車聯網五大風險　資安細節台廠不容輕忽

舒能翊

台灣ICT產業名聞遐邇，在車聯網時代佔有絕對優勢，但汽車連網也代表資訊安全受到考驗。

隨著各國個資法、資料保護規範訂立，產品如何在研發時即獲得國際市場的門票，成為許多業者資訊服務供應商、汽車零件供應商、設備供應商等頭號挑戰。車輛連網後會產生許多資料流，當涉及多元資料來源時，就算資料本身非個資，與其他資料拼湊起來後也可能有疑慮。

資策會科技法律研究所主任王自雄表示，數位信任議題與碳關稅一樣不可忽視。2021年歐盟個資保護委員會(EDPB)公布連網車輛與移動相關應用產品涉及之個人資料處理指引，規範對象包含車輛製造商、資訊服務供應商(如保險業者、App開發商)、汽車零件供應商、為車廠蒐集處理資料的設備供應商等。雖然指引範圍針對非職業使用，不包含智慧巴士、貨車等商業應用，但指引中還是有一些原則可以作為參考，如駕駛相關功能且包含任何能增進車聯網功能的資料處理應用。至於針對協作式智慧運輸系統(C-ITS)相關資料則另訂規範。

雖說是「指引」，但仔細觀察細則後不難發現此為建構於歐盟一般資料保護規則(GDPR)的原則。意味任何車載軟硬體未來要在歐盟境內國家銷售、使用、跨境傳輸全部都受到規範。不僅如此，美國的跨境隱私保護規則(CBPR)也必須符合。因此廠商應取得國發會個人資料保護與管理制度(TPIPAS)一驗雙證，以符合國際個資法遵。

在交通部推動D-City：淡海5G智慧交通實驗場域研究計畫(以下簡稱D-City試驗場域)中，所有的實驗業者都會成為上述指引所涵蓋的對象。車安中心也正與中華電信規劃資安憑證計畫，將輔導廠商不論場域內外都可以針對各種風險類型與手法作好準備。

針對連網車，王自雄也羅列五大風險。

資訊不對稱：數位時代是零信任的時代，但仍有其必要性，可藉由在車輛內建個人檔案管理系統，增加控制權。

處理之合法基礎：在連網車情境下，一般取得同意的方式通常難以使用，必須謹慎安排處理的合法基礎，如將告知義務落實建議使用階層選項與圖是，或不得使用汽車買賣契約取得概括同意等。

目的外利用：原始同意不能作為目的外利用一句，必須就新目的取得同意。例如用於車輛維護所蒐集的遙測資料，未經用戶同意不得揭露給汽車保險公司。

資料過度蒐集：隨車輛內外部感測器數量不斷增加，非常容易造成資料過度蒐集，尤其在採用機器學習演算法時更需注意。對此，隱私設計、預設要求、資料在地化處理、資料匿名化與假名化等皆是解方。

安全性：複數功能、服務、界面恐怕增加資訊安全攻擊可能性，車輛安全漏洞恐怕危及生命安全，此外也應注意資料在車輛內外部的儲存保護與管理。可行應對措施包含利用與時俱進的眼演算法加密資料、建立加密鑰匙管理系統、區分車輛安全行駛相關功能與其他依賴通訊能力的功能、儲存對車輛資訊系統的瀏覽歷史紀錄等。

本文獲授權轉載自《DIGITIMES》
新聞來源：https://www.digitimes.com.tw/iot/article.asp?cat=158&cat1=20&id=0000649924_H4Z8J1XB3K8SOX307J4E8

上稿時間：2022年11月15日

文章標籤