資料探勘之資訊隱私權研究

The Study of Informational Privacy on Data Mining

謝建成 Jiann-Cherng Shieh
佛光大學資訊學研究所
Institute of Information Science, Fo-Guang University
宜蘭縣礁溪鄉林美村林尾路一六〇號
jcshieh@mail.fgu.edu.tw

吳寂絹 Chi-Chuan Wu
佛光大學資訊學研究所
Institute of Information Science, Fo-Guang University
宜蘭縣礁溪鄉林美村林尾路一六〇號
g9005011@stdmail.fgu.edu.tw

戚國雄 Kuo-Hsiung Chi
佛光大學哲學研究所
Institute of Philosophy, Fo-Guang University
宜蘭縣礁溪鄉林美村林尾路一六〇號
kchi@mail.fgu.edu.tw

摘要

以資料探勘技術，由繁複的資料中擷取有用的資訊，支援決策分析參考，是目前此技術於各領域之主要應用。然而從收集資料、分析資料、到解釋資料，在這一連串的運用過程中，確實已引發種種不同的倫理議題，其中最常被探討的為侵犯隱私權的爭議。Tavani 於 1999 年提出資料探勘技術對隱私權的嚴重影響，並藉由假設個案的分析，論証資料探勘技術違反了經濟合作組織（Organization for Economic Cooperation Development，OECD）個人資料保護原則中指定目的與使用限制二原則。本文將基於 Moor 的「限制存取隱私理論」重新檢視探討 Tavani 所提的假設個案。我們亦將更進一步就此個案提出資料探勘技術應用的模式，以符合 OECD 個人資料保護規範，避免引發其是否會侵犯隱私權的爭議。

關鍵詞：資料探勘、隱私權、資訊隱私權

Abstract

In recent years, most of data mining applications are going to extract useful information from comprehensive data stores to support business decision-makings. The processes of data collection, data analysis and data explanation of data mining have inspired various kinds of serious ethical issues. The privacy violation is the most important one that people concern. In 1999, according to the principles of OECD's "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", Tavani proposed a scenario of bank load to address that the application of data mining should cause privacy violation. In this paper, based on Moor's "Restricted Access Theory of Privacy", again we take the scenario to inspect the informational privacy issue. By reengineering the procedure of bank management, we propose a practical solution to

prevent privacy violation as applying the data mining techniques.

Keywords：Data Mining, Privacy, Informational Privacy

壹、緒論

一、資料探勘衍生之資訊倫理議題

資訊時代來臨，人們可以利用先進的技術，更方便地收集到所要的資訊，當然，這些資訊也更容易在世界各地傳佈。對於一個企業而言，資料愈多，提供的資訊就愈多，但要從這些繁複的資料中擷取有用的資訊，則必須依賴資料探勘技術的妥善運用。

資訊時代的倫理議題主要有四個，分別為隱私權（privacy）、資訊精確性（accuracy）、財產權（property）、資訊存取權（accessibility），英文簡稱之為”PAPA”。簡單地說，所謂隱私權指的是在何種狀況及何種保護措施下，可向他人揭露個人的那些資料？那些又是不願向他人揭露的資料？正確性則是指誰負責資訊的真實性與正確性？資訊有誤時由誰負責？財產權強調的是誰擁有資訊？資訊交換的公平價格是多少？誰擁有傳佈資訊的管道？這些少量的資源如何分配？資訊存取權則是指個人或團體誰有權去取得何種資訊？在何種狀況下取得？有何種安全措失(Mason,1986) ？其中庶關個人隱私權的議題，正是資料探勘應用上最為人所關注的。在資訊社會中隱私權的角色與地位，是否與傳統的隱私權有所不同，是我們必須先探究釐清的。

二、資訊時代的隱私權

在與使用電腦相關的社會與倫理議題上，電腦化的記錄保存方式對個人隱私所造成的影響，是最受人注目的。保存記錄的現象從數千年前即產生，但電腦技術卻讓記錄的保存方式產生相當大的改變。首先，資訊蒐集的範圍改變了；其次，資訊的種類改變了；最後，交換資訊的範圍同時也改變了(Johnson,1994)。

電腦科技的發展，改變了傳統的記錄保存方式。透過電腦，人們可以蒐集、保存、交換、操控資訊，當這些資訊非屬於公開性質時，便涉及了隱私的問題。舉個例來說，公司的主管可以透過軟體監控每位員工輸入鍵盤的各個指令，就公司的立場而言，這種作法乃為了確保每位員工於上班時間內，不得從事與工作業務不相干之活動，以藉此提昇工作效率，但這種行為是否正確?員工於上班時間利用公司的資產進行私人活動，確實是不適當之行為，但若為了避免此行為而侵犯到員工的隱私，這種做法就有待商榷。

同樣地，由於電腦化資訊的性質，使得人們可以輕易的交換資訊、結合資訊。原本屬於公開性質的資訊，結合後可能變成一種「新資訊」，而這種新資訊的內容若為個人資訊，就可能侵犯了當事人的隱私，資料探勘技術的應用即為其中一例。

事實上，電腦並不是真正的問題所在，或上述各問題之原因，真正的問題在於創造、蒐集、交換、使用資訊的這些個人及機構，電腦充其量只是個工具；若真有上述問題，問題在於使用電腦的人，而非電腦本身。不過，由於電腦能執行特定類的任務，個人或機構才有可能去參與這些活動。因此，電腦是決定人們能做什麼，及塑造我們能有什麼樣的社會之重要因素(Johnson,1994)。

電腦及隱私議題的標準探討方式，即探討如何在使用個人資訊的需求者（通常是政府機構或公司）與被蒐集資訊者間取得平衡。一般而言，需要個人資訊者，其蒐集資訊的目的在於利用資訊來協助他們制訂較佳的決策

(Johnson,1994)。舉例來說，銀行之所以要掌握資訊，是因為他們覺得對個人的資訊掌握得愈多，即較能判斷個人是否有能力償還貸款。同樣地，超級市場經營者也認為擁有顧客購買行為的資訊，加以分析後，可使他們調整貨品擺放位置，以節省顧客尋找相關商品的時間，換言之，即提供顧客較佳的服務。我們甚至可以將資訊視同「商品」般進行買賣，利用電腦技術蒐集個人資訊後，再將之販售給需要資訊的機構。對他們而言，資訊是個大商機，但在看好這個市場之前，是否該先有個機制來保護個人的隱私？

大部份的人都會因我們的資訊被蒐集而感到不自在，事實上是，我們通常不知道誰擁有這些資訊？他們將如何使用這些資訊？為什麼我們要感到不自在呢？我們在懼怕什麼？我們能否限制公家及私人機構蒐集有關個人資訊的數量？我們能否讓個人操控他們自己的資訊(Johnson,1994)？這些皆是值得探究的問題。

於 1999 年，Tavani (1999a)以一個銀行申請貸款的假設個案，說明銀行利用資料探勘的技術來審核顧客是否符合申貸條件的做法，使顧客的隱私受到威脅，進而結論在 OECD 個人資料保護原則下，資料探勘技術的應用，勢必會侵犯個人隱私權。因此，本文擬以 Moor「限制存取隱私理論」為基礎，再由銀行的管理面重新探討申貸個案，並提出實際解決方案，避免資料探勘技術所引發之隱私爭議。

本文架構如下：首先彙整資料探勘及隱私權的定義，並介紹個人資料保護原則的內容，接著描述 Tavani 的假設個案，並藉由個案之分析說明為何資料探勘會引發隱私爭議，然後就該個案實際作業情境，提出解決侵犯隱私權方案，最後則為本文的結論。

貳、文獻回顧

一、資料探勘

簡單地說，資料探勘是指自大量資料中擷取或挖掘出知識，以支援決策分析之用；廣義而言，資料探勘指的是從儲存於資料庫、資料倉儲或其他資訊貯藏所中發掘出使用者有興趣的知識之過程，或者是針對使用者所提出的問題，自儲存大量資料的資料庫中萃取出有用資訊、資料樣式與趨勢的過程(Han and Kamber,2001)。至於原始資料的價值高低，端視是否能萃取出較高水平的資訊能力而定--能提供支援決策的有用資訊、對所產生的資料有較佳的理解與探討(Wong,et al.,1998)。

一個典型的資料探勘系統應包含六個主要成份，詳見圖 1(Han and Kamber,2001)。

1. 資料庫、資料倉儲或其他資訊貯藏所—可能是一個或一組資料庫、資料倉儲，可能需要運用資料清理或整合的技術；
2. 資料庫或資料倉儲主機—負責依使用者的資料探勘需求來取出相關資料；
3. 知識庫—作為查詢或評估結果樣式的指引，包括概念階層（concept hierarchies）、使用者的理念（user beliefs）、元資料（metadata）等等；
4. 資料探勘引擎—此為資料探勘系統的基礎，涵蓋任務的一組功能性模組；
5. 樣式評估模組—運用興趣測量與資料探勘模組的互動，針對興趣的樣式做查詢，為了有效的探勘，建議在評估興趣樣式時能愈深入愈好；
6. 圖形化的使用者介面—作為使用者與系統間的溝通介面，並且讓使用者能瀏覽資料結構、評估探勘的樣式，及將樣式以不同形式的視覺化呈現。

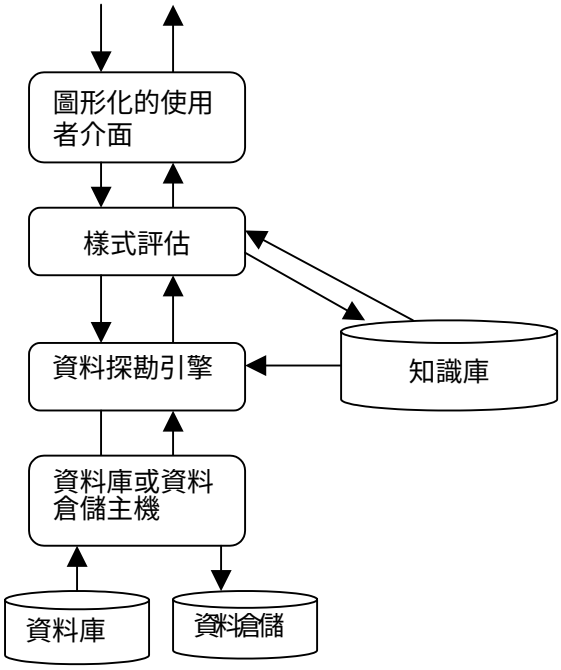

圖 1 資料探勘系統架構

資料探勘常與「知識發掘術」（Knowledge Discovery in Databases，KDD）混為一談，知識發掘術指的是從資料中萃取絕對的、未知的及潛在的有用資訊，萃取後的資訊可作為支援決策用(Wong,et al.,1998)。 有些人則認為資料探勘只是在整個知識發掘術過程中的一個基本步驟，他們將知識發掘的過程分為七個步驟，分別為資料清理（data cleaning)、資料整合（data integration）、資料選擇（data selection)、資料轉換（data transformation)、資料探勘（data mining)、樣式評估（pattern evaluation)、知識呈現(knowledge presentation)(Han and Kamber,2001)。本文所探討的資料探勘擬以前者的定義來認定之，即不將資料探勘視為知識發掘術之其中一個步驟，且將侷限於對個人資料所引發之隱私爭議部份。

二、OECD 的個人資料保護原則(Council of the OECD,1980)

OECD 的個人資料保護原則，已成為許多國家制訂隱私保護法案之依據，且由於 Tavani 認定資料探勘技術之應用，將違反 OECD 個人資料保護原則中的「指定目的」與「使用限制」原則，因此，在我們進行個案研究之前，先行了解何謂個人資料保護原則。

個人資料保護原則（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）是由經濟合作發展組織（OECD）25 個會員國所提出的非正式推薦書，旨在平衡隱私與個人自由權利保護，以及個人資料之自由流通利益。其中的八個國際應用基本原則（Basic Principles of National Application）分別為：

1. 限制蒐集原則：個人資料應以合法、公正的手段，於適當之場所，並經本人同意始得蒐集。
2. 資料品質原則：資料之利用須符合蒐集之目的，並保持正確、完整及新穎性。
3. 指定目的原則：蒐集資料的目的應於蒐集時即明確的指定，且使用上不得有不符目的之情況產生。
4. 使用限制原則：個人資料不應被揭露、取得或用於第三個原則以外之目的，除非取得本人的同意或是經由法律授權。
5. 安全保護原則：個人資料應採取合理之安全保護措施。
6. 公開原則：關於個人資料之開發、運用及政策應採一般之公開政策。
7. 個人參與原則：個人有權利向資料管理者確認是否保有自己的資料、了解個人資料內容，並可請求刪除或更正自己的資料。
8. 責任義務原則：資料管理者的責任。

三、隱私權

隱私是一個很廣義的概念，各家對隱私的定義及分類互歧，以下將分別介紹之。

（一）隱私分為「工具性的善」及「內在性的善」(Johnson,1994)

隱私具有工具性的價值，同時也是建立親密關係及信任的必備條件(Fried ,1968)。在社會上，個人若無隱私，則無法建立友誼、親密及信任關係。若我們要擁有這樣的關係，我們就必須擁有隱私。也有人認為隱私是民主的必要條件(Westin and Baker,1972)，或認為隱私是自主的必要條件，一個人沒有隱私則沒有自主權。康德理論認為自主不只是在眾多價值中的一個，它是人類生存意義的基礎，同時也是身為人的價值。也有人認為隱私不只是自主、尊敬及民主的手段，而是這些意涵的一部份。我們不是為了獲得自主才去尋求隱私，相對地，沒有隱私根本不可能會有自主(Johnson,1994)。

Warren 與 Brandeis 認為隱私權應該在一般的法律認可範圍內，他們建議在個人資訊與不被侵犯的人格權利間建立連結關係，因為一般的法律承認個人有不被侵犯之人格權利，而這就包含了個人的生活事實(Warren and Brandeis,1890)。此觀點與康德的理論很接近。當我們著重於社會關係時，自主與個人資訊間的連結將變得更清楚易辨(Johnson,1994)。

資訊是建立社會關係與決定該關係的特色之基礎。Rachels 認為人們必須能控制有關自己的資訊，才能發展種種的社會關係，包括與父母、配偶、員工、朋友、汎汎之交等關係，每一個關係都不同，因為他們擁有你的不同資訊。Rachels 引用這個觀點來聲稱隱私是重要的，因為它可以讓我們發展不同程度的關係(Rachels,1975)。這種關係是屬於個人對個人，至於個人與機構間的關係，最重要的是個人有權力去控制建立或塑造彼此間的關係。個人的資訊會讓機構 (如：行銷公司、發卡公司) 建立與我們之間的關係，同時，資訊也會決定我們將如何看待此關係(Johnson,1994)。

（二）區域性、個人及資訊的隱私

隱私可分為三方面探討。第一，區域性的隱私，指個人身體親密範圍的保護；第二，個人隱私，保護個人免於被過度妨礙，例如搜身或違反道德感的資訊；第三，資訊隱私權，控制個人資訊被蒐集、儲存、處理或選擇性的傳佈之處理方式，並控制前述行為之適切性(Rosenberg 1992；Holvast 1993)。

資料保護僅是為了確保隱私而保護個人資料，它只是隱私權概念的一部份。依照德國憲法法庭於 1983 年對個人資訊隱私權的定義，資訊隱私權指的是個人可自行決定揭露及使用個人資訊的權利(Fisher-Hubner,2000)。

（三）不受侵擾、隱遁、限制、控制的隱私理論

Tavani (1999b) 把隱私權理論分為四類。第一，不受侵擾理論；第二，隱遁理論；第三，限制理論；第四，控制理論。早期提出隱私概念的學者，Warren 及 Brandeis，於 1890 年將隱私定義為「獨處」（to be let alone），或「不受干擾」(Warren and Brandeis,1890)。這個理論的問題在於「不受干擾」易與「自由選擇的權利」混淆，因為隱私包含了「使其獨處」。批評者指出，一個人可能不須獨處，但仍擁有隱私；或是即使獨處，但卻無隱私可言。因此，隱私雖與自由選擇的權利密切相關，但二者間仍需區分。在此值得一提的是，有些支持不受干擾理論者，易將隱私的情境（condition of privacy）與隱私的權利（right to privacy）弄混(Tavani,1999b)。所謂隱私的情境，簡單的說就是需要什麼條件才能擁有隱私，這種情境可以是自然的環境，也可以是受規範所保護的環境，因此，與享有隱私的權利是不同的概念。

所謂隱遁理論，意指依個人之自由意願，讓他暫時脫離社會，處於一獨居狀態下生活，即將個人隱私視同「獨居」(Westin,1967)。其與不受干擾理論不同之處在於，它將隱私與自由分開。這個理論的缺點為易將隱私與獨處混淆，因為它假設一個人愈孤獨，即擁有愈多隱私，就好比認為將一個人擱置在孤島上即會擁有最多的隱私。批評者同時也指出，一個人可以擁有隱私，但卻不必要完全的獨處(Tavani,1999b)。

不受侵擾理論與隱遁理論相當於「心理的隱私」（psychological privacy）(Regan,1995)，或有人稱之為「親近的隱私」（accessibility privacy）(Decew,1997)，其強調的是當一個人的身體被侵犯，或是個人的事務被干擾所造成的心理傷害。近年來有學者指出，在美國隱私已由對個人侵犯、干擾的關注，轉移至對個人資訊的注重。與隱私相關的資訊包括儲存在電腦資料庫中個人資訊的存取，有人稱之為「資訊隱私權」，並視其為隱私之一類(Moor,1997)。而與個人資訊隱私相關的二個理論分別為「控制理論」與「限制理論」。

控制理論指的是，個人有能力掌控自己的資訊時才能擁有隱私。這個理論的第一個優點是它將隱私與自由、獨居分開；第二個優點是它正確地指出有隱私的個體，有權去選擇同意或拒絕他人對與自己相關之個人資訊的存取。然而，批評者卻認為控制理論有二個瑕疵，第一個是屬於實務上的問題；第二個是屬於理論或觀念上的問題。首先，就實務上而言，人們不可能完全掌控攸關自己的所有資訊；其次，就觀念上而言，一個人可以在完全透露自己的資訊後，仍能保有隱私，因為他可以保有顯露資訊的控制權。控制理論的另一個缺點是它幾乎完全著重在控制或選擇方面，易與自主性混淆(Tavani,1999b)。

最近頗受重視的一個理論為限制理論，認為隱私在於能將個人資訊限制在存取特定內容的程度上，其與控制理論不同的是，限制理論正確地察覺到隱私內涵的重要性。限制理論的另一個優點為，它可避免將隱私與自主性、自由及獨處混淆。然而，限制理論仍有其問題，它忽略了一個事實—即擁有隱私者應可選擇同意及限制或拒絕他人存取其個人資訊。此外，限制理論認為關於個人資料能存取的範圍愈有限，則擁有的隱私愈多。就這個觀點而言，隱私似乎又會與秘密混為一談了(Tavani,1999b)。

這四個理論皆無法明確地辨別隱私的情境（condition of privacy）與隱私的權利（right to privacy）間，及隱私的喪失（loss of privacy）與隱私的侵犯（invasion of privacy）間有何差異性(Tavani,1999b)。

（四）控制/限制隱私存取理論

Moor 提出控制/限制隱私存取理論，他認為一個人要有隱私，必須處於免於侵犯、干擾、及被他人存取資訊之保護情境。Moor 的理論較前述四個理論對隱私有著更周延的解釋。首先，他的定義涵蓋了干擾、侵犯、資訊存取等概念；其次，他將情境定義得較模糊，以適用於任何一種所謂的「隱密」（private）範圍(Moor,1997)。 Moor 的中心思想即在於他在「自然地隱密」（natually private）及「規範性的隱密」（normatively private）情境上作區隔，如此可使得我們容易區分隱私的情境與隱私的權利間，及隱私的喪失與隱私的侵犯間有何差異性(Tavani,1999b)。

在自然的隱密情境，個人受到「自然」方法的保護。例如：當你單獨一人徒步旅行於森林中，你可免於被他人侵犯、干擾或接近。在那裡，基於人有被保護的權利，隱私可能會喪失，但卻未被妨礙，因為沒有任何形式上、法

律上、道德上的規範。換言之，規範性的秘密情境就是指個人受到形式規範的保護(Moor,1997)。 Moor 提出的隱私觀點整合了限制理論的優點，即隱私需要依情境來闡釋。它同時也整合了控制理論的優點，即個人會被某特定情境所影響，這個特定情境需要一些控制或選擇，以便決定該情境是否為規範性的隱私(Tanavi,1999b)。依照 Moor 的觀點，個人不需要絕對或無限的控制權始得擁有隱私。

我們通常認為規範性的隱私情境是一個實體場所，像我們居住的房子，就是一個規範性的隱私情境，外人要進入屋內，必須先敲門，得到允許後始得進入。事實上，情境除了場所外，還包括關係、活動及資訊，如：投票行為、醫療記錄，都是屬於隱私的情境--在一個隱私理所當然地受到規範保護的區域。這些隱私情境的規範面，限制了個人、群體或政府在某些程度上的「接近」（access），在此所表達的是受保護的權利，它避免被某人干擾及擁有資訊(Tavani & Moor,2001)。簡單地說，規範性的隱私情境指的是受到道德上、法律上或形式上的準則保護之情境，當一個未經授權的行為闖入的規範性的隱私情境中，則隱私不僅喪失，而且被侵犯(Moor,1997) 。

依「控制/限制隱私存取理論」之觀點來制訂隱私權政策的好處在於它可以視情境作調整，也就是說，受保護的是在該情境下的隱私資訊，而非資訊本身。不同的人在不同的時間，可存取的資訊種類不同，存取的資訊層級亦不同。舉例而言，個人的財產所得是屬於隱私性的資訊，誰也無權要求你將財產公諸於世，但為了端正政風，確立公職人員清廉之作為，政府規定相當職等以上之政務官要申報財產，向全國民眾公開，此即針對個人財產這個資訊，在不同的情境下，有不同的保護程度。同樣地，銀行在承辦不同的業務時，應針對個人資訊給予不同的保護措施，就申請貸款中的授信業務而言，因牽涉許多個人資訊，故銀行應創造一個規範性的保護情境，來保障顧客的隱私。

在資訊社會中，隱私的保護已加入對「個人資訊」的掌控權，雖然有人認為「控制/限制隱私存取理論」不足以解釋個人在保護隱私中所扮演的控制個人資訊之重要角色(Elgesem,1999)，但若以對資訊的掌控權來界定隱私的概念，則會大大縮小隱私的範圍，因為我們能掌控的資訊實在是太有限了(Tavani & Moor,2001)，為避免混淆，Moor 於 2001 年以「限制存取隱私理論」的字眼取代之前提出的「控制/限制隱私存取理論」。我們不可能控制所有有關自己的個人資訊，但我們若能確切知道那些人可存取這些個人資料，且只能適時、適地存取，則可保障我們的隱私。Moor 的「限制存取隱私理論」正好提供了這樣的保護機制，較其他隱私理論符合現代社會之需求，因此，本論文將基於此理論，以假設個案為例，對個人資訊隱私做更進一步的解析，並提出解決之道。

參、個案研究

一、個案描述(Tavani,1999)

Lee，一位在美國 ABC 行銷公司的資淺經理，向當地一家銀行申請汽車貸款。為了確保能貸款成功，Lee 同意填寫該銀行要求的申貸表格。例如，Lee 指出他受雇於 ABC 公司已超過三年，目前年薪 90,000 美金，在另一個戶頭裡存了 10,000 美金是為了支付新車 BMW 分期付款的頭期款。他同時也指出因為去年他們全家去歐洲旅遊，所以目前正在支付一筆 15,000 美金的貸款。Lee 希望銀行不會將他這些個人資料與第三者交換，銀行同意不會向第

三者揭露或交換他的資料，但對這些個人資料是否供銀行內部分析用卻未明確說明。假設銀行從它的資料庫中發掘出以下這些樣式，包括：經理，年薪 70,000 至 120,000 之間，購買豪華汽車（如：BMW），從事昂貴的旅遊活動，通常都在受雇五年內會自行創業；另一個樣式配對程式顯示：大多數自行創業的行銷企業家都在創業一年內宣告破產。我們突然發現，Lee 屬於某一群體中的一員，這個群體的特徵顯示：「行銷經理很可能自行創業，同時在一年內宣告破產。」由於這個類別及關於 Lee 的這個"新資訊"，銀行認定 Lee 或是符合這個群組條件的人，皆是屬於具有長期信用風險者。

二、個案分析

根據 Tavani 的看法，資料探勘技術的應用，因會產生下列幾個問題，故引起大家對隱私權的嚴重關切。

（一） 將個人資料做進一步的使用及分析

Tavani 認為這些技術的使用者在收集個人資料前，並未告知被蒐集資料者，亦即對這些特定企業或機構有用的這些資訊之蒐集與使用並未取得被蒐集者的同意授權；即使對方已明確授權收集有關其個人資訊供企業使用，也不表示他們有授權給企業將這些個人資料做進一步的使用及分析(Tavani,1999a)。我們來審視 Lee 的個案，當初他自願填寫年薪、前一次旅遊貸款及他想購買的汽車類型等資料，是為了特定目的（申請貸款）之用。他給予銀行的每一個資訊能讓銀行針對他的汽車貸款申請需求，判定一個合理的決定。然而，事實顯示，Lee 授權銀行使用他的個人資訊，進行一般的申請貸款分析，最後卻出現一個 Lee 與銀行事先都不知情的樣式。換言之，銀行不單單使用 Lee 所填寫的個人資料來判定其是否符合申貸條件，這些個人資料在本質上是屬於外顯式的，或者稱之為非秘密型態的，我們通常假定這樣的資料為公開的資料，銀行還進一步分析這些個人資料，因而產生內隱式的資訊。

（二） 無法事先得知探勘結果

透過資料探勘技術所發掘出的資訊原先在資料庫中是不存在的，也就是說它找出關於個人的新資訊或新關係。以 Lee 的個案而言，「Lee 可能會自行創業，最後宣告破產」這個樣式的資訊，並不在當初 Lee 所填寫的任何資料中，它是內隱式的資訊，代表著某些與 Lee 相類似的人之群組特徵，而 Lee 可能在其他重要方面與這個群組的人大不相同。由於銀行無法預測在資料探勘的過程中，執行樣式配對演算法後將出現何種資料，因此無法事先告知 Lee 探勘後的結果，當然，Lee 對於他最後被歸屬至這個群組更是全然不知情(Tanavi,1999a)。

（三） 在單一資料庫中運作

Tavani 認為資料探勘技術的應用與傳統資料庫的擷取過程不同的是，資料探勘的資料通常是在資料倉儲或單一資料庫中運作，而不是跨數個資料庫彼此交換資料(Tavani,1999a,1999b)。

根據上述分析，我們再以 OECD 的「個人資料保護原則」來檢視此個案。依照 Tavani 之說法，Lee 的隱私顯然未受到形式規範的保護，因為銀行的做法已違反了 OECD 個人資料保護原則中的「指定目的」與「使用限制」原則。首先，銀行在蒐集 Lee 的資料時，告知 Lee 的使用目的為將這些資料拿來分析是否符合申貸條件，但最後銀行卻將之拿去用於指定目的之外的第二個目的—資料探勘分析，因而違反了「指定目的」原則；其次，銀行將蒐集來的所有 Lee 的資料用於資料探勘分析，卻未先取得 Lee 的同意，故違反了「使用限制」原則(Tavani,1999a)。因此，就 Lee 這個個案來

看，銀行運用資料探勘技術處理申貸資料之做法，違反了 OECD 個人資料保護原則中的「指定目的」及「使用限制」二個原則。

肆、研究結果

對於銀行、銀行的客戶與隱私擁護者而言，要在運用資料探勘技術與保護隱私間取得平衡或許並不容易，但我們不禁要提出質疑：難道資料探勘對個人資料的運用一定會威脅到個人隱私嗎？事實不然。以下將針對 Tavani 對該個案之分析，提出幾個不同觀點，同時由銀行的管理面來探討 Lee 的申貸案件，規劃出一個具體的申請貸款流程，來避免侵犯顧客之隱私。

一、 資料探勘技術無罪

事實上，對於運用資料探勘技術者而言，限制資料不得用於第二個目的是個相當棘手的問題。因為資料探勘技術是要從大量資料中萃取出有用的隱藏資訊，以供決策參考，但我們換個角度來看，若銀行在蒐集資料時即明確地在使用目的加上「資料探勘」的字眼，就真的構成有意義的資料保護行為嗎？如之前的個案分析所述，會引發隱私爭議的應是資料來源與探勘結果呈現方式，而非資料探勘技術本身，也就是說，隱私之爭議無關乎銀行所採用之技術。事實上，銀行只要在整個申貸流程中（包括從申請到結果呈現）提供一個隱私保護之情境給申請貸款者，至於要使用何種技術，對隱私的影響就微不足道了。

二、妥善處理內隱式資料

我們也同意資料探勘技術所探勘之結果，非銀行或當事者可預先獲知之資訊，但只要銀行處理得當，這類新資訊的產生並不會侵犯到當事者的隱私權益，也就是說，我們不能因為資料探勘技術產生的新資訊非屬於外顯式的資訊，就認定這個技術侵犯或威脅到申貸者之隱私。

三、內部及外部的資料來源

我們發現 Tavani 一直強調資料探勘的資料通常是在資料倉儲或單一資料庫中運作，而不是跨數個資料庫彼此交換資料，但事實上，資料探勘的資料來源通常不止一個，以銀行為例，在授信作業流程中的徵信資料來源應不會侷限於銀行內部之資料，我們較難掌控的不是這些內部資料庫，而是外來資料對隱私所構成之威脅。

一般而言，銀行的徵信活動應會去取得同業間的個人信用狀況資料，由於這種外來的資料來源，並未事先告知申貸者，當然也就無法取得當事者同意，以規範性的隱私情境而言，銀行此舉已使得申貸者置於喪失隱私之情境中。就這個觀點而言，銀行在承辦整個申貸業務中，會引發隱私爭議的是資料來源本身與資料探勘之結果，而非資料探勘之技術，此與 Tavani 認為資料探勘技術將引發隱私爭議之觀點不同。雖然 Tavani 假設銀行僅利用內部資料庫進行資料探勘，故無前述之疑慮，但就現況而言，銀行徵信活動不需用到他行資料之機會微乎其微，因此我們不免對 Tavani 之說法提出質疑。

四、解決侵犯隱私權之方案

我們以 Moor 的「限制存取隱私理論」來檢視這個假設個案。銀行運用資料探勘的工具來存取 Lee 的個人資訊，構成了所謂的「情境」。就自然情境而言，銀行將 Lee 的個人資訊拿來探勘分析，Lee 即喪失了隱私，但這並不代表銀行侵犯了 Lee 的隱私。就規範情境而

言，我們要探究的是，是否該由國家立法限制銀行對個人資訊的存取，以保護個人的隱私權？或是銀行該制定政策來保護顧客的隱私？我們發現，從銀行管理面的角度，為顧客建構一個保護隱私之情境，同時在做法上不違反 OECD 個人資料保護原則中的「指定目的」及「使用限制」二個原則，則可讓銀行的申請貸款業務不會引發隱私爭議。具體做法如下：首先，銀行要制定一份隱私權政策，據以向申貸者說明，同時作為業務承辦人員之規範；其次，將個人資料輸入系統中，透過資料探勘技術處理後，以密封方式將探勘結果通知申貸者，由申貸者自行決定是否要繼續後續的申貸流程，若不願意繼續，則銀行需提供刪除資料之機制，來確保申貸者個人資料之隱私。茲將整個流程詳述於后：

（一）制定隱私權政策

由於 Moor 強調規範性的隱私界限可依時、依地、依群體而有所不同(Moor,1997)，且根據 OECD 個人資料保護原則中的公開原則表示，凡有關個人資料之蒐集皆應制定一份公開性的政策，說明其使用目的與方法，及使用資料者之特徵與所在地。因此，銀行應根據本身之條件，制訂一份完整的隱私權政策，將有助於避免引發隱私權之爭議。根據 Moor 的建議，隱私權政策可透過理性的決策過程（如：公開及理性的辯論方式）來制定完成。該政策應同時考量使用者（即銀行）與被蒐集資料者（即銀行之顧客）雙方面的需求(Moor,1997)。依據美國國家衛生署（National Institute of Health）的認定，一份正式的通知應包括下列五個要素(Brown,et. al,1998)：

1.個人必須被告知資料蒐集的程序及目的；
2.個人必須被告知提供資料的可得利益；
3.個人必須被告知參與後的合理預期風險；
4.蒐集資料的機構須有回答相關問題的人員；
5.個人可隨時要求自資料庫中刪除名單。

我們同時也採用 Moor 的公開原則來看待這份隱私權政策的內容，至少應包括那些項目。首先，該份政策應確切告知顧客有關資料探勘技術的存在及資料探勘所使用之資料來源包括那些；其次，應告知顧客蒐集資料的目的，及其資料被資料探勘的技術應用之方式，同時告訴顧客個人資料輸入方式有二種，並以加密保護，且探勘的結果將以密函之方式通知，最後，應將業務呈辦人員所應遵守之倫理守則詳列於政策上，作為規範。此外，銀行應派專人為申貸者解說隱私權政策中有關資料利用之方式，在正式取得顧客同意後，銀行始得進行該顧客之申貸後續作業。

期望每個顧客了解資料探勘的技術是不合理的，但至少讓顧客知道資料探勘技術的應用，及整個申貸流程中，銀行對個人資料的處理方式。當顧客看完這份政策內容後，即可依其意願自由選擇是否確定要進行交易（如：申請貸款）。有了這份公開且公正之隱私權政策，除了在蒐集個人資料前先告知顧客蒐集資料的目的及使用之技術，且將資料用於當初指定之目的，同時告之資料的來源，以確保用來作為資料探勘分析的所有個人資料，無論是內部或外部資料，在蒐集前皆能取得當事者同意，如此即符合指定目的及使用限制之原則。銀行以這份隱私權政策作為保護顧客隱私之規範依據，可使得顧客的隱私免於受到威脅。

（二）個人資料輸入系統之處理

若申請者在了解所有相關問題後，表示願意接受徵信調查，則可填寫相關個人資料，並將這些個人資料輸入系統中。在此有二種作法，一種由申請者自行將資料輸入電腦系統，另一種由業務承辦人員將資料輸入。第一種做法由銀行給予申請者一組帳號及密碼，除個人基本資料外，其他資料由申請者自行輸入，輸

入後之資料即加密保護，爾後若申請者不願申請貸款，亦可提出刪除資料之請求。因資料輸入系統後即予以加密保護，故不論是第一或第二種做法，皆可保有其隱私。同時，系統應依業務性質之不同給予承辦人員不同之存取權限，以確保資料不會被不當地存取使用。此外，因資料來源除了內部資料外，尚有其他外部資料，為避免資料有誤而致影響探勘結果，申請者可要求審視有關其個人之相關資料，一旦發現有誤，只要申請者提出證明，銀行即應予以更正。

（三）以密函處理探勘結果

以 Lee 的假設個案來看，銀行運用資料探勘技術來處理申請貸款案件，最後出現的資訊並不在 Lee 當初所填寫的任何資料中，對於銀行而言，他們也無法預測在資料探勘的過程中，執行樣式配對演算法後將出現何種資訊，因此，較恰當的做法為，將探勘結果的資訊以密函之方式寄達申請貸款者手中，也就是說，連銀行也無從得知配對結果，該資訊僅當事人知道，由當事人自行判斷是否要將結果公開。若結果判定符合申貸條件，則由申貸者自行攜帶探勘結果，前往銀行辦理後續作業；若結果判定不符合申貸條件，則由申請者自行決定是否要公開結果，繼續爭取申請貸款；倘若不願繼續，則向銀行提出刪除個人資料及探勘結果。以 Lee 而言，當他得知被歸屬至「行銷經理很可能自行創業，同時在一年內宣告破產。」群組中時，若他認為自己毫無創業之意願，且願意至銀行說明，以爭取貸款機會，則是 Lee 自己願意讓自己置於「喪失隱私情境」中，就銀行的立場而言，自然無侵犯 Lee 隱私之虞。

個人為了掌控對隱私的管理，可由三種方式來進行：選擇、同意、更正(Tavani & Moor,2001)。讓個人自由選擇保護隱私的程度、取得其同意，並提供更正錯誤資訊之管道，乃對隱私有效管理之方式，本文所提供之申貸流程完全符合這三項要件，且因一開始即指定資料使用之目的，在整個過程中亦無不符合指定目的之使用，故完全不違反 OECD 個人資料保護原則中的「指定目的」及「使用限制」二個原則。

伍、結論

資訊技術應用所引發之倫理問題的解決方法，無論是以法律規範、道德勸說等，仍舊是被動的解決模式。本文為首次以較積極主動的手段，從改善實際作業流程，來解決資訊倫理的爭議。文中所提出的解決侵犯隱私權方案，乃針對 Lee 的申貸個案所設計，我們發現，只要銀行管理作業運用得當，妥善處理顧客個人資訊，資料探勘技術的應用未必會引發隱私爭議。

為了保障個人資訊的隱私，除了要普及資訊倫理教育，及加強電腦專業人員之資訊倫理素養外，政府亦應設立個人資料保護的專責機構。在消費者意識抬頭的今日，如何發展一個機制，在資訊技術的發展與保護個人隱私之間取得平衡點，是值得大家深思的問題。

參考資料

1.Brown, D.J. et al. “Information & Ethics in Insurance,” *CPCU Journal* (51:4)1998, pp:227-237

2.DeCew, J. W. *In Pursuit of Privacy：Law, Ethics and the Rise of Technology*, Cornell University Press, New York, 1997

3.Fischer-Hubner, S. “Privacy and Security at Risk in the Global Information Society,” in Thomas, D. and Loader, B.D. ed., *Cybercrime*, Routledge, London, 2000, pp:173-192

4.Fried, C. “Privacy,” *Yale Law Journal*（77）1968,p: 477

5.Han, J. and Kamber, M. *Data Mining：*

Concepts and Techniques, Academic Press, San Francisco, 2001
6.Holvast, J. *Vulnerability and Privacy*, North-Holland, New York, 1993
7.Johnson, D.G. *Computer Ethics*, Prentice Hall, Upper Saddle River, 1994
8.Mason, R.O. “Four Ethical Issues of the Information Age,” *Management Information Systems Quarterly* (10:1)1986, pp:5-12
9.Moor, J.H. “Towards a Theory of Privacy in the Information Age,” *Computers and Society* (27:3)1997, pp:27-32
10.OECD, “Guidelines on the Protection on Privacy and Transborder Flows of Personal Data,” <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>.
11.Rachels, J. “Why Privacy Is Important,” *Philosophy and Public Affairs*, (4)Summer 1975, pp:323-333
12.Regan, P. *Legislating Privacy：Technology, Social Values, and Public Policy*, University of North Carolina Press, Chapel Hill, 1995
13.Rosenberg, R.S. *The Social Impact of Computers*, Academic Press, Boston, 1992
14.Tavani, H.T. "KDD, Data Mining, and the Challenge for Normative Privacy," *Ethics and Information Technology* (1:4)1999, pp:265-273
15.Tavani, H.T. ”Informational Privacy, Data Mining, and the Internet,” *Ethics and Information Technology* (1:2)1999,pp: 137-145
16.Tavani, H.T. and Moor, J.H. "Privacy Protection, Control of Information, and Privacy-enhancing Technologies," *Computers and Society* (31:1)2001, pp:6-11
17.Warren, S.D. and Brandeis, L.D. “The Right to Privacy,” *Harvard Law Review* (14:5)1890, pp:193-220
18.Westin, A.F. and Baker, M.A. *Databanks in a Free Society*, Quadrangle/New York Times Book Co., New York, 1972
19.Westin, A.F. *Privacy and Freedom*, Anatheum Press , New York, 1967
20.Wong, J. S. K., et al. “A Framework for a World Wide Web-based Data Mining System,” *Journal of Network and Computer Applications* (21) 1998, pp:163-185