PCPD HK

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Addressing Privacy Risks of AI: Experience from Hong Kong

"Enhancing Personal Data Protection in the Age of Artificial Intelligence"
Programme on Artificial Intelligence and the Law, The University of Hong Kong

10 January 2024

Ada CHUNG Lai-ling

Privacy Commissioner for Personal Data, Hong Kong, China

Local Context

Hong Kong embraces AI

HK is keen to grow its AI industry

AI as a focus of HK's new **industrialisation**

Building an AI **supercomputing centre**

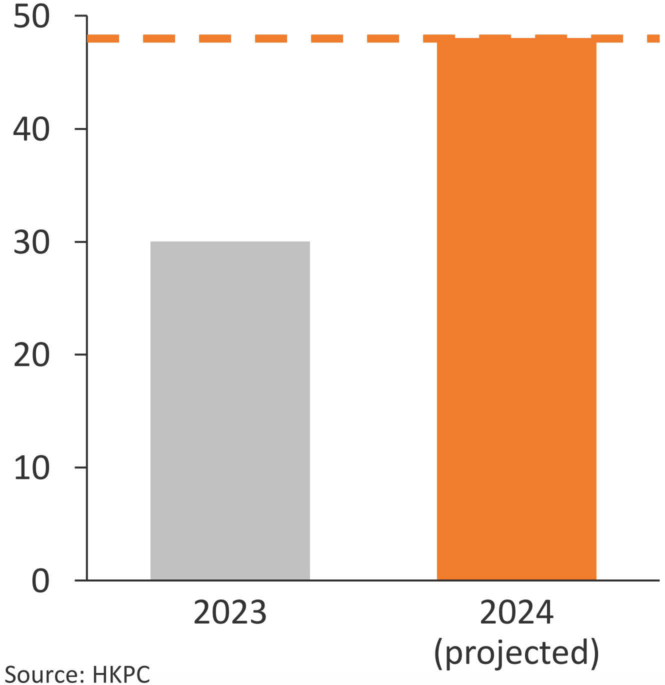
14 research labs under AIR@InnoHK

Access to **mainland and international data** as HK's appeal

Businesses keen to adopt AI; nearly ½ to use by 2024

AI Adoption Rate

Hong Kong, 2023-24, %

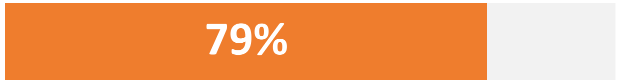


Source: HKPC

Individuals have used AI in work or life

Use of generative AI

Hong Kong youth, age 15-34

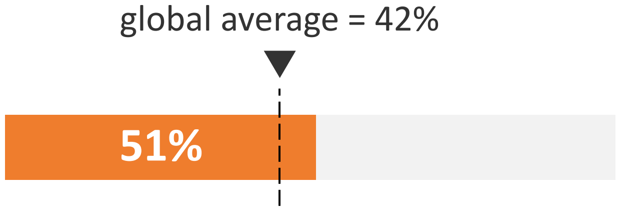


Have used generative AI before

Source: Youth I.D.E.A.S.

View towards AI Adoption

Hong Kong employees, 2023



Positive view

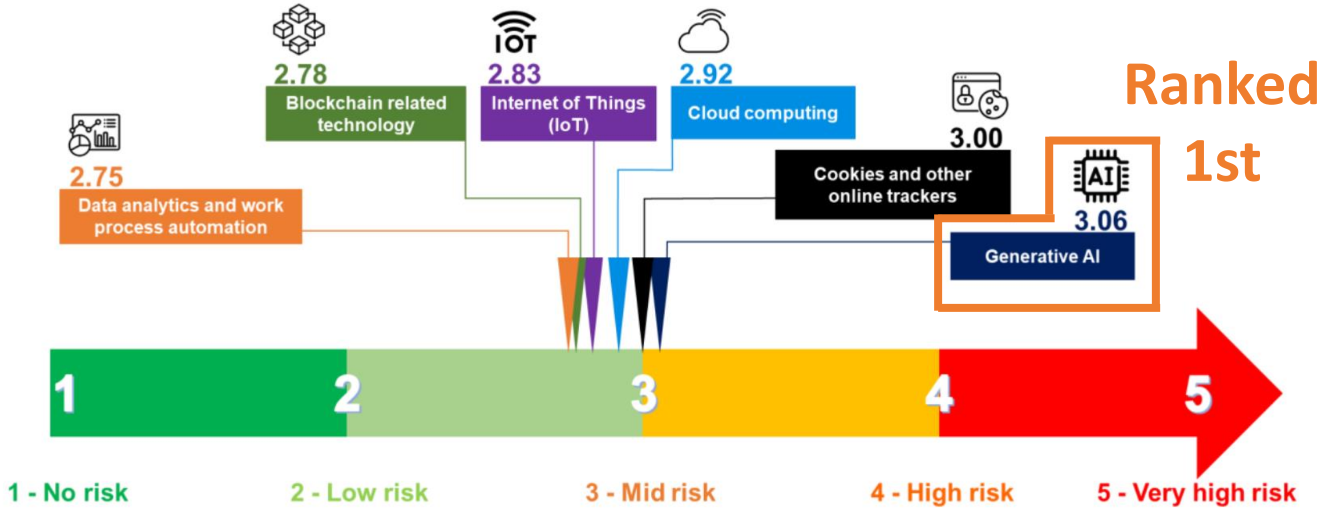
Source: CDO Trends

Challenges

Stakeholders worry about AI's privacy risks, despite awareness of the issue's importance

Businesses and society's concerns over AI's privacy risks

Enterprises saw genAI having the highest privacy risk among emerging technologies



Source: PCPD & HKPC

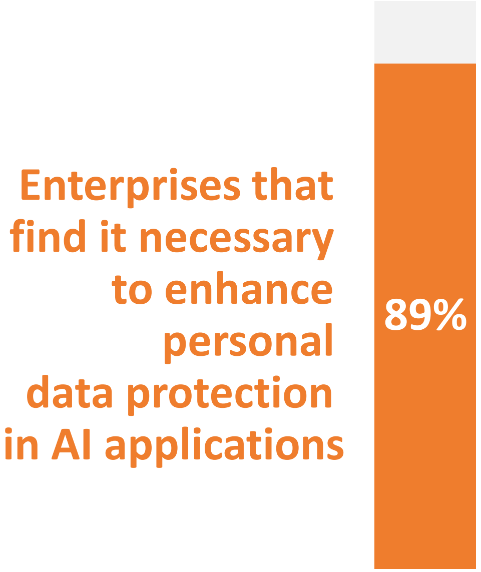
Examples of AI-powered crimes that took place in HK

Deepfake to deceive financial institutions

Blackmail on dating app with deepfake video

Despite awareness, knowledge gap exists

HK businesses aware of personal data protection



Source: Cisco reported in IT Pro

Knowledge is an issue

Experts say lack of knowledge hinders AI use

Source: HKPC

Risks

AI poses privacy risks

Risk	Explanation	Illustration
Excessive data collection	AI applications tend to collect and retain as many data as possible, which includes personal data	OpenAI reportedly scraped 300 billion words online to train ChatGPT
Use of data	AI models can be so advanced that people find it hard to understand how their personal data would be used	The “Black box” problem: users of AI are unable to know the internal logic of the AI systems
Identity re-identification	Some AI models may be able to re-identity individuals’ identities by collecting and matching data from different sources	A study shows that it is possible to identify 93% of people in dataset with 60mn people using 4 pieces of data
Data accuracy	Training AI models requires lots of data, and data quality & accuracy is an issue	AI may make incorrect analysis because of inaccurate data, which hampers decision-making

Hong Kong’s Regulatory Regime

PCPD has published guidance to help facilitate ethical use and development of AI

Despite a lack of overarching regime governing AI, existing laws apply

Overarching regime?

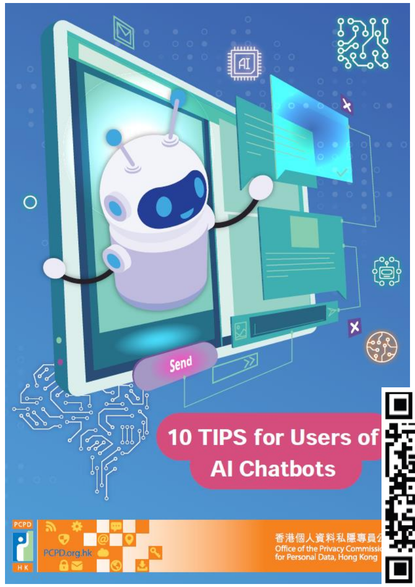
- **No overarching AI regulatory regime** in Hong Kong
- Government would keep an **open mind** and **closely monitor the development of AI**

Existing laws on areas relevant to AI include:

- Personal Data (Privacy) Ordinance (“PDPO”)
- Anti-discrimination
- Intellectual property
- Others …

PCPD facilitates ethical development and use of AI & compliance with PDPO with …

Guidance on Ethical Development and Use of AI (Aug 2021)



10 Tips for Users of AI Chatbots (Sep 2023)

AI Guidance

The three components

A

3 Data Stewardship Values

1. Being Respectful

2. Being Beneficial

3. Being Fair

B

7 Ethical Principles for AI

1. Accountability

2. Human Oversight

3. Transparency & Interpretability

4. Data Privacy

5. Fairness

6. Beneficial AI

7. Reliability, Robustness & Security

C

4-Step Practice Guide

1. ESTABLISH
AI Strategy & Governance

2. CONDUCT
Risk Assessment and Human Oversight

3. EXECUTE
Development of AI Models & Management of AI Systems

4. FOSTER
Communication with Stakeholders

AI Chatbot Users

The 10 tips help users protect their personal data privacy while enjoying AI's benefits

Send
10 TIPS for Users of AI Chatbots
PCPD.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Protecting Personal Data Privacy

Before registration / use

1. **Read the Privacy Policy, the Terms of Use** and other relevant data **handling policies**

2. **Beware of fake apps** and **phishing websites** posing as known AI chatbots

3. **Adjust** the settings to **opt-out of sharing chat history** (if available)

During interaction with AI chatbots

4. **Refrain from sharing** your own personal data and others' personal data

5. **Submit** a **correction or removal request**, if necessary

6. **Guard against cybersecurity threats**

7. **Delete outdated conversations** from chat history

Safe & Responsible Use

8. **Be cautious about using the information provided by AI chatbots**

9. **Refrain from sharing confidential information and files**

10. **Teachers / parents should provide guidance to students** when they interact with AI chatbots

Quote

Get the best by avoiding the worst

> Success in creating AI could be the biggest event in the history of our civilisation. But it could also be the last, unless we learn how to avoid the risks

— Stephen Hawking