出國報告（出國類別：技術交流）

基於智能玩具的隱私識別鑑定模型

服務機關：臺北科技大學

姓名職稱：黃士嘉 教授

林敬傑 博士生

趙大衛 碩士生

派赴國家：泰國

出國期間：106/04/22 - 106/05/03

報告日期：106/06/05

摘要

現今孩子的玩具已經變得越來越複雜，從簡單的實際產品玩具變成一種能透過使用軟體和硬體將玩具使用者語音及畫像資料數字化的產品。 一個智慧玩具被定義為由一個零件組成的一個設備，新一代的智能玩具正在向越來越多的家庭尋求途徑，例如近年來非常受歡迎的智能電視。雖然智能電視越來越受歡迎，但它肯定會給用戶帶來新的隱私問題和潛在的安全隱患。因此，重要的是要考慮智能電視使用的具體隱私問題，法律和法規。如果未充分了解隱私概念的兒童等未成年用戶參與使用智能電視服務，則成為特別關注的問題。在這項研究中，我們考慮基於數字成像的方法來識別和正確地標記兒童面孔，以防止不必要的個人信息洩露。

目次

目的

本次的台泰雙邊合作計畫主要目的係為研究與開發一個基於 Smart TV 內置攝像頭之考量隱私的兒童臉部辨識系統。本研究團隊與泰國先皇技術學院（King Mongkut's Institute of Technology Ladkrabang）的 Prof. Panwit Tuwanut 所帶領的研究團隊進行研究交流與合作。

透過兩方研究團隊以及泰國先進企業的技術交換和交流討論，來開發出一套考量孩童隱私權的臉部辨識系統來嵌入至智慧玩具中。

過程

第一部份：泰國技術交流參訪流程

雙方研究團隊先舉辦研討會議討論如何考量兒童隱私的同時開發一個適用於兒童的智慧型玩具。會議過程中，雙方認為現今智慧型玩具有兩種趨勢：語音以及影像處理，而由於現今 Smart TV 的普及，在影像處理方面著手的話不僅可以套用到智慧型玩具，更可以更加泛用的套用到其他配備攝影機的任何智慧型設備上。

因此實驗過程雖是使用 Smart TV 攝像頭，但基本上任何的智能玩具或智慧設備都能夠套用此演算法。

討論結果將演算法分為多個 Stage 處理：影像收集階段（Image Collection Stage）、分類器訓練階段（Classifier Training Stage）、以及最後的臉部辨識階段（Face Classification Stage）。在影像收集階段的實驗中，使用 Smart TV 之攝像頭收集訓練以及測試用的影像來提供分類器的訓練以及效能驗證，其中收集的影像被分為了訓練集（Training Set）以及測試集（Test Set）。在分類器訓練階段中，必須要先將分類器訓練過大量的訓練樣本，並且依照分類器在訓練樣本中的表現來評估是否完成訓練，若否，則增加樣本數量來提供更多的資訊給分類器進行訓練。而臉部辨識階段就是使用收集好的測試影像來評估該分類器的效能，若表現很好，則套用此分類器到演算法中；若否，則回到訓練階段繼續訓練。預期透過本次的實質討論，進行技術交流，有效的開發出能夠兼顧到孩童隱私權的臉部辨識方法及未來的研究方向和計畫內容。

圖一、雙方會議結束後互贈禮品

圖二、會議報告狀況

於會議結束後，泰國研究團隊特地帶領台灣研究團隊參訪其校內研究單位、工廠、實驗室，以及

帶我們去和泰國的省電力局 PEA 及其研究智慧電表之分部門、科技公司 NECTEC 進行技術交流。

圖三、研發團隊跟省電力局負責人留影

圖四、團隊參訪控制中心之討論情況

PEA 研究團隊跟我們交換了許多想法，並帶我們到其控制中心參觀，給我們看其是如何由中央監測並控管泰國各地的電力供應。接著我們來到 PEA 的智慧電表分部，其所開發的智慧電表能夠監控企業隨時的用電量，其類似於智慧型玩具、家電的即時監控性質也非常值得我們參考。分部的部員跟我們分享了他們是如何設計、推廣一個企業用的智慧電表，並跟我們分析了智慧型設備的利弊及展望。

圖五、團隊和 PEA 分部成員留影

圖六、PEA 團隊報告情況

接著我們到 NECTEC 科技公司進行技術設計方面的探討，NECTEC 科技公司有許多研究人員在研究機械學習以及深度學習方面的領域，因此對於影像處理以及物件辨識、偵測等都有非常豐富的經驗。期間我們交流了許多遭遇到的技術問題以及實驗瓶頸，其所給予的建議及交流所得到的結論達到了啟發的作用。

圖七、團隊參訪 NECTEC 留影

圖八、團隊與該公司技術團隊之交流情況

第二部份：考量隱私之基於智能影像設備的兒童人臉辨識系統

出國考察期間，雙方團隊認為若是將演算法設計在影像處理方面，那麼應用的範圍不僅可以涵蓋所有具有攝像頭的智能玩具，還可以更加通用到任何有攝像頭的家用電子配備中。因此，後續討論會專注在隱私權以及智慧設備之攝影機上。

通常採用隱私政策來解決隱私保護問題：作為向最終用戶傳達數據如何收集，管理，共享和保留的方式。 隱私政策應包括對用戶收集的信息的標準描述，信息將被保留多長時間，信息將被使用，信息是否以及如何與第三方共享等等。 儘管在實地取得了進展，但據我們所知，目前還沒有針對智能電視，特別是兒童的隱私保護政策目前的標準化工作。

Google 基於 Android 的智能電視用戶構成了消費群體的一大部分，對於收集他們的個人數據和針對性廣告使用模式的市場研究人員特別感興趣（Salomon，2010）。第三方廣告客戶可以根據上下文信息進一步推斷其他與人相關的知識，從而構建可用於未知或不需要的目的的詳細行為概況。個人數據可以有許多形式，包括瀏覽歷史，朋友列表，位置信息等。相關語境信息的其他示例（Schmidt，2005）可以包括口頭語境，溝通夥伴的角色，溝通的目標以及相關個人在社會環境，以及物理環境的空間，化學等特徵。收集的信息可能看起來微不足道，通常可能不被用戶特別敏感，但在實踐中，如果正確處理，可能會顯示很多重要的個人信息。

世界經濟論壇（2011 年）定義了三種類型的上下文數據，按照收集的方式，即自願，觀察和推斷。用戶明確提供了數據，包括個人資料信息或偏好設置。另一方面觀察到的數據不是用戶直接給出的。通過諸如全球定位系統（GPS），攝像機，時鐘等設備傳感器的應用來檢測它。最後，通過分析志願者和/或觀察數據來編程推斷出的數據，例如用戶是可能會根據典型行為等進行操作。可以通過數據分析和推論創建大量用戶敏感信息。由於既不自願也不觀察（因此不是直接獲得），因此可能難以對用戶進行全面披露。一方面，對自願和觀察數據的推論可以以非常高的確定性來預測，這可能引起安全問題，例如基於個人習慣的旅行目的地和時間的預測（Dewri 等人，2013）。在智能電視中，特別是基於通過嵌入式傳感器和其他環境數據收集和推斷的上下文數據，向用戶提供個性化服務，這兩種數據

都是自願提供的。此外，智能電視通常涉及網絡環境，引入更多的用戶隱私和安全問題，特別是與智能電視正在處理的上下文信息有關（Shabtai，2010）。

確定要收集的信息量通常需要在公開敏感數據和在智能電視中接收上下文感知服務之間進行權衡。顯然，為了向用戶提供高度相關的服務，需要收集更多的個人和上下文信息，這引起了對隱私的關注。例如，智能電視中的服務可以設計為根據與他們有關的內容向用戶發送特別促銷和優惠券。為了確定最相關的促銷活動，這樣的服務將需要收集與用戶行為相關的某些上下文數據以及包括年齡和性別在內的分析信息。應用甚至可以收集和保留用戶的歷史數據確定他們在某些時間可能做什麼，並分析與應用程序之間的早期交互，以確認對以前提供的促銷活動的興趣。在這個例子中，顯而易見的是，用戶收集到的信息越多，可以向他們提供的相關服務越多，但用戶可能不會對收集和推斷的數據的級別感到滿意。知道你在哪裡的應用程序以及你在任何時候可能做的事情不僅會引起隱私，還會引起安全問題。這就是為什麼上下文數據是關於智能電視應用的隱私問題的核心。

因此，必須定義隱私目標，以確保敏感數據確實以負責任和安全的方式進行管理。應進行詳細分析，以確定和建立安全策略，以確保無法從此類保留數據中導出用戶行為的敏感細節。雖然有不同的方法旨在保護敏感上下文數據的隱私，但我們將會在討論在評估智能電視隱私範圍時必須考慮的具體數據類型。一般來說，智能電視的應用程序必須在受控環境中運行，並且必須將數據和資源與可能在設備上運行的其他不可信應用程序保護起來。這通常受最終用戶級別協議（EULA）格式規定的安全和隱私規則的約束。然而，智能電視經常運行可能有意或無意地違反此類安全政策的第三方服務。在信息技術方面，隱私和安全始終是確保有效實現既定目標而不損害個人資料的核心。關於安全性的三個主要問題是保密性，完整性和可用性。保密意味著對信息的訪問僅限於目標方。誠信意味著數據準確和一致，並沒有被篡改，而可用性意味著資源和數據在合法各方需要時仍然可用。所有這一切意味著必須有安全機制的堅實基礎，作為有效和可靠的隱私執法的先決條件。

Hung and Chen（2009）將信息隱私定義為“個人確定如何，何時以及在何種程度上將自我信息轉讓給另一人或組織的權利”。特別是個人身份信息是可以鏈接到特定個人的任何類型的信息，參考他們的活動，偏好，歷史，對話等等。在智能電視環境中，如上所述，也可能從上下文數據中收集個人身份信息。信息隱私目標可以通過隱私保護機制實現，如訪問控制，隱私政策和隱私偏好。當用戶相關信息（包括從智能電視背景導出或推導出來）暴露於不應該訪問的用戶時，會發生用戶敏感數據洩露。為了本研究的目的，我們假設儘管信息披露規則可能已經在私人政策中得到適當的陳述，用戶可能已經提供了他們的同意，但用戶可能仍然不知道所有隱私隱私相關細節和因此可能缺乏充分的了解。實際上，雖然用戶可能隱含地或明確地提供同意，但在許多情況下，這種同意只是通過使用服務來暗示。對於明確的同意，可以給出，例如，如果用戶需要按照隱私政策條款和條件點擊“我同意”才能接收服務。另一個相關的問題是當用戶不知道在其上收集的上下文相關信息（例如他們的行為信息）時發生的內容不知情。事實上，互聯網工程任務組（IETF）關於隱私權問題的 RFC6973（Cooper 等，2013）清楚地將信息披露和內容不確定性視為高度重要的特殊次要威脅。

不同的國家和立法對隱私保護有不同的法律，還有許多國際準則和行業規定，概述隱私權最佳做法。這些法律法規也可能因所收集的信息類型（例如健康信息）或用戶（例如 13 歲以下的兒童）而

異。例如，“個人數據保護法案”是一個數據保護框架，用於管理對巴西所有個人數據處理和收集進行處理的數據保護框架，其中規定了個人數據的數據保護義務和要求（CIPP Guide，2016）。在日本，“保護個人信息法”法案保護個人信息的個人權益（內閣秘書處，2016 年）。在阿拉伯聯合酋長國，阿拉伯聯合酋長國保護個人資料和隱私保護規定了“通過郵遞，電報或其他通訊方式進行交流的自由，其保密依法保密”（Dearsley et al ，2012）。在台灣，“個人信息保護法”（PIPA）規定了政府和非政府機構對公民或非公民的個人信息和個人資料的收集，處理和使用。個人信息收集，處理或使用之前，PIPA 需要通知（類別司法部，2015 年）。另一方面，“個人信息保護和電子文件法”（PIPEDA，2000）中概述了加拿大的隱私法，該法規定瞭如何在商業業務中收集，使用和披露個人信息。 PIPEDA 基於加拿大標準協會（CSA）“個人信息保護示范守則”（加拿大政府，2000 年）概述的十項隱私原則，該標準自 1996 年起被確認為國家標準（加拿大標準 Association，1996）。該示範法代表了包括美國和歐盟在內的許多國家的隱私立法原則。它也與歐洲經濟合作與發展組織（經合組織）保護個人資料隱私和跨境流動指南（OCED，2013）有所不同，歐洲聯盟成員國通過（WIPO，1995 年） 。

關於上述隱私，我們的研究重點是智能電視背景下的兒童面部識別技術框架。參考圖 1，孩子（用戶）可以在物理和社交環境中與智能電視服務（可能與智能電話）進行交互。由於智能電視能夠收集和操縱諸如文字，圖片，視頻，聲音等各種數據，其使用範圍比傳統電視複雜得多，特別是考慮到用戶可以是成人和兒童在共同的身體和社會環境中。請注意，在這樣的環境中，如果敏感信息洩露給兒童捕食者，隱私設置不當可能危及兒童的身體安全。這與智能電視收集的數據有關，其中包括有關用戶的信息（例如，兒童臉部的照片）和從其物理和社會環境中提取的上下文信息（例如其他人的照片，環境視頻和音頻記錄，註冊環境條件和基礎設施等）

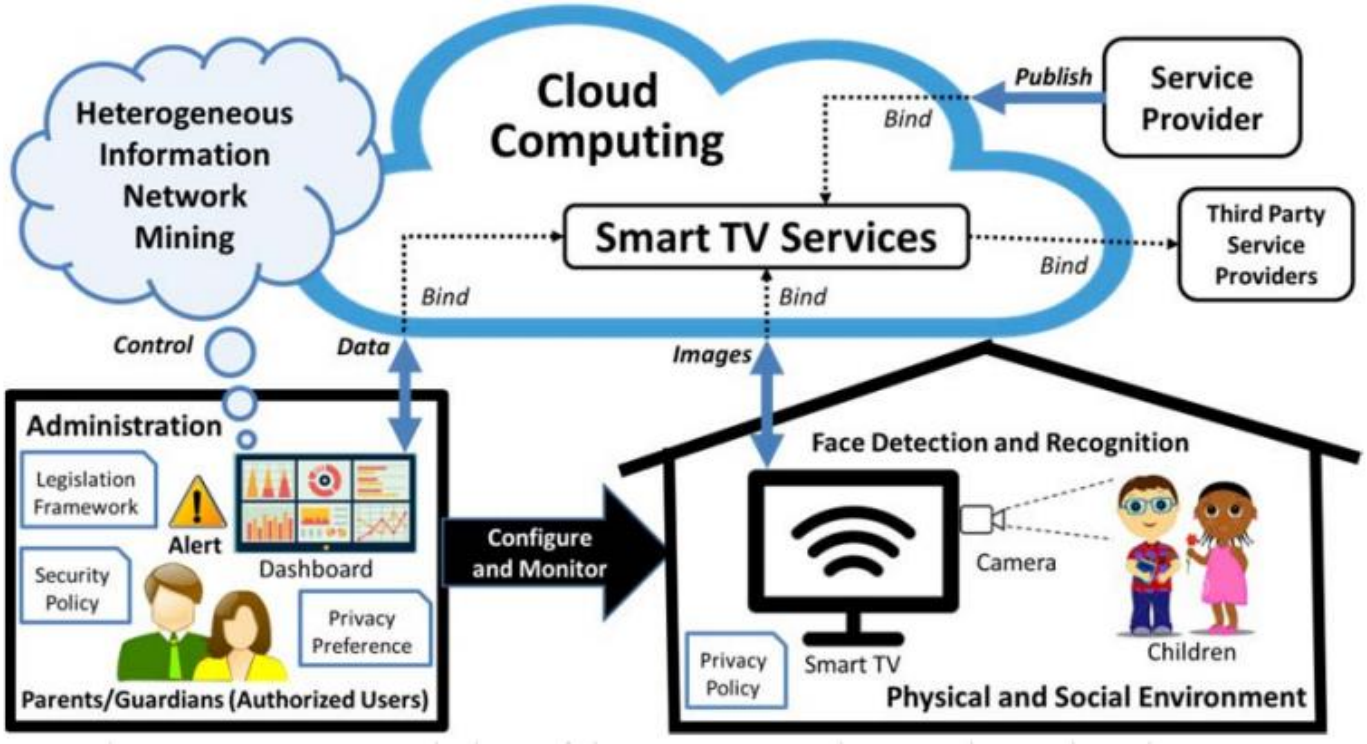

Figure 1. 智能電視隱私增強環境的概念視圖

我們認為，家長控制功能將最好地實現為嵌入式智能電視功能，使父母能夠限制兒童可以發佈到

智能電視的內容。請注意，此類功能與嵌入傳統電視機和機頂盒的標準家長控制功能不同。可以通過豐富的數據可視化模型（例如，支持文本，圖片，視頻，聲音，位置和其他感測數據），以儀表板的形式提供有效訪問此功能，以通過常用應用程序來維護家長控制智能電視服務的編程接口（API）。儀表板還將用作一個集成，驗證和可視化工具，用於調查和識別適用於智能電視的隱私政策，偏好和特定規則。根據美國聯邦貿易委員會“兒童在線保護法”（COPPA，1998）控制執行隱私規則的值得信賴的第三方（法律機構）也可能參與此過程。 13 歲以下兒童 COPPA 隱私保護規定，未經家長同意，無法收集該兒童的個人信息。 2010 年，COPPA 的修訂進一步闡述了個人信息包括地理位置信息，照片和視頻。基於此，我們將建議的家長控制儀表板結構化為以下兩個主要功能組件：

- 隱私偏好：授權用戶可以定義自己的喜好，了解如何以及將收集，共享，保留等數據，並將其與智能電視的隱私政策相關聯。 這樣的偏好將被用於為符合政策的知識數據庫生成一組隱私規則。這些隱私規則將明確規定給定的主題可以執行的操作，並確定與此類操作相關的目的，收件人以及具體義務和保留政策
- 警報機制：參考授權用戶註冊的隱私偏好，系統將實例化通知服務，為用戶提供關於在相應物理和社會環境中檢測到的所有檢測到的隱私違規或其他隱私相關可疑事件的反饋意見。

有了完善的文獻探討、理論架構以及實驗，我們開發出一套完善的演算法能夠在避免洩漏隱私的情況下獲得高精準度的人臉辨識結果，並且已投稿至頂尖 SCI 期刊論文中。

心得及建議

非常感謝本次台北科技大學所給予的支援，能讓我們前往泰國進行技術交流以及研究。本研究群致力為國家發展最新之科技與技術，並會饋到社會中。