



## 國立中山大學資訊工程學系

804 高雄市鼓山區蓮海路 70 號  
(07)525-2000 轉 4301, 4302, 4303



【主題】106 學年度第 1 學期資工系每週演講心得分享(10)

【TITLE】1st semester of the 106th academic year, CSE weekly speech notes 10

【日期&時間】106 年 11 月 24 日(星期五)，14:10~15:40

【DATE & TIME】Nov. 24, 2017 (Fri.) 14:10 ~ 15:40

【主講人】游家牧 助理教授/國立中興大學資訊科學與工程學系

【SPEAKER】Assistant Prof. Chia-Mu Yu / Department of Computer Science and Engineering, NCHU

【講題】隱私資料的釋出與收集機制

【TOPIC】Private Data Release and Collection

【摘要】因為開放資料 (Open Data) 已經成為趨勢，勢必有越來越多包含個人資訊的被釋放出來，但也因資料內含個人隱私資訊而有侵犯隱私的嫌疑。因此如何在不侵犯隱私的條件下將具隱私性的資料釋出將是一門值得討論的議題。另外，隨著商業公司藉由其各種的軟體與裝置收集越來越多我們的個人資訊，這也代表著使用者的隱私正在逐漸地被知曉，商業公司如何在不侵犯隱私的條件下收集具隱私性的資料恰巧與上述隱私資料釋出成為一種對比。

【ABSTRACT】Open data is a trend, with the cost of individual privacy violation. Private data release is a technique of sanitizing and releasing the data while ensuring the individual privacy. On the other hand, commercial companies collect individual information such as user behavior to improve their products, thus leading to potential individual privacy breach. Private data collection refers to a technique of collecting high-utility personal information while ensuring the individual privacy. In this talk, I will give an overview of these two techniques and present their recent development.





## 國立中山大學資訊工程學系

804 高雄市鼓山區蓮海路 70 號  
(07)525-2000 轉 4301, 4302, 4303



### 【心得分享】

◎梁庭瑋（國立中山大學資訊工程學系碩士班一年級，平行處理實驗室）

今天演講的主題是”隱私資料的釋出與蒐集機制”，講者為國立中興大學資訊科學與工程學系游家牧教授，主要內容是講述因為開放資料(Open Data)已成為趨勢，但同時也會出現很多隱私問題，因此游教授簡單介紹如何在不侵犯隱私條件下將具隱私性資料蒐集及釋出，也講解各種不同方法把資料加上雜訊、使其模糊化。講者以循序漸進的方式讓我們了解各種方法的演進及需要改善的部分，還有各種他人可能會攻擊、從中獲取資訊的方式，其中還運用許多資料壓縮加密、解密技術，也有使用機器學習 GAN 方法等等。最後問與答中，游教授提到



即使加入上述所介紹的雜訊後，資料也並不保證完全安全，而這方面隱私則是和法律層面息息相關，因此這項議題仍需我們繼續努力找出完善的方法。聽完這場演講，讓我了解到這項技術其實已在我們生活應用得相當頻繁，若是沒有經過這項技術的保護，我們的隱私、個人資料都將暴露於無形，今天真的獲益良多。



## 國立中山大學資訊工程學系

804 高雄市鼓山區蓮海路 70 號  
(07)525-2000 轉 4301, 4302, 4303

◎劉珊如（國立中山大學資訊工程學系碩士班一年級，平行處理實驗室）



今天的演講主題是一隱私資料的釋出與收集機制，資料通常都需要經過一些處理才能釋出，以確保隱私資料不被他人擷取，因此講員介紹幾種比較常見方法，像是刪除某些欄位、抹去部分資料(用符號取代)、打亂資料順序或增加雜訊等等，這些方法雖然可以讓我們的資料不被他人知道，但是在真實性上卻是讓人有所疑慮，因為經過這些處理，不僅少了原始資訊，還多了雜訊，很多政府機關都希望他們提供的開放資料是真確的，因此有許多其他較複雜且困難的處理方法被提出。聽完這場演講後我才知道，原來我們平常從網路上得到的各種開放資料都不是最原始資料，而是經過特別處理，雖然不確定這會不會影響到我們分析結果，但我想這也是必要的前置處理，若原始資料都被完整的公開，便沒有隱私可言，對我們也不是一件好事呢。

單位：國立中山大學資訊工程學系  
聯絡人：吳秀珍行政助理、黃莉萍行政助理  
聯絡電話：(07)5252000 分機 4301、4303