2024

人工智慧（AI）技術發展的社會成本：台灣人民對個資保護的認知與全球個資保護法的發展

報告人：張佑宗

臺灣大學政治學系教授
臺灣大學社科院東亞民主研究中心主任
臺灣大學公共政策與法律中心主任

2024.3.27

研究緣起：AI for Bad

Crawford（2021）在《Atlas of AI》（比喻AI是一肩扛起世界的罪人）這本書中指出，AI常被視為一種無形技術，但其實它有著重大的物質基礎。例如AI技術背後的環境成本，包括大量數據中心的能源消耗，以及所需硬件的資源開採。AI也影響勞動市場，特別是在自動化對低技能工作的影響。Crawford同時指出，數據標註等工作往往由低薪工人在貧窮國家完成，加深全球分配不平等。更重要的，資料與數據是目前人工智慧技術的核心。Crawford分析個人數據的收集及其對隱私權影響，也討論AI技術如何被用於監視和社會控制。所有「公共」的數位資料--包含所有可能其實是屬於私領域的資訊，都被用為AI模型的訓練資料集。這些資料包含大量人像照、對話紀錄、街頭攝影機影像等，都被用以做為機器學習辨識人像、情緒、物品與自然語言處理(natural language processing) 的訓練基礎。

研究緣起

研究計畫：臺灣人工智慧(AI)技術發展的社會成本與治理準則

能源短缺

勞動市場供需

AI與教育

AI與社會分配

AI與個人隱私

（張佑宗、紅貞玲、蘇翊豪）

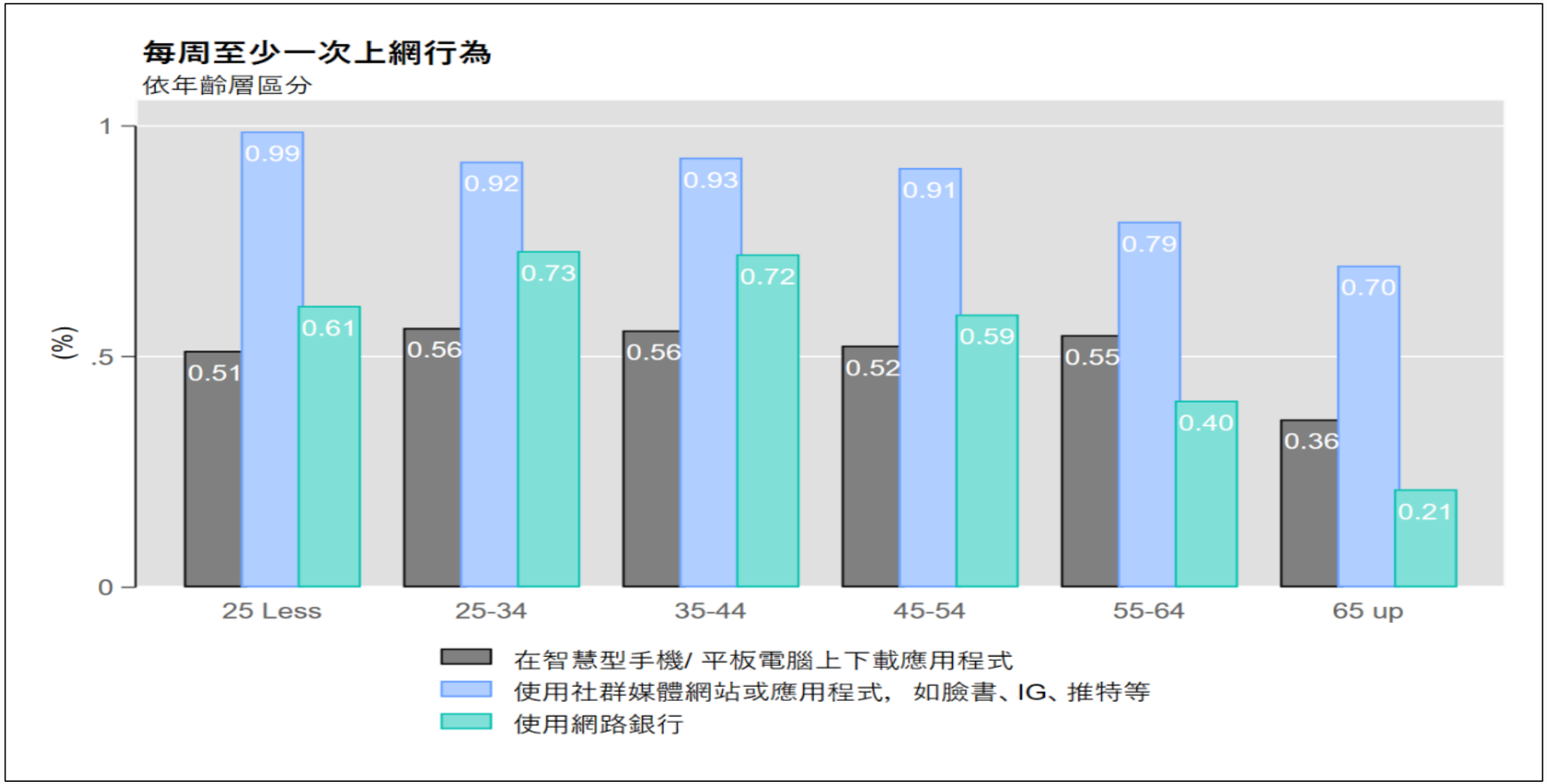
問題意識

被大量用以增進AI準確度的資料，究竟與個人私領域有多少重疊？有多少個人日常的影像、對談甚至是聲音，在無形之中被用來作為AI的訓練資料，甚至可能有個人隱私遭外洩、濫用甚是損害個人權益的可能？台灣《個人資料保護法》在2010年公布生效，其後經過多次的修訂，但台灣民眾是否有充分了解個人資料外洩（data leakage）的風險？是否具備相應的資安風險識知，並理解各種法律面與實務面的保障措施？我們日常所使用的網路與社群媒體服務，對你我日常生活中生產的資訊又能盡到多少保護的責任，或僅僅是用完即棄？

研究目的

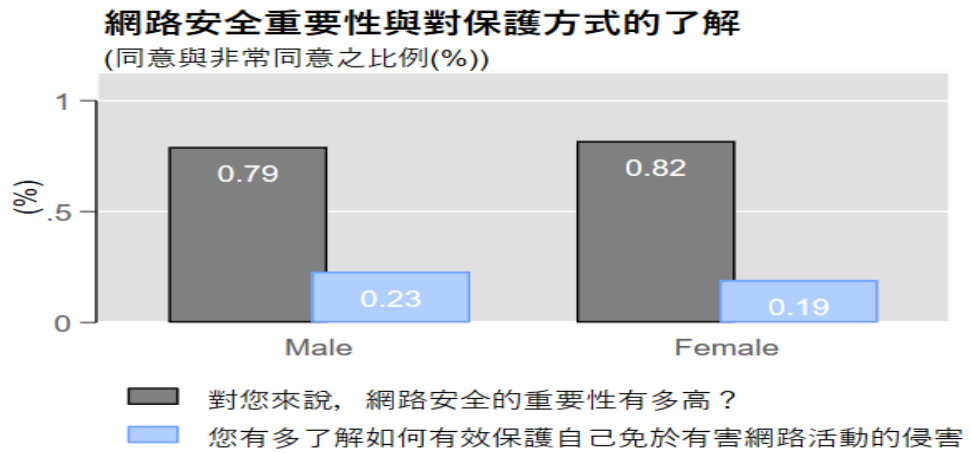
本文以這三年來中技社補助的研究計畫研究成果（計畫名稱：臺灣人工智慧(AI)技術發展的社會成本與治理準則）為基礎，主要使用英國數位、文化、媒體與運動部（Department for Digital, Culture, Media & Sport），以及國家網路安全中心（National Cyber Security Centre），在2019至2021年所進行的全民網路安全調查（UK Cyber Security Breaches Survey – General Public）問卷為核心，在2022年及2023年完成兩次民意調查，分析台灣人民對保護個人資料隱私的認知有多深？其次，台灣對個資保護的法治基礎足不足夠？本文將分析歐盟及美國對個人資料隱私保護的法治基礎，以此做為台灣未來修訂《個人資料保護法》政策的參考依據。

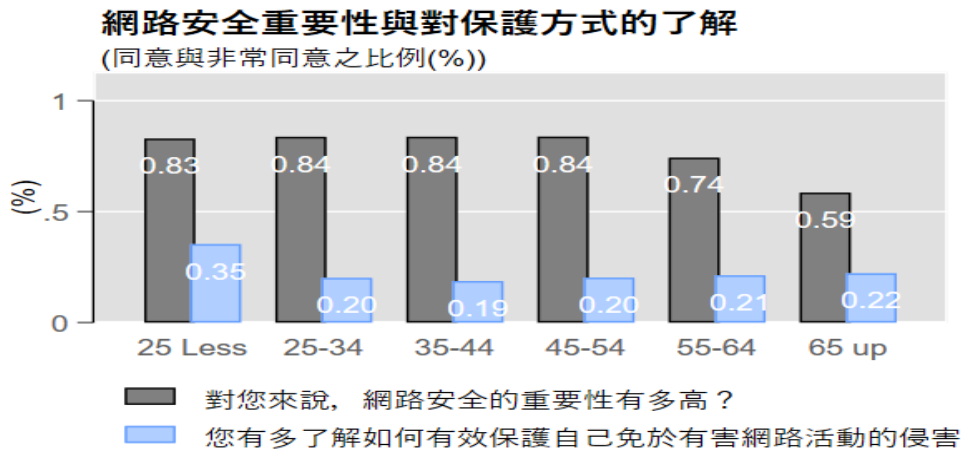
台灣民眾的上網行為

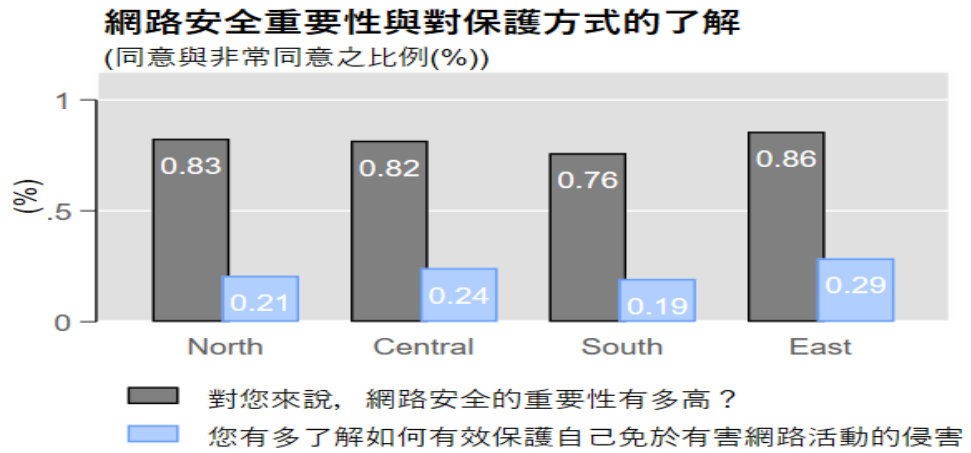


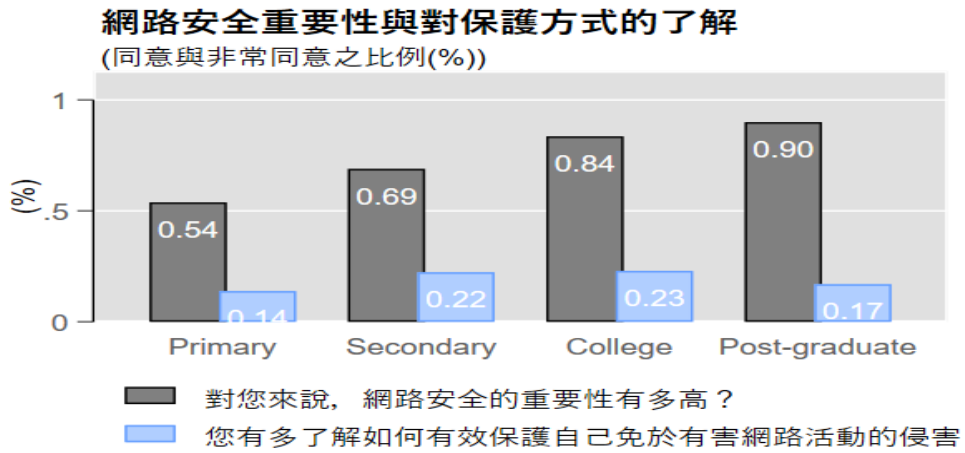
資料來源：張佑宗，臺灣全民網路安全調查（2022）。

對上網安全的重視



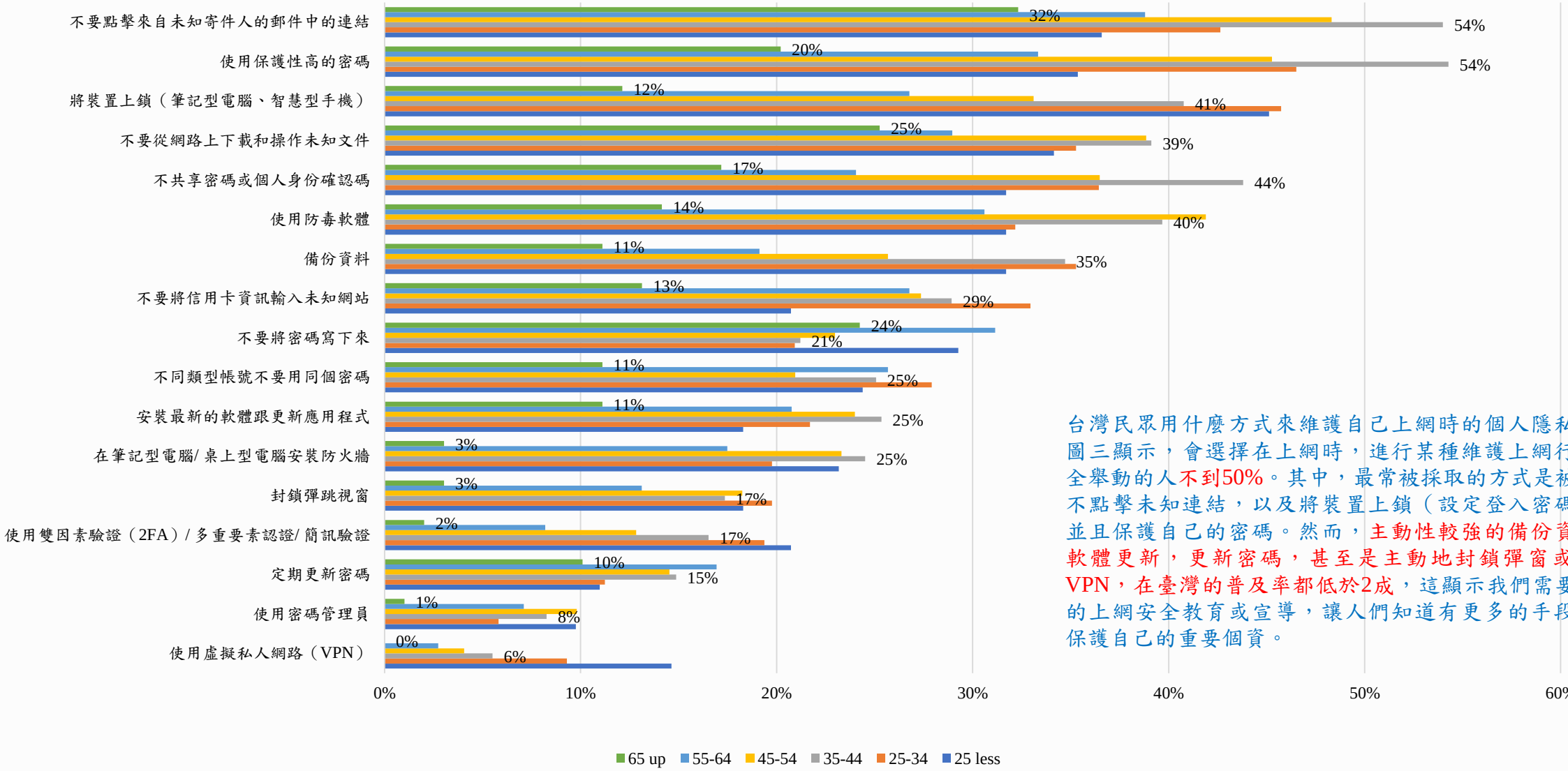






資料來源：張佑宗，臺灣全民網路安全調查（2022）。

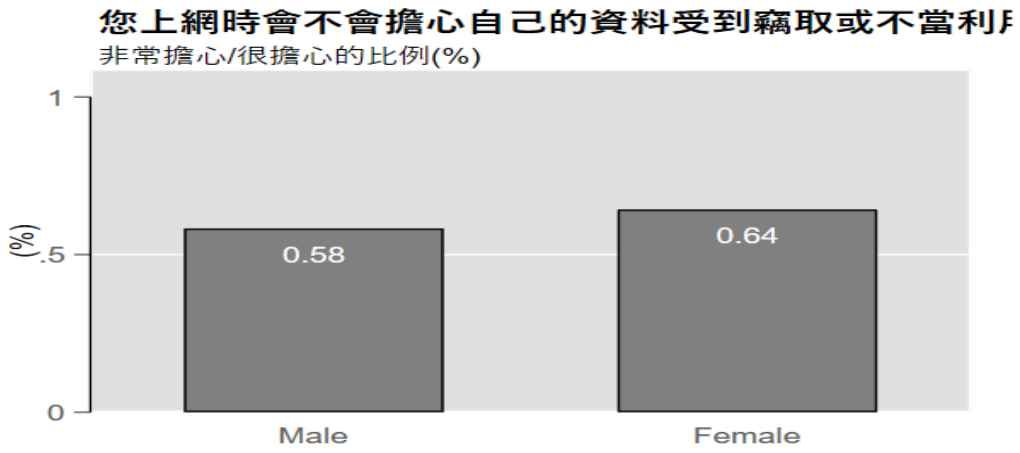
保護安全上網的行為模式

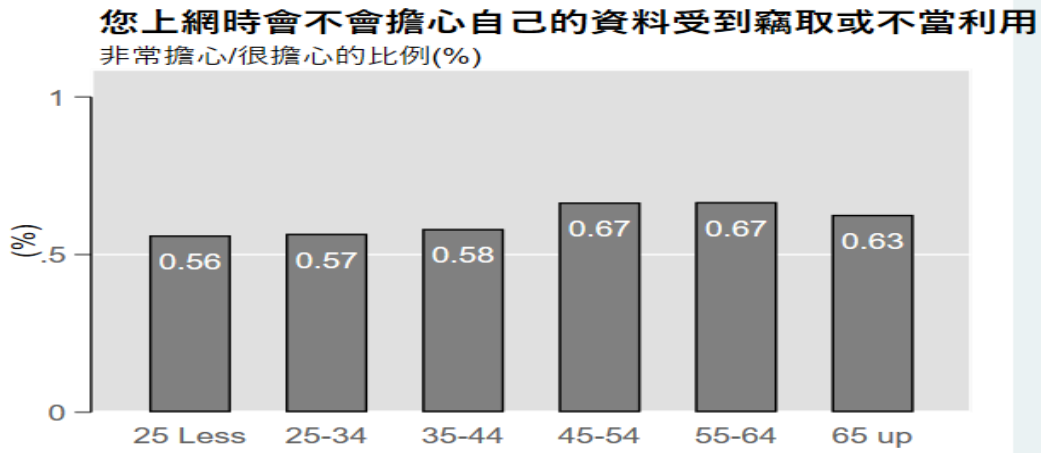


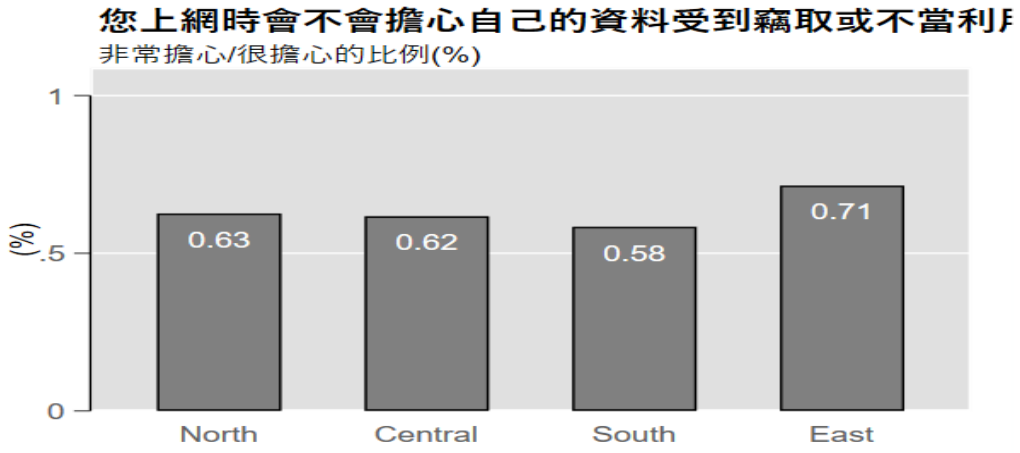
台灣民眾用什麼方式來維護自己上網時的個人隱私呢？圖三顯示，會選擇在上網時，進行某種維護上網行為安全舉動的人不到50%。其中，最常被採取的方式是被動地不點擊未知連結，以及將裝置上鎖（設定登入密碼），並且保護自己的密碼。然而，主動性較強的備份資料，軟體更新，更新密碼，甚至是主動地封鎖彈窗或使用VPN，在臺灣的普及率都低於2成，這顯示我們需要更多的上網安全教育或宣導，讓人們知道有更多的手段可以保護自己的重要個資。

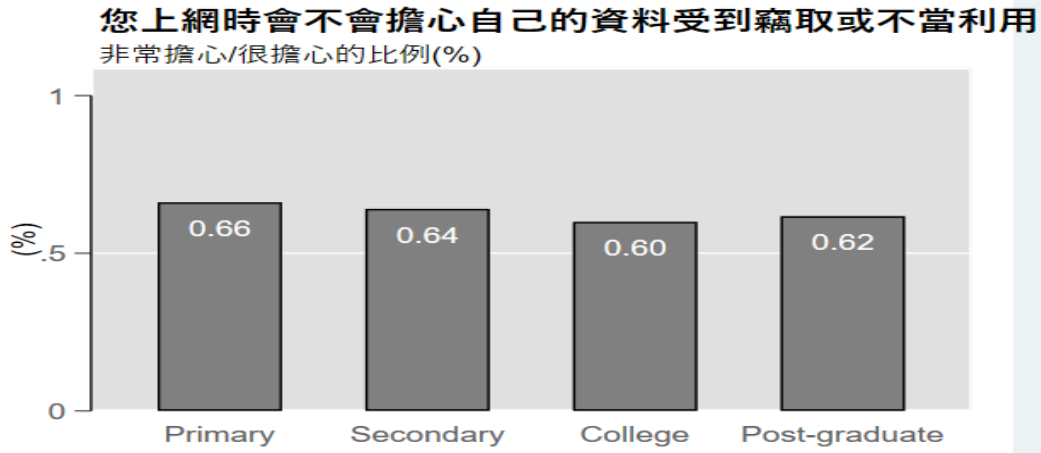
資料來源：張佑宗，臺灣全民網路安全調查（2022）。

擔心個人資料被盜竊的風險



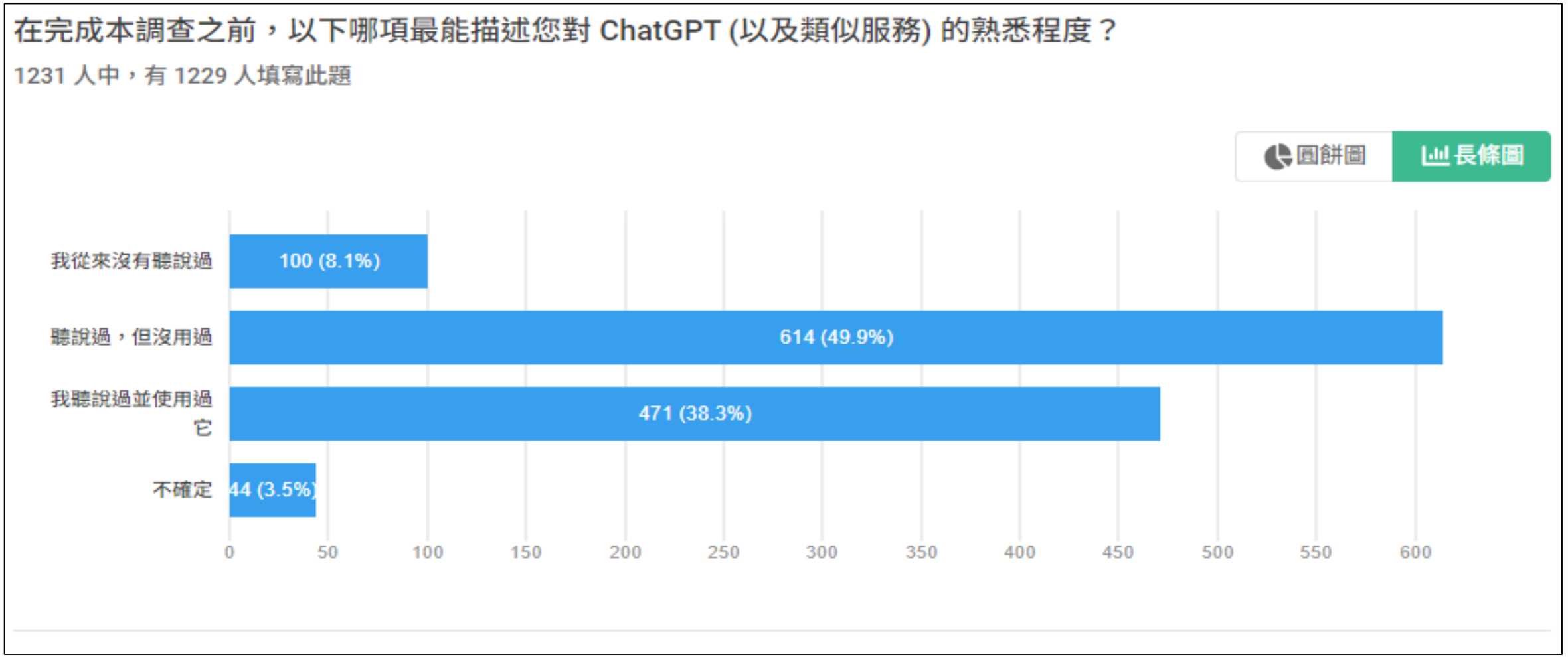






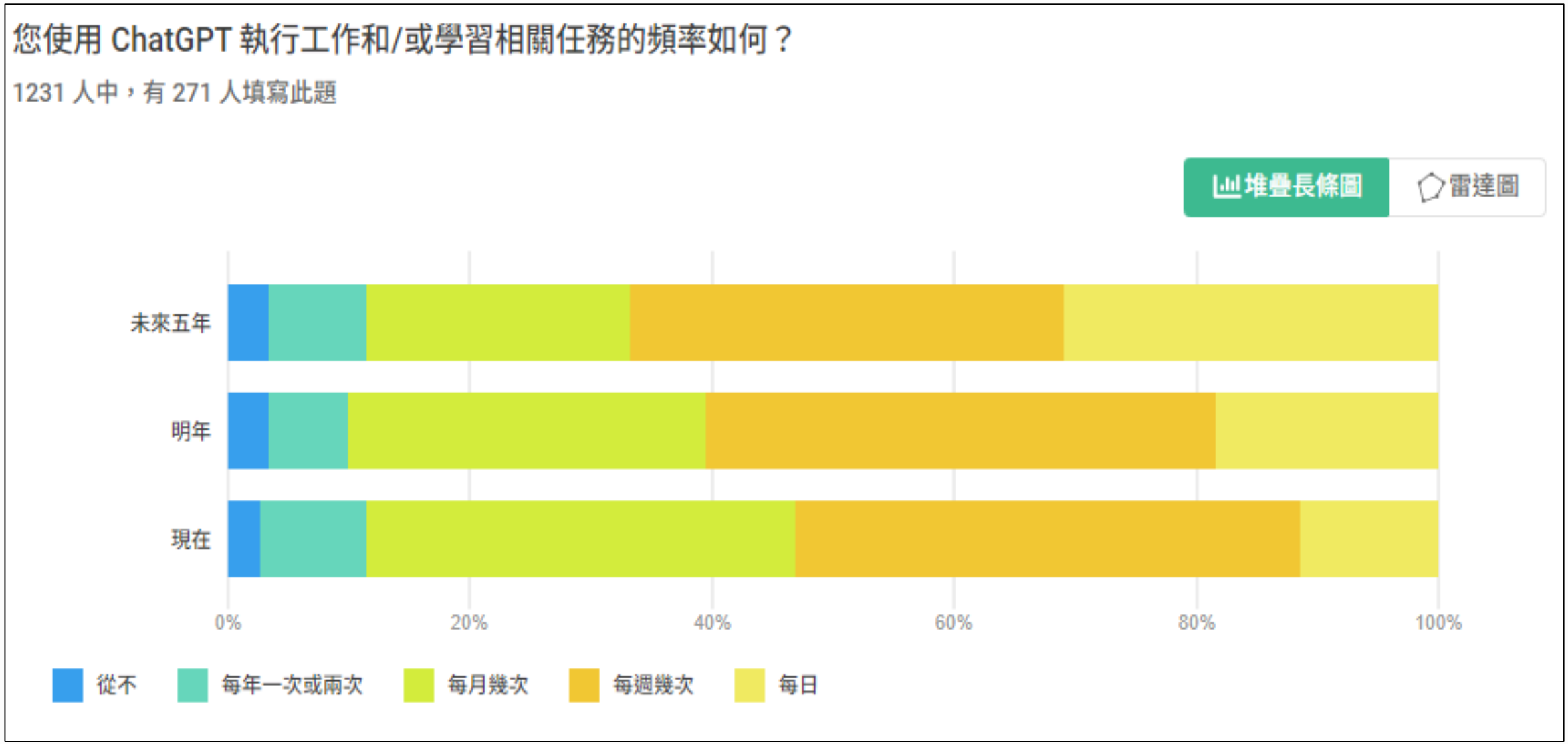
資料來源：張佑宗，臺灣全民網路安全調查（2022）。

對ChatGPT熟悉的程度



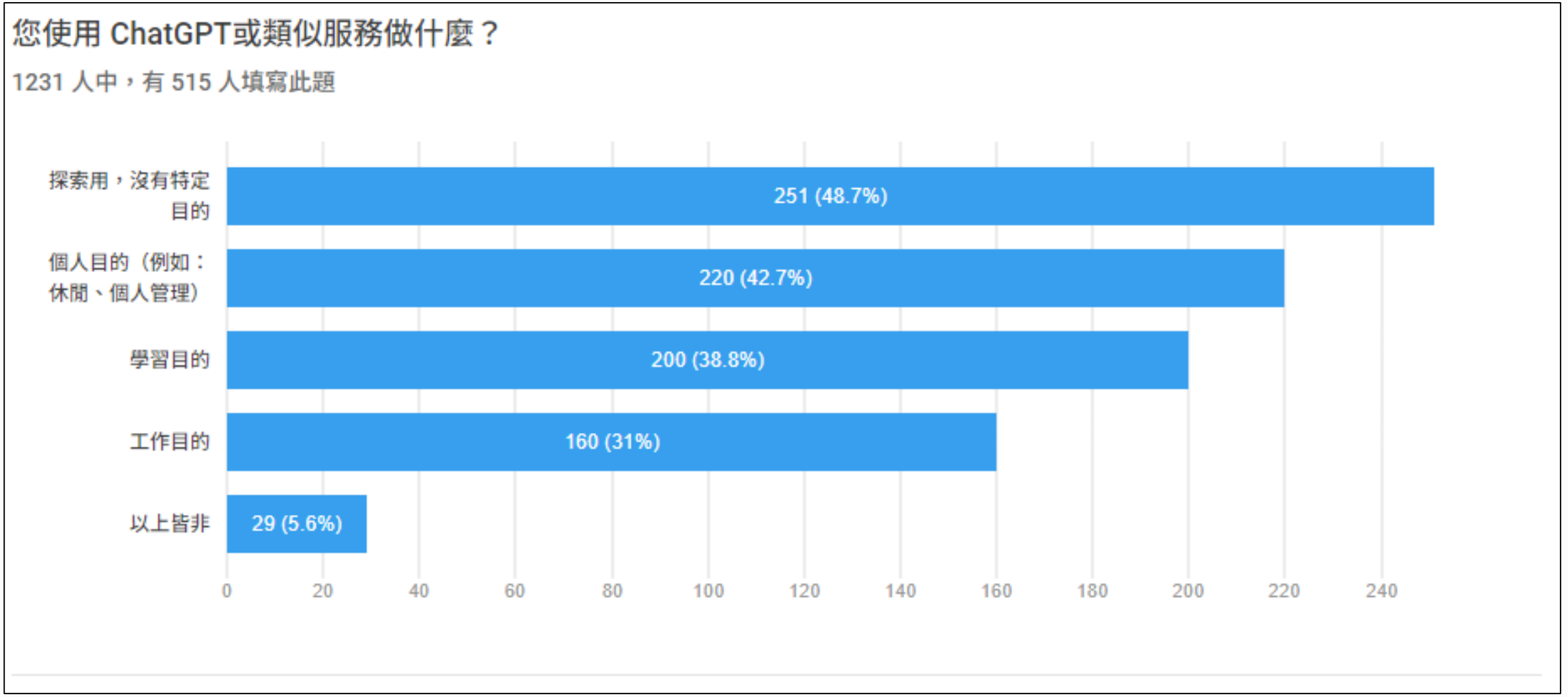
資料來源：張佑宗，臺灣全民網路安全調查（2022）。

未來使用ChatGPT的狀況



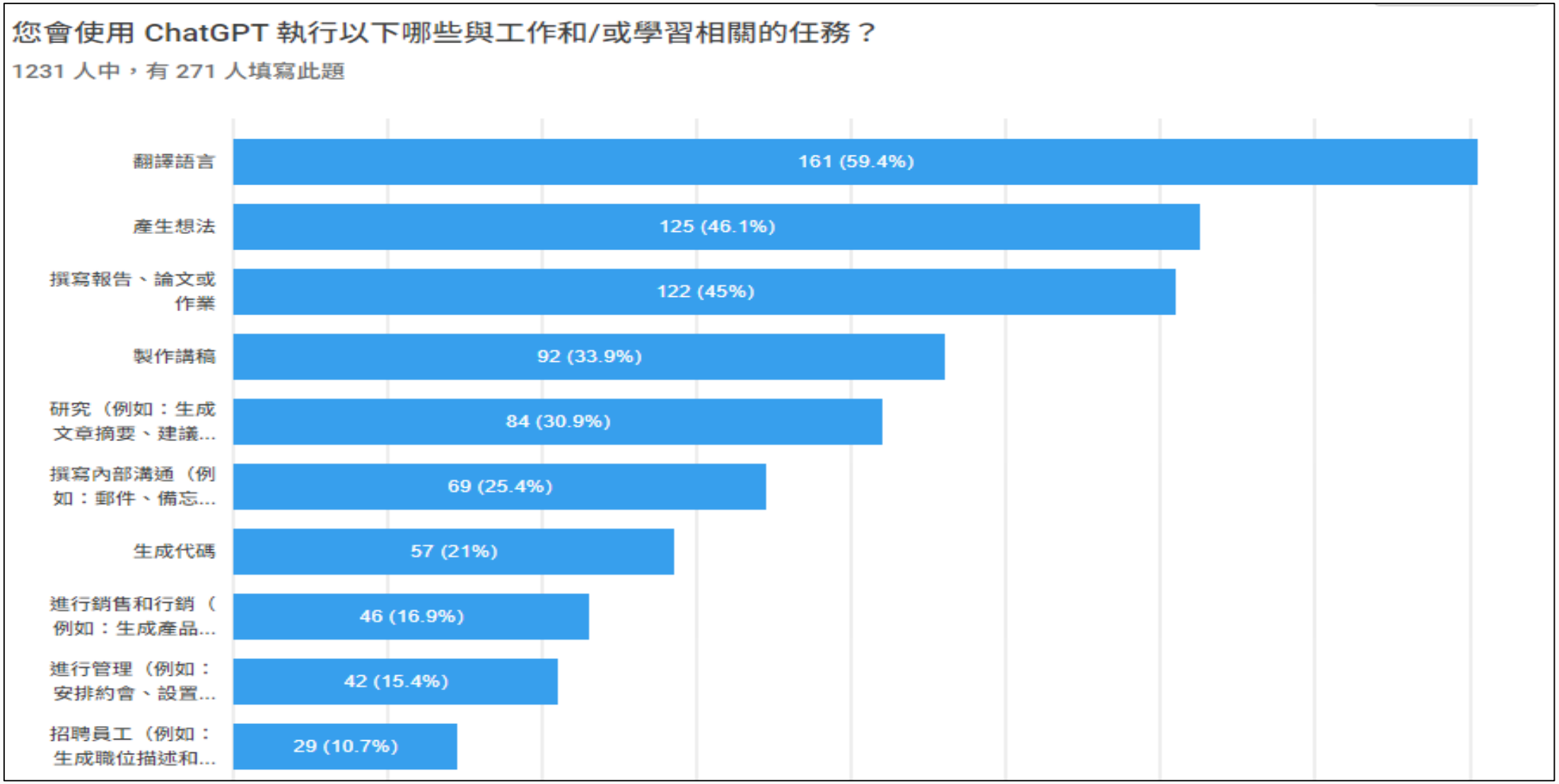
資料來源：張佑宗，臺灣全民網路安全調查（2023）。

使用ChatGPT的目的



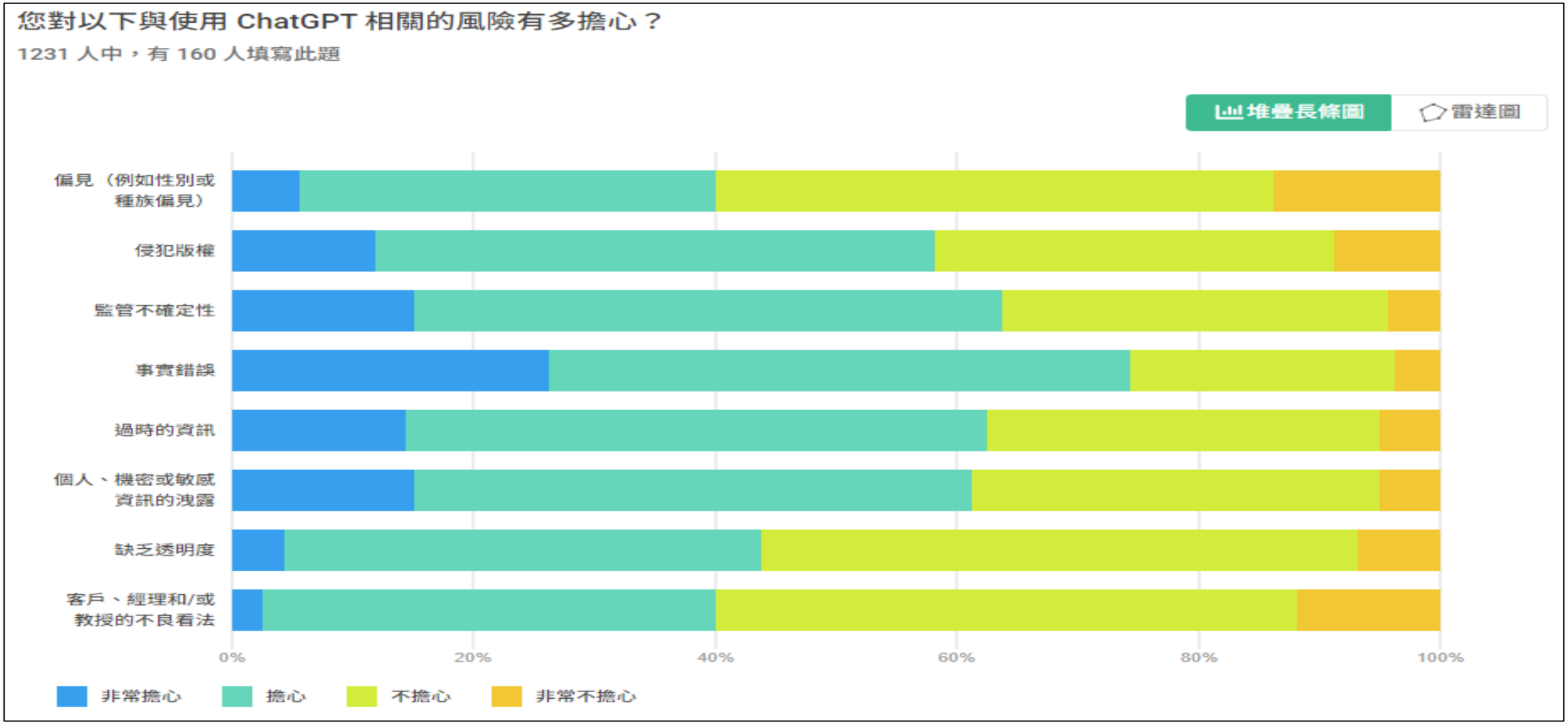
資料來源：張佑宗，臺灣全民網路安全調查（2023）。

使用ChatGPT的目的



資料來源：張佑宗，臺灣全民網路安全調查（2023）。

擔心使用ChatGPT的風險



資料來源：張佑宗，臺灣全民網路安全調查（2023）。

歐美國家對個資保障的法治基礎

針對個人隱私保護，主要見於個資保護的相關法令，此類型法令由來已久，但因為數位科技及人工智慧等技術推陳出新，因此相關資料法案及保護法規也持續修改及新訂。以下介紹歐盟的《一般資料保護規則》，以及與資料相關的資料法、資料治理法。美國的資料法制相對發展得較慢，先以20018《加州消費者隱私保護法》率全美之先，以及2020年整合了「美國消費者資料保護法」（U.S. Consumer Data Protection Act）、「資訊篩選器透明法」（Filter Bubble Transparency Act）、「降低線上使用者詐騙經驗法」（Deceptive Experiences To Online Users Reduction Act），關於資料隱私保護的內容整合而成為「安全資料法」。

歐美國家對個資保障的法治基礎

一、歐盟於2018年實行《一般資料保護規則》（General Data Protection Regulation, GDPR），作為取代1995年發布之《資料保護指令》（Data Protection Directive），成為歐盟個人資料保護之主要規範。

本規則對於適用主客體與地域之範圍上有明確規範，主體分別為控管者（controller），指單獨或與他人共同決定個人資料處理之目的與方法之自然人或法人、公務機關、局處或其他機構；以及處理者（processor），指代控管者處理個人資料之自然人或法人、公務機關、局處或其他機構。客體適用範圍為凡屬於自然人或法人所為之「自動化之個人資料處理」及「儲存於檔案系統中之非自動化個人資料處理」之個人資料處理活動皆受規範。

歐盟國家對個資保障的法治基礎

本規則在個人資料保護歐洲化的進程中，為首個統一歐盟國家個資保護立法的先驅，賦予資料者主體以下權利：

1.接近使用權：　　資料主體對被蒐集之個資有容易、於合理之時間間隔行使接近使用的權利，以知悉並確認該處理之合法性。

2.被遺忘權（更正權及刪除權）：料主體應有修改或刪除其個人資料之權利。

3.資料可攜權：資料主體有權以有結構的、通常使用的、機器可讀的形式，接收其提供與控管者之資料，並有權將之傳輸給其他控管者。

4.拒絕權：資料主體於下列情形有權拒絕其個資處理。

歐盟國家對個資保障的法治基礎

資料控管者須遵守以下個資處理原則：

1.透明原則：個資控管者在處理個資時應符合合法、公正及透明等要件。控管者應向當事人公開個資處理之目的、所依據之法律、資料被儲存之期間等資訊；並應以簡明、透明、易懂且方便取得之格式，及清楚簡易之語言告知當事人有關個資處理之風險、規範、保護措施、司法救濟等相關權利。

2. 料控管者之處理應具合法性：處理係為符合公共利益執行職務或委託控管者行使公權力所必須者。

3.處理個資亦應經過當事人同意，同意指當事人就其個資處理給予具體肯定且自由形成、明確、受通份告知及非模糊之指示，如口頭或書面之聲明，單純沉默、預設選項為同意或不為表示不構成同意。當事人得隨時撤回同意，其方式應與給予同意一樣容易。

歐盟國家對個資保障的法治基礎

二、歐盟《資料法》草案（European Data Act）

歐盟於2020年為形塑歐洲「數位十年（Digital Decade）」，執委會發布數據戰略與人工智慧白皮書等規劃，旨在樹立歐洲數位資料治理之指引，以促進資料於歐盟境內流通，並預期在2050年前達到歐洲氣候中和之目標。根據此政策，歐盟已通過或研議以下政策與法律，包含：數位服務法（Digital Services Act, DSA）、數位市場法（Digital Markets Act, DMA）、. 歐洲晶片法（European Chips Act）、歐洲數位身分（European Digital Identity）、人工智慧相關（Artificial Intelligence）、歐洲資料戰略（European Data Strategy）、歐洲產業戰略（European industrial strategy）、歐洲防衛貢獻（Contributing to European Defence）、太空行動（Space）、歐盟-美國交易與技術議會（EU-US Trade and Technology Council）。其中歐洲資料戰略的主旨為使歐盟成為資料驅動社會的領導者，打造歐盟內的單一資料市場，讓資料流通於公民、企業、政府機關與研究者。

歐盟國家對個資保障的法治基礎

三、歐盟《資料治理法》草案（Data Governance Act）

《資料治理法》於2022年5月16日正式通過，2023年9月開始適用。與資料法Data Act同為歐盟歐洲資料戰略European Data Strategy的立法規劃。本法旨在增加對資料共享的信任、加強提高資料可用性的機制、克服資料再用的技術障礙等，以達成促進資料經濟目的。並支持與建立戰略性領域中的歐洲資料空間，包含私人與公眾，在衛生、環境、、能源、農業、交通、金融、製造、公共管理和技能等領域的資料使用。其中，歐盟提出「資料利他主義（data altruism）」，主張基於無償且係公益用途，資料主體得提供並允許他人使用其個資於研究等公益目的。

美國家對個資保障的法治基礎

美國對於經濟、科技、以及數據的管制措施，深受自由主義思維的影響，近年來卻一反常態，試圖在純然的戰略安全與完全的放任主義之間取得平衡點。以社群媒體和數據管制為例，在歐盟於2016年推行《一般資料保護規則》（*General Data Protection Regulation*；GDPR）的兩年後，美國加州也於2018年頒布《加州消費者隱私保護法》（*California Consumer Privacy Ac*，CCPA），雖然伊利諾州等各州紛紛制定類似規範，但並非每一個州都跟進效法，而聯邦層級的隱私保障法案迄今尚未過關。美國部分州政府與消費者也對臉書、谷歌、中國社群媒體抖音（TikTok，母公司字節跳動ByteDance）等公司提起集體訴訟。然而，法院體系做出若干起結論相悖的判決，伊利諾州與加州法院認同州政府對臉書等企業違反資料安全的看法，不過印第安那州法院卻駁回州檢查總長對抖音侵害兒童權利和資料安全的指控。

美國家對個資保障的法治基礎

在各州落實的隱私權法律之中，最接近歐盟GDPR保障水準的版本為2020年實施的《加州消費者隱私保護法》，隨後成為美國各州的隱私保障標竿（Voss & Houser, 2019）。在CCPA之後，科羅拉多州、維吉尼亞州等州陸續通過《隱私法》（*Colorado Privacy Act*，CPA）、《消費者資料保護法》（*Consumer Data Protection Act*，VCDPA）等法律，逐步賦予各州州內居民刪除權、更正權、選擇退出權等權利。

歐盟GDPR的規範密度與保障程度較高，而美國各州由於受到商業利益驅動的影響下，在盡可能降低對商業活動的衝擊前提下，制訂出上述對個資主體的保障措施。

美國家對個資保障的法治基礎

美國這些法規也增加資料主體發起抗議與訴訟的依據，以及提供法官判決的依據（受訪者A，2023）。加州地方法院在2022年與2023年的集體訴訟判決中，認定谷歌即使在用戶選擇無痕模式的狀況下，仍然藉由Chrome 瀏覽器追蹤用戶的數位足跡（Scarcella, 2023）。而臉書也在2022年同意支付50億美元的罰款，換取美國聯邦貿易委員會（Federal Trade Commission）終止對其涉及劍橋分析事件（Cambridge Analytica）的數據隱私調查行動（Ahn, 2022）。

除了美國社群媒體巨擘，中國社群媒體抖音也在伊利諾州付出慘痛代價。這起集體訴訟指控抖音透過推薦貼紙與濾鏡功能，蒐集用戶的性別、種族資訊，進行演算法訓練並傳送至中國的伺服器。歷經一年多的纏訟，抖音決定在2021年付出9,200萬美元的和解金額，並且同意不再記錄用戶的生物特徵、手機位置變化（Allyn, 2021）。

美國家對個資保障的法治基礎

美國各州對臉書、抖音等社群媒體違法蒐集個資的判決可知，美國聯邦主義與分權的影響之下，導致每個州的立法進度與執法狀況不同，進而出現大公司規避遵循的現象。比方說，社群媒體公司可以調整認定用戶的IP位置，轉移至規範密度以及執法能力較薄弱的州（陳柏良，2023；林昕璇，2023）。此外，美國不同政黨對於隱私管制之幅度，也有顯著差異。民主黨希望以加州的CCPA為範本，擴充隱私權的保障範圍並提升至聯邦立法層級；但共和黨認為這屬於總統的行政特權，應由總統組成調查委員會，如果調查結果成立，可直接以行政命令宣告全國統一的禁令或保障（陳柏良，2023）。針對抖音構成的資安疑慮，部分共和黨政治人物甚至有意強化中國威脅論或者地緣政治說帖，以便提高對中國產品的管制；箇中原因在於中國威脅論所碰到的國內阻礙力道比較小，而如果僅是一般層級的隱私保障論述，恐怕臉書等其他美國數位公司也會遊說、介入政策辯論與形成過程，不利於取得法案共識（陳柏良，2023；受訪者A，2023）。

歐美國家對個資保障的法治基礎

	GDPR	CCPA	VCDPA	CPA
適用區域	歐盟	加州	維吉尼亞州	科羅拉多州
個資保護模式	選擇同意（opt-in）	選擇退出（opt-out）	選擇退出	選擇退出
不在保障範圍內的資料	去識別化 充分假名化	去識別化	去識別化	去識別化
可公開取得的資料	仍屬於個資	不屬於個資	不屬於個資	不屬於個資

（Bloomberg Law, 2023）

結論

因人工智慧技術變化快速，各國在制訂硬法前大多以指引（guideline）或框架（framework）的形式引導部門立法。歐洲與美國之趨勢，亦是由歐盟各會員國及各州政府依各別區域情況制定規範，進一步帶動歐盟層次或聯邦政府層級的創新立法，尤其美國更重分散式立法。台灣對於人工智慧應用之規範，目前採取「先指引後法律」軟法先行之形式，與歐盟及美國的作法不謀而合，其目的在於透過軟法來減少對中小企業或新創的法遵成本，且在地方政府或企業若有值得參採的指引或立法，亦可能刺激中央政府訂立規範。在指引先行的模式下，台灣科技業與美國產業互動密切，更需注意美國立法動向。

結論

由於台灣在人工智慧技術與資料治理的政策發展上，尚未有長期的規劃，建議台灣採取政策型立法，先設立整體政策之主軸，並將可能涉及之相關議題一一列出，再參採美國部門式的分散立法，由對接產業端的各部會安排優先順序，並訂定立法計畫與執行期程，較能即時因應科技與產業環境的變遷。其中，可先從特定產業類別開始建構法制，如健康醫療、消費者保護等領域，來規範人工智慧與資料應用的開放及管制。

臺灣政府機關研擬AI、人臉辨識等法規時，比例原則也是個重要考量。例如臺灣民眾認為，在確保治安的前提下，可以接受授權警察建構與調閱人臉辨識資料庫，而臺灣社會文化對犯罪現象的恐懼感相當強烈，更加支持警政單位動用人臉辨識系統。事實上，《警察職務行使條例》迄今還未規範警察使用人臉辨識的原則與時機（林昕璇，2023）。相對地，不少民眾對於在COVID-19疫情結束之後，部分機關學校仍然保留人臉辨識、體溫檢測的監控硬體與工具，感到不安和警覺而向教育部提出陳情（林昕璇，2023）。是故，不同政治文化對安全的拿捏尺度有異，據此延伸的比例原則也會有所差異，值得政府制訂管制法規時參酌。

2024

感　謝　聆　聽