseas disclosure

IPP 13 – unique identifiers

Collection

Use

Disclosure

AI tools: new ways to use information



1990s

Physical records
and ways of
moving data



2000 - 2020

Computers are
normal

People get online

More sensors and
more ways to share



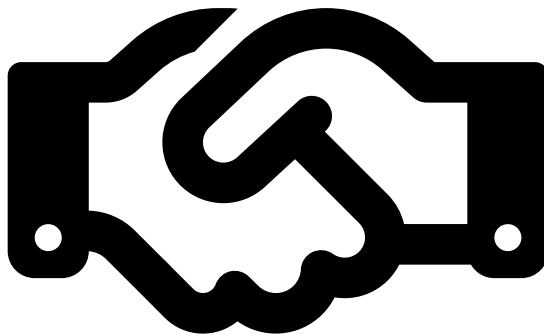
2020s

Transforming and
“reading” fuzzy
data sources

You can set up
computers to “read”
images, text, audio

“AI Agents”

Automation



Generative AI

Who is responsible during
development and
deployment of AI tools?

Opinion of the Board (Art. 64)



Opinion 28/2024 on certain data protection aspects related
to the processing of personal data in the context of AI
models

Adopted on 17 December 2024

European Data Protection Board

Ireland's DPA asked for an opinion about how personal information in **training data** affects **deployment** of AI models:

- When are they anonymous?
- When does legitimate interest apply?

EDPB decision 28/2024

Training

Mitigations in training:

Technical measures to limit PI and facilitate rights (eg erasure)

???

Is it anonymous after training?

Assess the risk of getting personal information out!

If it is anonymous, document it!

Deployment

Does personal info in training data affect deployment?

Anonymous? OK!

Otherwise? Assess Impact!

AI



Assess Impact

Questions?

Thank you!



Privacy Commissioner
Te Mana Mātāpono Matatapu