國立政治大學法學院碩士在職專班

碩士學位論文

指導教授 陳起行 博士

我國與美國聯邦對身分竊用法律之比較研究

A Comparative Study on the Identity Theft related Laws and Practices of Taiwan (R.O.C.) and U.S.A.

研究生 徐子文 撰

中　華　民　國　一　0　一　年　九　月

國立政治大學法學院碩士在職專班

碩士論文學位考試

論文題目：我國與美國聯邦對身份竊用法律之比較研究

指導教授：陳起行博士

研究生：徐子文

口試地點：綜合院館北棟 14 樓法學院第三研討室

考試委員 蔡蕙芳

考試委員 劉定基

考試委員 陳起行

中華民國 101 年 08 月 08 日

謝辭

本篇論文從題目構思、預研究到撰寫論文計畫，經過了三個月時間；真正緊鑼密鼓進行論文研究撰寫到口試通過及定稿，則又經過六個月的時間。這是作者的第三篇碩士學位論文，雖然沒有一篇論文是輕鬆完成的，但卻仍覺得這篇論文投注的精力和時間遠甚於前。第一篇論文是十多年前在英國完成的，當時是個剛揮別六年軍旅生涯不久，「投戎歸筆」的全職學生，雖負笈他鄉，讀書和生活都具挑戰，論文研究撰寫過程也頗有曲折，但至少可以全心全意的進行。第二篇和本篇則是分別在母校的商學院 EMBA 和法學院碩士在職專班期間，利用公餘假日累積點滴斷續的時間，一字字把它們完成。因為要同時兼顧公司的工作績效和個人的學習研究成果，時間和資源的分配常常遇到挑戰，所以當論文通過獲得學位時，那種喜悅和成就感也就更加珍惜。

而在研究撰寫本篇論文時，因為本研究主題在國內中文相關的研究成果並不多，所以徵引的參考資料必須直接自美國的英文素材中搜集。除了需要大量研讀參考美國的立法歷程、期刊文章和專題研究報告，供本研究使用，還要思考如何妥適的翻譯成適切的中文法律文字用語融入論文中。與之前兩篇論文基本上僅用英文和中文單一語言環境時比較，所花的精力實有數倍之多。但也因此，作者自己在此研究

學習過程中所得也因此而更加豐富。

這篇論文的完成，要感謝母校政大法學院恩師們讓作者在法學領域獲得啟蒙和指引，更要感謝陳起行老師願意擔任作者的指導教授，引導作者順利進行和完成論文研究和撰寫。另外還要感謝蔡惠芳老師和劉定基老師在學位考試過程對作者論文的精闢指導及釜正。雖然如此，作者的研究漏萬不足之處仍多，也希望各方家前輩不吝指導。

篇末，讓我再特別謝謝我的愛妻攸攸和家人，沒有你們這些年來的支持和體諒，這些美好，都無法成真。僅以此論文獻給你們！

中文摘要

因為資通訊科技之普及發達，提升經濟、社會活動的便捷性並豐富人們的生活品質，但一面兩刃，它同時也蘊藏了新興犯罪的機會，對經濟、社會活動之正常運作帶來威脅。其中，身分資料偷竊及身分冒用（以下簡稱「身分竊用」），已然成為資訊社會時代嚴重的新興犯罪之一。「身分竊用」一般俗稱為「身分竊盜」，其係由英文原文 identity theft 直譯而來。其實身分無從竊盜起，英文原文的 identity theft 其實也是簡稱，完整的意義是 identity theft and assumption，係指行為人未經授權擅用他人用已表彰其身分的證明或資訊，從而冒用他人之身分，遂行各式活動。本研究為求接近其實際文意內涵，在本研究中將其譯為「身分竊用」。

同為自由開放和高度科技化之社會，美國法律制度和社會機制環境雖與我多有不同，但其面對相同問題時的所受之影響和相對處理方式，或可為我國在處理同類問題時之參考。美國在身分竊用之相關法律，自從 1970 年代以降，至少制定 20 件以上的相關法律。先是從個人金融隱私權的保護著手，如在 1970 年制定《公平信用報告法》(*FCRA*)、1974 年所制定的《隱私權法》(*Privacy Act*)。1998 年則進一步制定通過《身分竊用嚇阻法》(*Identity Theft and Assumption Deterrence Act*)，明文規範「身分竊用」為刑事犯罪行為。《身分竊用嚇阻法》最重要

價值是確認了身分被竊用的人也是犯罪被害者，相較於之前只有因犯罪者使用身分竊用手法而被詐騙失去財務的人才被認為是受害者[1]，有了很大的進步。而之後的法律制定和實務處理即朝向個人資料保護、身分竊用預防和損害抑制，以及執法訴追等方向前進。

本研究以身分識別理論為起點，探討身分竊用在現代資訊社會中之角色和因身分識別資料被竊取冒用所發生之行為對個人社會和經濟的影響，蒐集美國聯邦自 1970 代迄今所制定和處理身分竊用相關之法律並予以摘錄分類，最後比較兩國對身分竊用問題處理之異同，並嘗試提出借鏡調和應用的建議。本研究蒐集整理，並將其群組為四種類型。分別是：（一）身分竊用罪法群；（二）個人身分證之相關法群；（三）消費者信用報告法群，以及（四）個人資料保護法群。

本研究發現，我國和美國雖然均面臨到身分竊用的問題，但因為國情和制度的不同，所受到的影響程度和所採取對應問題的方式也因此不同。例如：我國和美國在對個人識別號碼的態度和處理不同，美國是盡量打破個人利用單一獨特(unique)號碼進行識別的機制，而我國則是大量的使用。在個人身分證明文件上，我國較為統一，美國則較為分散，迄今尚未有全國統一性的身分識別證。在個人識別資料庫的建置和運用上，我國相對集中，美國重分散。我國對個人資料的保

[1]當時這類犯罪手法被稱為是 identity fraud

護是遵循歐盟模式，採取從上而下立法的方式。相反的，美國在個人資料保護作為上比較傾向建置一個結合法規、命令和自我管理的架構，而非由政府制訂的單一法規，係採由下而上模式。我國現在使用的國民身分證和身分證號在實體世界所建構的通用身分識別體系，因為個人資料庫雖分散但可集中連線查詢管理的特性，其在身分竊用防制機制的優勢因此建立。美國在對抗身分竊用問題所採取的方式雖因為國情和歷史的不同而和我國有相當程度的差異，但其在犯罪嚇阻控制上特別注意建立執法機關的查緝能力、訴追工具和司法機關量刑裁判的嚇阻效益，仍值得我國學習。本研究對於「美國聯邦量刑委員會」在其《量刑基準》上針對身分竊用罪的量刑考量及該委員會如此設計之源由稍有描述，或可為後續研究或實務參考之用。

關鍵字：身分竊用、身分竊盜、身分詐欺、冒用身分、個人資料保護、電腦犯罪。

(空白頁)

英文摘要(ABSTRACT)

Title: A Comparative Study on the Identity Theft related Laws and Practices of Taiwan (R.O.C.) and U.S.A.

Author: Daniel Tzu-Wen Hsu

Supervisor: Professor Chi-Shing Chen, S.J.D.

Identity theft is a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. The first victim of identity theft is the person whose identity has been assumed by the identity thief and this person can suffer adverse consequences if they are held accountable for the perpetrator's actions. The other victims are those who were defrauded by identity theft tactics. Along with the prevalence of information and communication technology, identity theft is becoming a great threat to common people and even to national security.

This study has collected more than 20 pieces of U.S.A. federal acts and statutes that related to combating identity theft problems. This study then categorizes then into 4 groups, namely 1) identity theft criminalization; 2) national personal identification system; 3) consumer credit report; and 4) personal data protection. In the mean time, this study also collected related laws and Taiwan (R.O.C.) for comparison.

The government organization structures and legal systems between U.S.A. and Taiwan (R.O.C.) are very different, though the common goal of

fighting identity theft is the same; the measures are quite different as well. In short, in terms of laws and personal identification system, the U.S.A. is more decentralized while in Taiwan (R.O.C.) it is more centralized. Taiwan (R.O.C.) has a national-wide and unified personal identification system that put it in a better position to respond and mitigate to identity theft impacts. On the other hand, from the law enforceability aspect, the study finds the U.S.A. provides better tools to law enforcement agencies and prosecutors to bring the offenders to justice in court and the judges have relatively more clear guidelines for case consideration and sentence.

Key Words: Identity Theft, Identity Fraud, Privacy, Personal Data Protection, Cyber Crime.

目次

圖表目錄

第一章 緒論

第一節 研究動機

自二十世紀晚期起，因為資通訊科技(Information and Communication Technology)之普及發達，因而帶動及提升新型態的經濟活動、增加社會的便捷性並豐富人們的生活品質，但在另一方面，新科技造就新環境，也同時成就新型態犯罪的機會，而對經濟、社會活動之正常運作帶來威脅。其中，身分竊用[2](Identity Theft)，已然成為資訊社會時代嚴重的新興犯罪之一。

作者從事企業安全風險管理多年，曾在航空運輸、電信和金融等國、內外跨國大型企業負責過台灣和東北亞區域的企業安全管理（企業資產安全防護、資訊安全、營業秘密及客戶資料保護政策、營運持續計畫和危機緊急應變）、法令遵循及金融犯罪風險（反洗錢及打擊資助恐怖主義、交易監察及報告、反貪腐、反詐騙和遵法內部調查等）等之政策制定、推行和督導等工作。在工作經驗中，作者觀察和見證到不少因個人資料被不當取得，進而利用該等資料冒名所進行之非法

[2] 俗稱「身分竊用」，其係由英文原文 identity theft 直譯而來。其實身分無從竊盜起，identity theft 意義中之 theft 實指身分資料或證明文件的被竊取，之後造成身分的被冒用(assumption)。本研究為求接近其實際文意內涵，將 identity theft 均譯為「身分竊用」。

行為，如不法份子利用人頭帳戶做詐騙和洗錢犯罪等現象。又，作者觀察，在我國新、舊個人資料保護法中，對個人資料的蒐集、處理和保管人(custodian)課與非常多的責任和相對沉重的罰則。但對使用不法獲得之個人資料，進而進行犯罪行為的不法份子卻似乎無相對應的規定和實效作為。以利用身分竊用手段進行的詐欺為例，似乎現行法律較關注於詐欺行為人和詐欺犯罪行為最後端被害人，較少注意到被冒名之人亦為犯罪被害人，而且係為第一被害人。而現行關於詐欺犯罪之司法實務處理，又因為被定罪和處分與犯罪所得利益之間顯著不對稱，尚難看出對詐欺犯罪行為產生嚇阻。作者遂直觀以為，在身分竊用問題中，我國在政策、法律的制定和司法實務上似有偏頗與不足。

作者以為，在各種個人資料的不法利用中，以利用身分竊用手段從事不法行為，對身分竊用的各階段受害人的名譽、財務、信用和間接引起的社會安定、經濟穩定所造成的影響最大和深廣，也因此是應是個人資料保護的重點目標之一。而根據美國聯邦貿易委員會(FTC)的統計資料也顯示，身分竊用問題已經對美國民眾生活造成嚴重威脅。據該委員會的報告指出，要清楚界定資料外洩和身分竊用之間的關連是相當困難的，因為身分竊用的受害者常常不知道他們的個人資料何時被他人不法使用，而且身分竊用被害人往往無法得知自己已經被害。

[3]因此，美國對身分竊用的法律策略重點，不再只針對個人隱私權和資料的保護，規範個人資料的蒐集、處理和保管人的責任義務，轉而加強對個人資料的不法利用的防制，特別是將身分竊用行為明確入罪化。

美國在身分竊用之相關法律，自從 1970 年代以降，至少制定 20 件以上的相關法律。如在 1970 年制定《公平信用報告法》(*Fair Credit Reporting Act*)、1974 年所制定的《隱私權法》(*Privacy Act of 1974*)。1998 年則制定通過《身分竊用嚇阻法》(*The Identity Theft and Assumption Deterrence Act of 1998*)，這是美國聯邦階層針對身分竊用問題的第一個專法，明文規範身分竊用為刑事犯罪行為。《公平信用報告法》把「身分竊用」定義為：「未經個人同意，使用或意圖使用有效的信用卡；未經同意，使用或意圖使用有效的帳戶」（例如支票帳戶）；挪用他人的個人身分資料以申請銀行帳戶、貸款或從事其他犯罪行為」。相較於之前只有因犯罪者使用身分竊用手法而被詐騙失去財務的人才被認為是受害者，《身分竊用嚇阻法》最重要價值是真正的確認了身分被竊用的人也是犯罪被害者。

作者以為，同為自由開放和高度科技化之社會，且美國於個人隱私和個人資料保護相關領域也被視為立於尖端領導地位。其法律制度

[3] "Federal Trade Commission – 2006 Identity Theft Survey Report", Synovate, November 2007, at 4 available at http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf, (Last visited on 2012/06/01)

和社會機制環境雖與我多有不同，但其面對相同問題時的所受之影響和相對處理方式，應可為我在處理同類問題時之參考。

第二節　研究範圍

本研究範圍中，「身分竊用」的定義係針對冒用他人身分衍生進行的詐騙犯罪為切入點。參照我國警政及犯罪學相關研究，對於詐騙所需的人頭資料的來源，主要可分成三種，一是偽造證件向銀行或公司申請被冒名人之進一步資料；二是向販賣者購買已申請好的名義，如銀行帳戶或電話，或是直接購買身分證件來申辦之；第三則是從非自願提供個人身分資料者而來，如用拾獲的證件或用各種方法騙取或偷取他人身分證件者來申辦人頭帳戶，[4]以及不法利用他人個人資料在網路上的應用和活動上：因為這類網路活動毋須驗證實體證件，僅輸入個人相關資料即可開立帳戶，進而進行虛擬貨物甚至是實際物品之交易或其他活動。其中第二項所列之手法，因係身分資料擁有者本人自願配合提供，故其本質非屬身分被冒用，在司法實務上對於提供該等提供其個人身分及資料供犯罪使用的，在詐欺案件上，亦幾乎以共同正犯論之，故與以排除。本研究中，身分竊用被害人的定義係針

[4] 參考廖有祿、江芝迎，「冒用人頭資料犯罪及相關防制對策」，《刑事政策與犯罪研究論文集(12)》，法務部編印，2009/12。

對第一項和第三項，非自願提供身分資料者為主體，因其身分被冒用而進行犯罪，實際上為身分竊用行為之第一被害人。

在界定本身分竊用犯罪被害人範圍後，本研究藉文獻研究法，蒐集美國有關處理和預防與前述身分竊用定義問題，在聯邦階層所倡議實施的相關法案、法律與判決及行政實務，並和本國法律與實務進行比較。

第三節　研究方法

本研究以文獻研究法，比較現行我國與美國聯邦有關個人身分識別，個人資料保護和處罰身分竊用的實務和法律。在論述方式上，以身分識別理論為起點，探討其在現代資訊社會中之角色和因身分識別資料被竊取冒用所發生之身分竊用行為對個人社會和經濟的影響；了解兩國在身分識別上個人資料運用上的實務；比較現行我國與美國聯邦有關個人資料保護和處罰身分竊用的實務和法律，了解美國聯邦將和身分竊用關的個人資料保護方向及身分竊用獨立成罪的理由和歷程，進而分析比較美國聯邦與我國現行法律對身分竊用問題處理之異同，並思考如何借鏡調和應用於我國。因身分竊用是個人資料和隱私權的重要保護目的之一，故在本身分竊用法律研究中必然和個人資料

保護和隱私權的議題有不少交合之處，惟為求研究標的集中，本研究範圍僅會提及與身分竊用問題直接相關之部分。

第二章 身分識別和身分竊用

身分竊用是在網路時代興起之前就有的犯罪型態。2002 年由名導演史帝芬史匹柏(Steven A. Spielberg)執導的電影「神鬼交鋒(Catch me if You can)」就是根據 1960 年代一個少年身分竊賊的真實故事改編。片中的主角 Frank W. Abagnale 是真有其人，他由於雙親突然決定離婚而離家出走，出走後的他不當利用老天賦予的天賦，開始了其傳奇的犯罪冒險之旅，從 1964 年到 1966 年的 2 年之中，他化身為不同的人士，從假扮泛美航空公司(Pan Am)副駕駛、喬治亞醫院小兒科住院總醫師、路易西安那州首席檢察長助理以及巴黎大學的美國史教授等各種不同領域的身分，還利用一些不存在的人開出高達 600 萬美金的空頭支票，詐騙地點遍及美國 50 州與 26 個國家。而當法蘭克被捕時，他的年紀還不滿 18 歲！

雖然身分竊用犯罪早在網路科技發達之前就已經存在，但是網路世界無遠弗屆的特性，卻大大提升身分竊賊的犯罪能力。在現代資訊化科技網際網路的幫助下，紙筆式的客戶服務或財務記帳幾乎已經不存在了。取而代之的是大型的數據資料庫。這些數據資料庫不只儲存客戶資料，也幫助企業分析各種重要訊息如客戶的消費傾向，品質管理，公司的財務狀況等。但就像很多因為現代科技帶來的便利，這也成為一個兩面刃。這些重要的個人資料庫一但被犯罪者入侵，這些數

據資料庫就好像金銀寶庫一樣，馬上可以獲的成千上萬的個人私密資料，用來作為其犯罪之用。網路也使的身分竊用成為一個專業分工的產業，有電腦程式高手扮演駭客(hacker)，專門撰寫駭客程式，有些是販售駭客程式圖利，有些則是破解企業數據庫，取得訊息，再轉賣他人。當然也有人願意出高價買這些訊息，用意則可想而知。各種網路技術的發展，也使得執法機構能夠阻止或抓到這些罪犯進而將其定罪的困難度大大增加。更深的事實是，身為資訊社會下的我們，為了獲得商品服務和與人交流，是無法避免必須讓別人取得自己的個人訊息。當使用個人資料成為一種必須且普遍的行為，個人資料的外洩就很難防範，也無法保證自己不會成為身分竊用犯罪的受害者。

第一節　身分識別理論

人們總是通過一些身分資訊(Identity Information)或識別憑證(Identifier)來證明自己或識別他人的身分。從本質上說，作為一種內在屬性，一個人的身分是無法被偷去的，身分只能被假冒；實際上能被偷去的是那些用來識別身分的身分資訊或識別憑證。身分竊賊首先必須竊取足夠的他人身分資訊，然後才能非法冒充他人以獲取利益。到了現代社會，Clarke 認為，從資訊系統的角度看，身分識別是「將

數據與具體的人相結合的過程」。[5]因此，身分竊用問題可以看成是一種特殊的資訊管理或者資訊安全問題。

Clarke提出，識別身分的方法主要有：(1)基於知識或資訊的識別：即判斷一個人「知道什麼」，例如：密碼、口令、身分證號等；(2)基於憑證的識別：即判斷一個人「擁有什麼」，例如：身分證，護照、信用卡、介紹信等；(3)生物性識別：即通過一個人的外貌、指紋、虹膜、聲音等生物性特徵以及一個人的行為資訊來識別身分。除了生物性資訊是源自於本身，所以很難被竊用外，其它資訊都是外界賦予或後天經人為創造出的，這些資訊是有可能被竊用或假冒的。

最真切的身分識別應是個人獨特之生物特徵，以現今科技能得著應為「去氧核醣核酸」(deoxyribonucleic acid: DNA)編序、視網膜、指紋和面部特徵等。惟此種身分識別恐侵犯人民隱私權，因太具爭議性，故僅適用於特別環境和情況，以符法律保留及比例原則。司法院大法官釋字第 603 號解釋文就有如此解釋。目前為止，唯一通用且較無爭議的生物特徵識別之個人資料係相貌，一般方式係以相片或其他影像資料方式存儲運用。但個人相貌本身就不是個精確的「憑證」，所以尚不足為單一有效的身分識別方式。

Lopucki 對 Clarke 的理論進行了擴展，他提出身分識別是一個「特

[5] CLARKE R . Human Identification in Information Systems : Management Challenges and Public Policy Issues[J] . Information Technology & People, 1994, 7(4) : 6- 37.

徵值」 (Characteristic Values)匹配過程，而且特徵值必須是識別行為雙方都掌握才行[6]。特徵值可能是姓名、身分證號、密碼、相貌、指紋，等等。身分識別者（可能是人，也可能是系統）總是通過對比自己所掌握的特徵值與對方所出示的特徵值是否匹配來識別對方的身分。例如，我們通常通過相貌來識別朋友，而朋友的獨特相貌就是他的特徵值之一。Lopucki 還提出，身分識別是分層的，有時身分識別需要前一階段提供的證明資訊。這是因為身分識別者所掌握的特徵值經常並非直接觀察得到，而是依靠一些間接記錄。[7]因此，身分識別的準確性取決於前一階段身分識別的準確性。例如，我們到銀行開戶和辦理自動櫃員機(ATM)提款卡需要出示身分證來證明自己的身分，如果身分證是假的，那麼銀行所發出的 ATM 卡對該假身分證上資料的本人也是無效的。Clark 雖然沒有提出身分識別過程的分層性質，但他也指出，很多身分證明文件的產生需要「種子文件」(seed documents)作為基礎。例如我們申請護照時需要提供身分證和戶口名簿。種子文件可能是出生證明(birth certificate)、居住證明、移民文件等等，其中最重要和起基礎作用的就是出生證明。[8]

不同情境下，識別身分所需要的身分資訊的質量和數量是有很大

[6] LOPUCKI L M. Human Identification Theory and Identity Theft Problem[J] . Texas Law Review, 2001, 80(1) : 89- 136.
[7] *Ibid*.
[8] CLARKE R (1994)

差異的，例如在遠端申請信用卡開卡服務時，我們需要提供一系列的個人資料；而在使用電子郵件服務時，只需要用戶名和密碼。有時身分識別需要採用多種識別方式的組合，例如我們在自動櫃員機(ATM)上取款時，既需要擁有 ATM 卡（基於憑證的識別）又需要知道密碼（基於資訊的識別），ATM 機才會認為我們是合法用戶。

Willox 和 Thomas 進一步指出，在身分識別的最開始階段，身分識別者對目標沒有印象，目標也沒有任何的憑證資訊，因此，只能採用基於知識或資訊的識別方式，而無法採用基於憑證的或基於生物資訊的方法[9]。特別是在電子商務的經營環境下，由於其虛擬特性，基於資訊的識別應用尤其廣泛。Willox 和 Thomas 認為，理論上可以使基於資訊的識別變得非常安全。他們的假設前提是：冒名者不可能知道他人的全部個人資料，因此，只要用來識別身分的資訊足夠多，我們就可以準確的識別一個人的身分。但是，用於身分識別的特徵值必須是雙方都掌握才行，所以要求身分識別者必須收集到足夠數量和品質的個人身分資訊，但由此又會引出成本、隱私保護、識別過程效率等一系列問題。[10]

由於個人資訊的範圍相當廣泛，其所涵蓋的資訊類型亦相當多元、

[9] WILLOX N A, REGAN T. Identity Fraud: Providing a Solution [J] . Journal of Economic Crime Management , 2002, 1(1) : 2-17.

[10] *Ibid*.

複雜。如，黃昭元(2005)所提出之個人資訊分類如下：[11]

1. 個人的資訊或有關個人的資訊：

所謂個人資訊，可區分為「個人的資訊」(information of persons)和「有關個人的資訊」(information about persons)兩類。前者和個人不可分，通常具有獨特性與專屬性，如姓名、性別、年齡、五官面貌、身高、指紋、DNA 等。後者多半因個人的行為或活動所產生者，如教育程度、職業、財務狀態、婚姻狀態等。個人的資訊所具有的身分確認功能明顯高於有關個人的資訊。

2. 敏感或非敏感資訊

有些資訊對於個人具有一身專屬與高度隱密性或其揭露將對個人造成嚴重的影響者為敏感性資訊,如個人感情及性生活為具有一身專屬與高度隱密性之資訊;另如個人財務狀況、政治傾向等。其他則屬非敏感資訊。因敏感性資訊於個人具有一身專屬與高度隱密性或其揭露將對個人造成嚴重的影響，故對敏感性資訊的干預，應要從嚴審查。

3. 顯性型或隱性型資訊

如以資訊的解讀方式作區別,則可分為顯性型及隱性型的資訊。所謂顯性型資訊係指依一般人知識能力或經驗感官即可為認知,例如

[11] 黃昭元，「無指紋則無身分證？換發國民身分證與強制全民捺指紋的憲法爭議分析」,《民主、人權、國家 - 蘇俊雄教授七秩華祝壽論文集》, 2005 年 9 月, 頁 474、475。

個人之姓名、身高、性別等等。此種資訊通常以人工即可判讀，有一望即知，即可當場確認，如姓名；有些為半公開資訊，如身高。因而顯性型資訊敏感度或私密度較低，亦稱為人工判讀型資訊。而隱性型資訊則需透過機器才能判讀，甚至須經過特殊專業訓練的極少數人才能解讀機器的判讀結果，如血液、指紋、視網膜、虹膜、DNA 等各種生物特徵資訊，又稱機器判讀型資訊。

學術界在這一領域的研究成果是分散和起步性的，沒有形成系統的理論體系，還不足以為解決身分識別問題提供一個堅實的、可即用的理論基礎。[12]但這似乎也是必然的，因為就身分識別而言，其應用目的不一，方式多變，且會隨著時代進步而變化。

第二節　身分竊用的概念

第一項　從竊用途徑的角度來定義

身分竊用自古有之，並非是一種新型犯罪。比如，一方利用長相相似而冒充本人的故事在不少處傳出。而時至今日，金融機構還常常收到官方發送的文件，要求各機構注意某某人等之身分證被冒領的事

[12] 參考閩庆飞、季绍波、仲秋雁，「身分盗用的发展及其治理和研究趋势」，大连理工学院《公共管理学报》，第四卷，第一期， 2007 年 1 月。

件，常見的情況是本人之身分證被近親（大部分是兄弟姊妹，甚至有孿生手足）至戶政機關冒名掛失後冒領。雖偶有發生，但是此種類型的身分竊用的難度相對較大，因為這種身分的冒用必須還要有實體上的相似，機率低，所以受害範圍也相對較低。常見的身分竊用是竊取他人身分資料，偽造或變造他人身分證，將本人照片換成持證行為人的照片，以冒用他人身分，進行下階段之不法行為。

另有一說為，身分竊用真正被重視源於電腦和網際網路的廣泛應用。由於電腦使用日益頻繁，人與人之間並非按照傳統的物化標準(如長相)來區分，而是根據一系列的資訊來辨認。在美國，社會保險號碼、母親的姓、銀行帳號、信用卡卡號、電子郵件號碼已經成為最主要的識別身分的標準，而這些標準基本上都是用電腦進行處理。[13]因此，身分竊用犯罪常被認為是資訊時代的產物。

第二項　從竊用目的的角度來定義

歹徒竊用身分的目的主要在於實現其經濟目的。歹徒通過掌握被害人的名字、地址、社會保險號碼、銀行帳戶、信用卡卡號、母親的姓、出生年月日等個人資料，從而用被害人的身分來申請貸款，辦理信用卡等財務服務，將其財務責任嫁由身分本人負擔，從中牟取不法

[13] 參考陈立峰，「浅议身分盗用犯罪问题」，《江西公安专科学校学报》，第 6 期总第 98 期， 2005 年 11 月

利益的行為。其它的竊用目的則較多元，通常是為了獲得身分本人的特權(privilege)，如特殊通行權限等，以進行其他目的，如恐怖破壞行動等。本研究之範圍主要針對於前者，即歹徒竊用身分的目的主要在於實現其經濟目的。

第三項　從與詐騙犯罪比較的角度來定義

身分竊用與欺詐有一定的相似性。詐騙是指故意隱瞞真相、虛構事實以損害他人利益。而身分竊用往往是歹徒竊取被害人的名字、地址、社會保險號碼、銀行帳戶、信用卡卡號、母親的姓、出生年月日等個人資料並利用它們來冒充被害人的身分。而身分竊用的特徵即故意隱瞞真相、虛構事實的方式來損害他人利益。因此，身分竊用常見於詐欺罪一種手法，稱為「身分欺詐」(Identity Fraud)。

第四項　從竊用途徑和目的相結合的角度來定義

隨著社會的不斷發展和進步，以及一些新的身分竊用形式的出現，對身分竊用的定義也出現了新的發展。首先，雖然電腦是獲取身分資訊的主要途徑，但是並非是唯一途徑，因此，純粹從獲取資訊的途徑來定義顯然有失偏頗；其次，身分竊用不僅為了獲取經濟利益，有時候歹徒是利用被害人身分對他人進行侮辱或者誹謗。因此，目前對身

分竊用比較通行的定義是:非法獲取被害人個人資料來冒充其身分，以實現非法目的的行為。

第三節　身分竊用的過程

身分竊用的過程主要分為兩個步驟：一是竊用被害人個人資料；二是冒充被害人從事非法行為。竊用個人資料主要通過以下四個途徑:

一、被害人不認真管理個人資料

大多數身分竊用都是因被害人自己對個人資料管理不善，保護不全引起的。比如在自動取款機取款結束後沒有撕毀提款證明、將信用卡明細或帳單隨意丟棄在垃圾桶內，以及不慎被他人知道信用卡密碼。有時候在餐廳刷卡時也會被竊用個人資料。如果你將信用卡交給服務生付賬，除了一般刷卡過程外，也使用刷卡機記錄你的信用卡資訊。還有一個常見的方式是假冒借貸人員以低利吸引申請者提供個人資料。另外一個主要的方式就是求職陷阱。由於就業壓力的增大，一些歹徒便利用求職者求職心切，以招聘為幌子騙取求職者的個人資料。歹徒也會通過一些求職網站，那些求職者的簡歷上面會有他們的姓名、家庭住址和社會安全號碼等資訊。

二、利用網路竊用個人資料。如：

1, 假冒網際網路服務提供者(ISP)，要求用戶提供個人資料。即使多數 ISP 廠商已經表明，絕對不會要求使用者提供身分證號碼，但依舊有使用者回復此類郵件。

2, 網路釣魚術(Phishing)。網路釣魚術，又被稱為釣魚欺詐，是指駭客利用電子郵件誘騙受害者前往虛設的銀行或零售商的網站或電子郵件，哄騙消費者登錄他們的金融資料和密碼。因此，受害者的信用卡、銀行帳戶，甚至個人身分就可能被竊用。

3, 電腦入侵術(Pharming)。電腦入侵術，是指駭客通過操縱一台電腦的設置，因此用戶在訪問合法網站的時候將被直接引導向假冒網站，然後再利用網絡釣魚術騙取消費者的個人資料。

三、遺失實體身分證明文件

遺失身分證最容易產生身分的竊用。通常遺失的錢包裡會有身分證，犯罪集團可以相對輕鬆的變造身分證，設立銀行帳戶，進而申請信用卡。部分犯罪者會在很短的時間內將信用額度竊用一空，但有些罪犯會慢慢累積信用卡的信用額度，以便未來購買更高價的物品。

四、通過其他途徑獲得他人的個人資料

如在網際網路或實體世界上向個人資料蒐集者購買他人的個人資料。此類資料的來源可能來自合法或非法手段。例如在美國的新澤

西州，就曾有一個網站[14]，專門進行被竊的個人資料的交易。在台灣，利用「電話行銷名單」、「電訪名單」、「客戶名單」等關鍵字至各大搜尋引擎如 Google、Yahoo 等搜尋，就可輕易獲得。甚至有如「中華民國經貿企業文化協會」，以合法社團為掩護，大賣個人資料者。[15]

第四節　身分竊用的危害

根據美國聯邦貿易委員會的數字，2003 年，全球由於身分竊用所引起的直接經濟損失為 2,210 億美元，其中，美國損失 738 億，是 2002 年的 3 倍[16];美國有 2,700 萬人成為身分竊用犯罪的受害人，在每起身分竊用案件中，企業的平均損失是 10,200 美元，而消費者個人的平均損失是 1,180 美元。在很多案例中，受害人的信用等級遭到嚴重的損害，以至於無法申請貸款、抵押和信用卡，而受害人平均要用 60 個小時來解決身分竊用引起的麻煩。而且，受害人平均要 14 個月以後才能發現自己的身分被竊用，大約只有一半的受害人知道其身分資訊是如何被竊取的。[17]還有學者相信，身分竊用的實際發生量是報

[14] 即 www.shadowcrew.com

[15] 參見：臺灣臺北地方法院刑事判決 九十三年度訴字第四九五號

[16] U. S. Government. Committee on Ways and Means: Identity Theft Facts and Figures[R/OL] .[2004- 07-07] . http: //waysandmeans. house.gov/media/pdf/ss/factsfigures.pdf. (Checked on 2012-01-28)

[17] LAWSON P, LAWFORD J. Identity Theft: The Need for Consumer Protection[R] . Ottawa , Canada : The Public Interest Advocacy Center Working Paper, 2003.

告發生量的 8 倍。[18]除了金錢上的損失以外，還有很多更具傷害性的非經濟損失。如受害人有可能被銀行和信用卡公司追討債務，甚至由於別人冒用自己的身分犯下罪行而使自己遭到詢問或逮捕。此外，身分竊用的一個整體性社會成本就是使得消費者對線上電子商務的信任程度下降，由此所帶來的經濟損失是無法估量的。而且，像恐怖主義、洗錢、走私、販毒等惡性犯罪都常見以身分竊用為手段。

美國聯邦交易委員會(FTC)公布該組織 2011 年總計收到近 134 萬的消費者投訴案件，其中攸關身分竊用的投訴案件高達 25 萬，以 19% 名列十大投訴之首，這也是身分竊用第 11 次蟬聯冠軍。[19]身分竊用並非僅是消費者所面臨的威脅。各種組織以多樣化的方式處理、使用數量不斷提升的個人識別資訊時，身分竊用亦是重要課題。金融機構、信貸公司與政府機關等資料保存單位的機密資料外洩遭媒體宣傳報導，不但侵蝕公眾對於網際網路的信心，亦威脅壓迫線上商務及服務的成長。

軟體巨擘美國微軟公司(Microsoft)也曾在 2008 年 9 月發表名為「線上身分竊用：改變遊戲規則」[20]的白皮書。微軟認為數位形式的

[18] SLEWE T , HOOGENBOOM M. Who Will Rob You on the Digital Highway [J] . Communications of the ACM, 2004, 47(5) : 56-60, available at http://web.cs.dal.ca/~hathai/privacy/p56-slewe.pdf (Last checked on 2012/08/19)

[19] 參見 NII 產業發展協進網站，2011/03/09，http://www.i-security.tw/learn/sub_201106_1.asp

[20] "Online ID Theft: Changing the Game - Protecting Personal Information On The Internet", Microsoft Corp., 2008/9/16, available at http://download.microsoft.com/download/0/d/3/0d34ccfa-5498-4fab-bb32-16c881bafba7/Online%20ID%20Theft-%20Changing%20the%20Game.pdf, last check on 2012/05/12. 中文版「線上身分竊用：

「個人識別資訊」(Personal Identifiable Information: PII)是網際網路時代的命脈。因為個人、組織、企業、政府均願意信任服務供應商處理此類個人識別資訊，使得網際網路得以在過去十年間培植出種類繁多的新用途。個人識別資訊的存取不但促使電子商務與電子政府的應用實務產生爆炸性的成長，亦刺激各種線上社群的形成。無論是網路銀行與投資服務、旅遊與購物網站、電子報稅與換照等，均顯示出網際網路能開拓商機、提升效率、讓生活更加便利，並提供其他無數好處。

但個人識別資訊的廣泛運用除了有正面的效益外，負面影響亦同時產生，所以保障「個人識別資訊」安全的呼聲也越來越高漲。因為身分竊用者藉由網路釣魚[21]攻擊、間諜軟體[22]、社交工程詐騙及其他各種不當手法，在線上與離線管道收集個人資訊，並透過未授權的交易，以及利用不知情的消費者所建立的人頭信用戶，竊取了數百億美元的鉅款。雖然經由各界的努力和安全問題意識的提升，近來線上與離線身分竊用所造成的金融損失已稍減，但是在 2007 年，單是美國的受害金額仍高達 450 億美元。[23]

改變遊戲規則」, http://msdownload.longsun.net/privacy/Online-ID-Theft-Changing-the-Game.pdf, last check on 2012/05/12.

[21] 網路釣魚(phishing)：一種網際網路詐騙行為。加害人的目的為誘騙他人提供個人金融資訊，如銀行帳戶或信用卡資訊。常見手法 為傳送詐騙電子郵件，假冒為銀行、網際網路服務供應商或其他信任的來源，然後要求確認帳號或密碼。

[22] 間諜軟體(spyware)：未妥善告知，且未經使用者同意，暗中安裝於個人電腦的電腦軟體，其目的為攔截資料或部分控制使用者與 電腦之間的互動。

[23] "One person in eight in the EU27 avoids e-shopping because of security concerns", News Release, Eurostat, European Commission, February 2008. Available at http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-08022008-AP/EN/4-08022008-AP-EN.PDF (Last

2007 年歐盟商務委員會(European Commission)的報告[24]也指出：線上詐騙正動搖著大眾對網際網路的信心，並減緩線上商務及其他服務的成長。在 2006 年，年齡 16 至 74 歲的歐盟居民當中，有 12%表示曾因安全考量而避免線上購物。相比之下，共有 57%的受訪者曾使用網際網路，30%表示曾在 2007 年於線上購物。

當今網際網路環境是身分竊用者的溫床。他們開發多種狡猾手法竊用個人資訊，甚至在線上加以販售。例如，某位調查員在 2008 年 5 月 McAfee Avert Labs 部落格上爆料指出，有網站邀請犯罪者在該站買賣他們竊自世界各地無辜消費者的信用卡卡號、銀行帳戶登入密碼及其他各種資料。[25]

在台灣，新興詐欺犯罪是其中影響最廣、禍害最深的。據警政署統計詐欺案件的被害金額目前躍升為財產犯罪的第二名，其犯案手法中，人頭帳戶及人頭電話正是不可或缺的必要工具。顯見冒用人頭資料的影響性，當它被歹徒濫用時所造成的犯罪，無論是類型、規模都相當複雜而龐大，也衝擊民眾對治安的信心，並增加偵辦難度。[26]

身分資料的竊用情形相當多，其犯罪手法主要應用在如人頭帳戶、人頭電話門號、人頭證券交易戶、人頭董事、盜刷信用卡等，不勝枚

---

visited on 2012/06/22)

[24] *Ibid*.

[25] Francois Paget, “You have to pay for quality”, McAfee Blog Central, 2008105/07, http://blogs.mcafee.com/mcafee-labs/you-have-to-pay-for-quality (Last visited on 2012/5/12)

[26] 引自廖有祿、江芝迎(2009)

舉。犯罪者利用收購而來的人頭帳戶、人頭電話、人頭證券交易戶等，遂行其他重大的犯罪，逃避警方追緝。歹徒擄人勒贖時，會利用人頭帳戶取款、人頭電話聯絡被害人；詐欺犯罪集團作案時，為避免警方追緝，和共犯也用人頭電話聯絡；還有利用人頭開公司，用以掩護非法交易或進行詐騙，甚至有心人士會利用人頭戶洗錢、炒股票，影響大者甚至有上億的違法資金流動。

俗稱之信用卡盜刷也是利用身分竊用手法的詐欺行為，同時這也是讓美國重視身分竊用問題的重要原因之一。國內著名的案例有「偽卡教父」范哲維偽卡集團案。2002 年間范哲維竊取被害人的個資，製造出 18 萬張偽卡，盜刷超過數十億元，曾經讓金融界損失慘重。范哲維之前在馬來西亞取得電話夾線側錄信用卡內碼的技術，先選定信用卡特約商店，再利用徵信社業者及電信外包商，以查線一件三千元、轉線一件五千元價碼，從戶外的電話轉接箱中，選定特定號碼，再選定安全地點拉線裝設音頻錄音設備，將所有交易資料全部攔截。並定期更換錄音設備，短期內即獲取大量的內碼資料。事後范哲維集團再以音頻解碼器，把截取的資料還原成信用卡原始資料，再以每條內碼一千到二千元不等價碼，賣給下游的偽卡製造者。范哲維靠著盜賣信用卡內碼及偽造信用卡，短短幾年內累積數十億財富。不過，最後范還是躲不過追緝落網，警方及聯合信用卡中心還公開表示，至少

可以為國內銀行節省三十億以上的損失，也適時解除了各銀行客戶資料遭人到走的金融危機。但是，范哲維第一次被捕時，只關了三個月就交保了，出獄後還重起爐灶，而當他再度落網，也只被法院依照偽造有價證券將他判刑四年六月，併科罰金折合台幣四十五萬元[27]，與信用卡銀行損失的近卅億元，實在不成比例。[28]也因為不法獲利豐厚而相對應之刑事處罰低，無怪乎范哲維會重起爐灶重操舊業，因而在2012 年 8 月出獄三年後又再度被落網。這次他轉向駭客購買上萬筆國外客戶資料，再製作偽卡盜刷，挑選高單價商品，像是金飾或是智慧型手機刷卡買入，然後再到網路上，低價賣出變現，短短 4 個月，盜刷金額高達 2 千多萬元。[29]

身分竊用不只被用來行詐欺取財行為，也會對被冒用人帶來意想不到的負面影響。例如，報載高雄某馮姓男子因被人冒用身分應訊，遭板橋地檢署起訴，後來地檢署還給清白，但在檢方犯罪資料庫中還是有他被起訴的紀錄。馮先生表示，他收到板橋地檢署過失傷害的起訴書，因起訴內容與他無關，還以為是詐騙信件，後來向板橋地檢署查詢，才知道北市一名吳姓男子 2007 年 12 月 15 日與人發生車禍，

[27] 臺灣板橋地方法院 93 年度訴字第 136 號判決。

[28] 參考自戴志揚，「偽卡惡風再起，追尋昔日料頭身影范哲維：縱橫東南亞的金融頭號要犯」，大眾時代，2006/12/13。來源：http://mass-age.com/wpmu/blog/2006/12/13/偽卡惡風再起，追尋昔日料頭身影范哲維：縱橫東 e/ ，(前次檢索日：2012/08/19)。

[29] 參考自 黃念慈，「盜刷逾兩千萬 偽卡教父再度落網 向駭客購買個資 月花 50 萬養酒女 出獄三年重操舊業 依詐欺罪送辦」，2012/08/17，台視全球資訊網，(前次檢索日：2012/08/19)。http://www.ttv.com.tw/101/08/1010817/10108174942203L.htm

被對方控告過失傷害，吳男卻以他的身分資料應訊，他因此被起訴，事後檢方查明他非肇事者。[30]

又如，我國刑事警察局和大陸公安以及印尼、柬埔寨、馬來西亞和泰國，於 2011 年發動代號「0310」的跨國掃蕩詐騙集團行動，兩岸六地動員上千警力，逮捕 598 人，創下治安史紀錄。其中台籍 410 人、大陸 181 人，泰籍、韓籍、越南和柬埔寨共 7 人。[31]接著，六月我國警方從東南亞押解數百名詐欺犯回台，許多嫌犯看到長榮專機來接都喜出望外，大聲歡呼。他們料定：以兩岸司法對待詐欺犯的差異，回台形同「減刑」的保證。[32]

而這些詐欺嫌犯們的歡呼不是沒有原因，一方面是因為相較於大陸和周邊國家，我國《刑法》對詐欺的本刑就不高，所以在審判宣判量刑後，詐欺犯所實際得到的懲罰也相對的輕。監察院於 98 年 4 月調查發現，詐騙案詐欺罪判刑 1 年以下與拘役、罰金之比例 89 年為 73.17% ，至 97 年增加為 96.48% ，顯示法院對詐欺罪量刑刑度有逐年趨輕之勢，遂於 98 年 9 月提出調查報告，報告意見指出：「詐欺犯罪案件量刑刑度及入監率均有逐年降低之趨勢，實難發揮刑罰應報、

[30] 蘋果日報，「身分被冒用 竟留起訴紀錄」，2010/04/22，http://tw.nextmedia.com/applenews/article/art_id/32454700/IssueID/20100422，（前次檢索日：2011/12/12）。

[31] NOWnews 今日新聞網，「《空中監獄》真實版　上百人犯包機押回台」，http://www.nownews.com/2011/06/11/91-2719526.htm#ixzz1gI0WwT2W，（前次檢索日：2011/12/12）。

[32] 聯合報社論，「當詐騙犯歡呼遣返的謎底揭曉」，2011/11/08，（前次檢索日：2011/12/12）。

嚇阻、隔離與矯正等功能…。」[33]身分竊用是詐欺常用的手法之一，對詐欺犯罪之處刑都已經如此，身分竊用在司法實務判決上實難有特別期待。

因為一般的冒用身分，不論是在實體世界還是在網際網路上，都會統合視為詐欺的手法的一種，因為在遂行該等犯罪行為時，均不免會經過偽造文書的過程，故冒用身分行為自然地落入被歸為偽造文書和行使偽造文書的罪行下。我國現行《刑法》和實務通常只把受詐欺的人當作是受害人，而且注重在其財產法益的保護和補償，但是對被冒用身分之人，在加害人實行詐欺過程時，其實應是第一個受害人，但法律給予的保護對待是否足夠，值得研究。

[33] 引自監察院 2011/11/10 發布之「詐欺犯罪案件量刑刑度新聞參考資料」。又，詐欺罪判刑 1 年以下與拘役、罰金等低刑度案件之比例仍居高不下，由 97 年 96.48%、98 年 96.98%至 99 年 96.92%，各法院對詐欺罪量刑刑度偏低，實難以遏阻詐欺犯罪案件蔓延。

(空白頁)

第三章 美國處理身分竊用問題之相關法律

因為資訊科技的發展普及，已經深入且全面影響人們的生活和商務運行的方式。但不幸的，罪犯們的犯罪手法也跟著演化。以往需要實體的身分證明文件才能冒用他人身分的時代，因為資訊社會新的運作方式而被改變，現在只要擁有足夠的他人個人資料，就足以進行冒用身分的行為。

根據美國聯邦貿易委員會的統計資料顯示，身分竊用問題已經對美國民眾生活造成嚴重威脅。據美國聯邦貿易委員會的報告指出，要清楚界定資料外洩和身分竊用之間的關連是相當困難的，因為身分竊用的受害者常常不知道他們的個人資料何時被他人不法使用，而且身分竊用被害人往往無法得知自己已經被害。[34]

美國對身分竊用的問題很早就注意到，主要是因為因身分竊用所致生的或是為手段的詐騙事件頻傳，而且影響又因為資通科技的發達而迅速擴大，迫使美國政府必須拿出對應政策，加以控制。雖然在州法階層，1996 年亞利桑納州(Arizona)就已經成為第一個將身分竊用立法定義為刑事罪。[35]但將身分竊用定義成是一種聯邦罪則始自 1998 年。

[34] "Federal Trade Commission – 2006 Identity Theft Survey Report", Synovate, November 2007, at 4 available at http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf, (Last visited on 2012/06/01)

[35] FINKLEE, Kristin M., “Identity Theft: Trends and Issue”, CRS Report for Congress (R40599), Congressional Research Service, Library of Congress, February 2012. at 3

不過，美國在聯邦階層對抗日益嚴重的身分竊用問題並不是將身分竊用立法定義為聯邦罪才開始，其相關作為起始時間可回溯 20 年以上。為了防制身分竊用以及和緩彌補身分竊用被害，遠溯自 1970 年代起，美國聯邦階層則開始制定並施行一系列與處理身分竊用的問題有關的法律[36]。本研究蒐集整理，並將其群組為四種類型。分別是：

（一）身分竊用罪法群：係指偽造身分證明文件相關之詐騙犯罪及將身分竊用入罪化的相關法律；

（二）個人身分證之相關法群：係指規範建立管理全國性身分證明文件的相關法律。[37]

（三）消費者信用報告法群：係指規範處理消費者信用和消費報告的保護管理和當個人身分遭竊用後，信用資料因而受損，如何回復其原有之信用評等和合理限制其信用債務責任等相關法律。

（四）個人資料保護法群：係指規範個人資料的蒐集、使用和保護的相關法律，避免個人資料遭到不法使用，協助防止身分竊用問

[36] *See* Sara R. Paul, "Features - Identity Theft: Outline of Federal Statutes and Bibliography of Select Resources", 2006/02/07 (http://www.llrx.com/features/idtheftguide.htm. (Last visited on 2012/04/30)

[37] 美國並無全國一致的個人身分識別證，有的僅係各州自行管理授發的駕駛執照和州居民身分證。自 911 事件後，美國聯邦試圖建立一套全國性的駕駛執照其個人身分證授發及管理標準，以對應原來恐怖份子可以相對輕易的獲得州所授發的身分證明文件（如駕駛執照）。雖然這部分原本並非是為了解決身分竊用問題而設，且因美國國會對於這部分的提案和法律通過後尚未獲得各州全數的同意，甚至有隱私保護團體主張這些法案有違反美國憲法之虞，這類的法律尚在發展中，但整個歷程演進仍值得關注。因為其有協助處理身分竊用問題的綜效(synergy)，並且為了便於和我國的身分證制度作比較，故在本研究中予以納入討論。

題氾濫。

第一節　「身分竊用罪」入罪之相關法律

第一項　1982 年《虛偽身分證明文件犯罪控制法》

1982 年通過施行的《虛偽身分證明文件犯罪控制法》(*False Identification Crime Control Act*)是為了打擊使用偽造身分證明文件來進行的詐欺活動。本法在《美國聯邦法典》上增加了兩個章節，分別是 18 U.S.C. §1028「與身分證明有關的詐騙和犯罪活動」和 18 U.S.C. §1738「郵寄私人身分識別文件未加入免責聲明」[38]規範了製造或運輸偽造或偷得之身分證明文件所要面臨的刑責。本法同時禁止製造、運輸或持有任何以製作偽冒文件為目的的裝置。但本法的條文內「文件」這個字，被解釋為必須是實體文件[39]，讓其構成要件之適用因此侷限。也因而催生了《網際網路虛假身分防範法》(*Internet False Identification Act*)，以補足缺陷，如後述。

[38] 本條因《網際網路虛假身分防範法》之公布施行，已於 2000 年廢止。

[39] *See* Paul, Sara R., "Features - Identity Theft: Outline of Federal Statutes and Bibliography of Select Resources", 2006/02/07, http://www.llrx.com/features/idtheftguide.htm (Last visited on 2012/04/30)

第二項　1998 年《身分竊用嚇阻法》

1998 年的《身分竊用嚇阻法》*(Identity Theft and Assumption Deterrence Act*)[40]是第一部專門針對身分竊用問題而立的法。這也是第一次讓身分竊用成為一個正式的聯邦罪名，方便讓各級執法單位可以起訴罪嫌。在這之前，身分竊用只是一個簡單概念型罪刑分類，淺顯易懂的讓大眾及執法人員瞭解這種犯罪的手法及類型，而非實際罪名。

《身分竊用嚇阻法》亦引導「美國聯邦量刑委員會」(United States Sentencing Commission)，檢視並修正《聯邦量刑基準》(Federal Sentencing Guidelines)，對於身分竊用犯罪，訂定更為適當的罰則。

另外，《身分竊用嚇阻法》還規定聯邦貿易委員會以一個政府組織的身分角色，建立相關程序以紀錄和瞭解身分竊用受害者的申訴案件，並主導教育大眾對身分竊用危害的警覺和預防措施及受害後呈報程序瞭解。

立法過程

1998 年 10 月 30 日，美國總統 Clinton [41]簽屬發布，《身分竊用嚇

[40] Identity Theft and Assumption Deterrence Act of 1998, P.L. 105-318, Enacted H.R. 4151, October 30, 1998, 112 Sat. 3007, codified at 18 U.S.C § 1028

[41] William Jefferson "Bill" Clinton (born William Jefferson Blythe III; August 19, 1946) is the 42nd President of the United States from 1993 to 2001.

阻法》正式成為美國的法律。這個法律的特別之處在於這是美國聯邦歷史上第一次將「身分竊用」行為獨立成罪。此法案修改了《美國聯邦法典》[42] 18 U.S.C. §1028，讓「為遂行其他不法行為，而不法獲取他人之身分證明資訊」的行為成為可罰的罪行。

在本法案公布施行之前，1982 年曾通過施行《虛偽身分證明文件犯罪控制法》[43]是為了打擊使用偽造身分證明文件來進行的詐欺活動。因該法案所增訂的《美國聯邦法典》18 U.S.C. §1028 只規範「持有或偽造身分證明文件」才具可罰性。面對這樣的變化，依美國國會要求進行專題研究，1998 年 5 月美國政府審計總署(GAO)[44]公布名為《身分詐欺：有關其蔓延狀況、成本和對網際網路的衝擊等資訊尚不足》[45]的報告。這份報告指出身分詐欺的狀況，在美國已經是日益嚴重，並且嚴重的危害到受害者的財務狀況以及國家的經濟。報告中包含了大量的資料，主要都是來自美國秘勤局(U. S. Secret Service)，社會安全局(Social Security Administration)，美國郵政總局(U.S. Postal Service)，Trans Union Corporation（一個全國性的信用報告機構），VISA 卡和萬事達卡(Master Card)組織等。此報告提供了一個身分欺詐的定

[42] United States Code: U.S.C.
[43] "False Identification Crime Control Act of 1982", P.L. 97-398, H.R. 6946, December 31, 1982, 96 Stat. 2009, Added 18 U.S.C § 1028 & 18 U.S.C. § 1738
[44] U.S. Government Accountability Office
[45] "Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited", Briefing Report to Congressional Requesters, United States General Accounting Office, GAO/GGD-98-100BR, May 1998.

義，使得《身分竊用嚇阻法》得以據以為核心[46]。在這個階段，各報告上對「身分竊用」和「身分詐欺」用語上並未作出清楚分別，常常混用之。直到《身分竊用嚇阻法》頒布後，「身分竊用」正式成為法律用語。

自前述報告呈報公布後，美國國會隨後進行了《身分竊用嚇阻法》的起草訂定，讓法律能與時俱進，應對越來越嚴重的利用身分竊用手法所產生的各式詐欺犯罪。

1997 年 3 月 21 日，美國聯邦參議院議員 Jon Kyl[47]首次在參議院會中提出《身分竊用嚇阻法》案[48]。該法案隨後被提交到參議院的司法委員會(U.S. Senate Committee on the Judiciary)做討論。該法案將竊用個人身分資訊加以入罪化，並且制定了身分竊用被害人的賠償規定。

隨後，該法案被轉至參議院司法委員會下的「科技、恐怖主義和政府資訊小組委員會」(U.S. Senate Judiciary Subcommittee on Terrorism and Government Information)，並由其分別於 1998 年 3 月 29 日和 5 月 20 日召開相關的立法公聽會。在這系列的公聽會中，小組委員會成員聽取了美國秘勤局和聯邦貿易委員會以及被害者權益維

[46] "Identity Theft and Assumption Deterrence Act of 1998", MEMORANDUM FOR ASSISTANT REGIONAL COUNSEL (CRIMINAL TAX), INTERNAL REVENUE SERVICE, January 22, 1999
[47] Jon Llewellyn Kyl (born April 25, 1942), United States Senator from Arizona (1994~)
[48] S. 512, "The Identity Theft and Deterrence Act", 104th Cong. (1997)

護代表的證詞。美國秘勤局的證詞中指出：「執法部門所面臨的狀況令人沮喪，因為未經授權使用個人資料尚不構成犯罪，而身分竊用通常是由有組織的罪犯們所為，他們清楚的知道從事這種身分竊用的行為，相較於其它罪行，等於是不受懲罰。」[49]

1998年6月12日，小組委員會一致表決通過小幅更改過的法案，然後在同年7月9號經過參議院司法委員一致通過，送交聯邦參議院大會。聯邦參議院緊接著在7月30日通過本法案，然後送至聯邦眾議院。

在聯邦眾議院方面，也有一個幾乎和眾議院法案版本內容相同的草案由亞歷桑納州眾議員John Shadegg[50]於1998年6月25日提出。這個法案基本上是依據參議院的版本加以對應修改，之後在眾議院大會中討論，並於同年10月7日通過。然後這聯邦眾議院版本法案再送至聯邦參議院，於同年10月14日通過。最後，由美國總統柯林頓於1998年10月30日簽屬發布，讓這《身分竊用嚇阻法》正式成為美國的聯邦法律。

《身分竊用嚇阻法》獲得公部門和私部門的廣泛支持。主要支持者包括美國司法部(U. S. Department of Justice)、聯邦調查局(Federal Bureau of Investigation)、財政部(U. S. Department of the Treasury)、秘

[49] S. Rep. No. 105-274, at 6 (1998)
[50] John Barden Shadegg (born October 22, 1949) is the former U.S. Representative for Arizona's 3rd congressional district, serving from 1995 until 2011.

勤局、聯邦貿易委員會、美國郵政檢查署(U. S. Postal Inspection Service)、美國銀行協會(American Bankers Association)、Associated Credit Bureaus, Inc. (ACB)、威士卡(VISA Card)、萬事達卡(Master Card)、美國公共利益研究集團(United States Public Interest Research Group)等。

重要內容

於 1998 年 10 月 30 日生效的《身分竊用嚇阻法》修訂了《美國聯邦法典》18 U.S.C. §1028 的部分內容，使其成為美國主要規範身分竊用犯罪之法規。《身分竊用嚇阻法》特別對有關「身分證明文件」(identification document)、「身分證明方式」(means of identification)等做定義性之規範。

本法所稱之「身分證明文件」係指經美國聯邦政府、州政府、州轄下各級政府、國家特定重大活動之負責組織、外國政府、外國政府轄下各級政府、國際政府組織或準國際政府組織等，官方自主或授權授發之專供或常被接受為個人身分證明使用的文件。[51]而，「身分證明方式」係指當單獨或與其他資訊一併使用，可證明特定人之身分，包括：姓名、社會安全號碼、生日、駕照號碼、外國人登記號碼、護照

[51] *See* 18 U.S.C. §1028 (d)(3)

號碼、獨特電子身分證明號碼、地址、密碼等。[52]因此，本法所定義之「身分證明方式」包括了《美國聯邦法典》18 U.S.C.§1029(e)(1)裡對「存取裝置」(access device)的定義，[53]即：「任何卡(card)、版(plate)、碼(code)、帳號號碼(account number)、電子化序號(electronic serial number)、移動識別碼(mobile identification number)、個人識別碼(personal identification number)或其它電信服務、設備或儀器識別器(identifier)、或其他方式單獨或與其他任何存取裝置配合使用而控制帳戶，以用來獲得金錢、貨品、服務或任何其他有價值之事物，或可以用來啟動資金轉移者。」這讓一些電腦犯罪(computer crime)行為，也納入身分竊用罪的範圍內。

本法針對身分竊用罪特別增加的具體規範內容，如下：

1. 身分竊用罪包含未經合法授權而轉讓或使用任一他人身分證明方式，意圖從事或幫助違反聯邦法律、地方法律之非法活動；[54]
2. 未經授權竊用一種以上之他人身分證明文件而從事犯罪；其犯罪所得利益於 1 年內達 1,000 元美金以上，得處 15 年以下有期徒刑;若僅涉及他人身分證明未經授權之移轉或使用、

[52] *See* 18 U.S.C. §1028 (d)(7)

[53] *See* "*Report to Congress: Mandatory Minimum Penalties in the Federal Criminal Justice System*", United States Sentencing Commission, October 2011, at 326, foot note 788.

[54] *See* 18 U.S.C. §1028 (a)(7)

或利用該未經授權使用之身分證明從事犯罪，惟犯罪所得利益未達美金 1,000 元，則可處 3 年以下有期徒刑。[55]

3. 涉及身分竊用之罪犯，若其所協助之犯罪若係與毒品販賣或暴力犯罪有關，或曾犯「身分竊用罪」經判決確定後再犯者，得處 20 年以下有期徒刑並得科或併科罰金。[56]

4. 若是協助國內或國際恐怖主義活動，得處 30 年以下有期徒刑並得科或併科罰金。[57]

5. 意圖或共謀違反§1028 之行為者，得按§1028 相關罰則科以處罰。[58]

《身分竊用嚇阻法》同時引導美國聯邦量刑委員會，檢視並修正其《聯邦量刑基準》，對於《美國聯邦法典》第 18 篇第 1028 條所列犯罪，訂定更為適當的罰則。《聯邦量刑基準》建議身分竊用類犯罪於量刑時應考量之因素包括：犯罪涉及之被害人人數、犯罪所涉及偽造或非法取得之身分證明文件（方式）、犯罪導致受害者損失金額之多寡。由於身分竊用對於社會、經濟所造成的傷害難以量化，納入上述因素考量後，身分竊用已成為一種重罪。有關《聯邦量刑基準》對「身分竊用罪」量刑之操作請參照後面章節。

[55] *See* 18 U.S.C. §1028 (b)(1)

[56] *See* 18 U.S.C. §1028 (b) (3)

[57] *See* 18 U.S.C. §1028 (b) (4)

[58] *See* 18 U.S.C. §1028 (f)

本法的另一個重點是《身分竊用嚇阻法》還規定聯邦貿易委員會以一個政府組織身分，集中領導，建立相關程序以紀錄和瞭解身分竊用受害者的申訴案件，並主導教育大眾對身分竊用危害的警覺意識和對預防措施及受害後呈報程序的瞭解。[59]

聯邦最高法院對一般「身分竊用罪」適用範圍的重要判決

美國聯邦最高法院(U.S. Supreme Court)在 Flores-Figueroa v. United States[60]案中將「身分竊用罪」的適用範圍做了一次清楚的界定，即行為人必須明知(knowingly)其用的身分證明方式屬於某個真實存在的人所有，才會觸犯《美國聯邦法典》18 U.S.C. §1028 的「身分竊用罪」。

本案背景為墨西哥人Flores-Figueroa從2000年起在伊利諾州East Moline一家鋼鐵廠工作。他一開始用化名、偽造的社會安全號碼和外僑永久居留證號。2006 年，他告訴雇主他想要用真名，並且提交新的身分文件。這次，他用了別人的社會安全號碼，而他的外僑永久居留證號又屬於另一人。雇主感到可疑便聯繫移民當局，Flores-Figueroa

[59] *See* 18 U.S.C. 1028 note, § 005. Centralized Complaing and Consumer Education Service for Victims of Identity Theft. 本法要求聯邦貿易委員會在一年內要建立下列程序：(一)記錄並確認收達(acknowledge)來自民眾的投訴。這些民眾必須負責任的表示(certify)有合理確切的理由相信其一個或多個身分證明文件或資訊已遭到冒用、偷竊或者遭到其他形式的運用，用以進行與本法所涵蓋的不法行為；(二)提供相關合用資訊給前述民眾；並且(三)轉介前述投訴至相關部門，包括，提供至三個全國性的信用報告機構做註記和適當的執法機關，並視情況進行執法行為。

[60] Flores-Figueroa v. United States, 129 S.Ct. 1886 (May 4, 2009)

因此被逮捕。對他的五項起訴罪名中包括兩項「加重身分竊用罪」。之前他被控加重的身分竊用罪和其他罪名，並且被判處服刑 6 年。但美國各州聯邦上訴法庭對於被告是否必須知道其偽造的身分號碼係屬於其他人的才能起訴，意見紛歧。聯邦最高法院法官們經過審酌，決定接受 Ignacio Flores-Figueroa 的上訴。

2009 年五月聯邦最高法院法官以 9 比 0 一致認為，依立法意旨，身分竊用法律條文應僅適用於那些故意侵犯他人隱私，獲取其個人資料或社會安全號碼等，進而冒用他人身分，或更進一步藉此遂行犯罪行為等的情況。聯邦最高法院要求檢察官辦案時，必須要能證明被告明知(knowingly…)其用的身分證明號碼屬於某個真實存在的人所有，法院方能以「身分竊用罪」相繩。

第三項　2000 年《網際網路虛假身分防範法》

2000 年通過施行的《網際網路虛假身分防範法》[61]修改了前述《虛偽身分證明文件犯罪控制法》，加入了處理電腦產生的身分識別證明相關犯罪的條文。本法最重要的進程是將利用電子化傳送虛偽身分證明文件的行為也包含在傳統犯罪內。

事實上，本法之制訂，其中一個主要原因是為了終結在網際網路

[61] "Internet False Identification Act of 2000", P.L. 106-578, Enacted S. 2924, December 28, 2000, 114 Stat. 3075, Codified at 18 U.S.C 1001, 1028

上到處散播的偽冒身分證明文件。根據美國聯邦存款保險公司(Federal Deposit Insurance Corporation: FDIC)在其一份名為「終結劫持帳戶型身分竊用」[62]報告中表示，本法填補了《身分竊用嚇阻法》所遺留下來的一個空白地帶。在本法之前，在網路或是現實世界裡可以販賣假造的社會安全卡，只要保持一貫說法，說它是「新奇玩具」(novelty)而不是「偽造文件」 (counterfeit document)就不犯法。有了本法之後，執法機關得以逮捕販賣者，將其治罪。[63]

第四項　2004 年《身分竊用罪刑加重法》

鑒於身分竊用問題的情況日趨嚴重，在 2004 年六月美國聯邦眾議院和參議院又通過《身分竊用罪刑加重法》(*Identity Theft Penalty Enhancement Act*)[64]，並於同年 7 月，由美國總統 George W. Bush 簽屬公布。[65]本法擴大既有的身分竊用的涵括範圍到：

1. 意圖遂行特定的非法活動而持有他人的任一身分識別方法；
2. 增加對觸犯者的處罰；

---

[62] "*Putting an End to Account-Hijacking Identity Theft*", Federal Deposit Insurance Corporation, December 14, 2004, at 11

[63] *See* Paul, Sara R., "*Features - Identity Theft: Outline of Federal Statutes and Bibliography of Select Resources*", 2006/02/07, http://www.llrx.com/features/idtheftguide.htm (Last visited on 2012/04/30)

[64] "Identity Theft Penalty Enhancement Act of 2004", P.L. 108-275, Enacted H.R. 1731 / S.153, July 15, 2004, 118 Stat. 831, Added 18 U.S.C. § 1028A

[65] "*Final Passage of H.R. 1731, the Identity Theft Penalty Enhancement Act*", U.S. Social Security Administration, http://www.ssa.gov/legislation/legis_bulletin_062904.html (Last visited on 28Apr12)

3. 加入國內恐怖活動到身分竊用的禁制範圍內以對抗協助國際恐怖活動的行為[66]。

本法針對若干罪行，當其有使用身分竊用為犯罪手法達成其犯罪目的，在量刑時，會在主罪所應負刑責之上，再針對其身分竊用行為予以加重刑期。範圍如下：

一、 意圖從事或幫助違反下列罪行而未經合法授權而轉讓或使用他人身分證明時，在其犯之罪本刑上，再加重刑期 2 年。[67]

1. 觸犯偷竊公共財、物和獎勵補助金罪[68]；銀行主管或職員偷竊、舞弊和侵佔款項罪[69]；或是竊佔他人職工福利計畫利益罪[70]；
2. 觸犯偽冒公民身分罪[71]；
3. 觸犯提供不實資料以取得武器罪[72]；
4. 觸犯除了本節或《美國聯邦法典》18 U.S.C. §1028(a)(7)外，任何涵蓋在《美國聯邦法典》第 18 章[73]中有關詐欺和提供不實資料的罪行；
5. 觸犯所有《美國聯邦法典》第 63 章[74]中有關郵件、銀行和

[66] *See* 18 U.S.C. § 1028A(a)(2)
[67] *See* 18 U.S.C. § 1028A(c)(1)-(11)
[68] *See* 18 U.S.C. § 641
[69] *See* 18 U.S.C. § 656
[70] *See* 26 U.S.C. § 664
[71] *See* 26 U.S.C. § 911
[72] *See* 26 U.S.C. § 922(a)(6)
[73] United States Code : TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
[74] 18 U.S.C. CHAPTER 63 - MAIL FRAUD AND OTHER FRAUD OFFENSES

匯款詐欺的罪行；

6. 觸犯所有《美國聯邦法典》第 69 章[75]中有關國籍和公民身分的罪行；
7. 觸犯所有《美國聯邦法典》第 75 章[76]中有關護照和簽證的罪行；
8. 觸犯《金融服務現代化法》(*Gramm-Leach-Bliley Act*)[77]第 523 節中有關以虛偽表示方法獲得客戶資料的罪行；
9. 觸犯美國《移民及國籍法》 (*Immigration and Nationality Act*)[78] 第 243 及 266 節中有關獲驅逐出境處分後故意不離境及製造假的外僑永久居留證[79]；
10. 觸犯《移民及國籍法》第二篇第八章（即《美國聯邦法典》8 U.S.C. §1321 以下條文）中有關各種移民法罪行；
11. 觸犯《社會安全福利法》 (*Social Security Act*)[80]第§208, §811, §1107(b), §1128B(a), 或 §1632 條中有關提供虛偽陳述於各社會安全福利補助計畫的罪行。

二、 意圖從事或幫助違反《美國聯邦法典》18 U.S.C. §2332b (g)(5)(B)

[75] 18 U.S.C. CHAPTER 69 - NATIONALITY AND CITIZENSHIP
[76] 18 U.S.C. CHAPTER 75 - PASSPORTS AND VISAS
[77] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, Enacted S. 900, November 12, 1999, codified in scattered sections, mostly 12 and 15 U.S.C. § 6801-6810 &, 6821-6827,
[78] 8 U.S.C. § 1253 and 1306
[79] 「外僑永久居留證」(Alien Registration Card) 即美國「永久居民卡」(Permanent Resident Card)，俗稱「綠卡」，之正式名稱。
[80] "Social Security Act of 1935", Pub.L. 74-271, 49 Stat. 620, enacted August 14, 1935, codified as 42 U.S.C. § ch.7

所定義之「聯邦恐怖活動罪」 (Federal crime of terrorism)，而未經合法授權而轉讓或使用他人身分證明或偽造之身分證明時，在其犯之罪本刑上，再加重刑期 5 年。

三、 要求法院於審理量刑時應為以下之處分：

1. 禁止將被告的「加重身分竊用罪」與其他的罪刑予以合併執行(concurrent)，[81]除非是被告另有一個「加重身分竊用罪」時，法庭方得自由裁量[82]。
2. 禁止將犯前述「加重身分竊用罪」的被告予以緩刑宣告[83]；或
3. 禁止因前述「加重身分竊用罪」之考量而減輕被告本罪之宣告刑[84]；

美國的「合併執行」宣判和我國刑法「數罪併罰」在實質意義上相同。在罪責之歸屬，於現今學說實務均採一罪一刑之審判原則的前提下，雖然各罪皆有其宣告刑，但在裁判確定前犯數罪者，我國刑法第五十條規定應併合處罰之。此即數罪併罰。在美國則是規定在《美國聯邦法典》18 U.S.C. §§ 3553(a) 、(b) 和 §3584。國會授權讓地區聯邦法院在不抵觸《聯邦量刑基準》的規定下，在量刑時自由使用「數

[81] *See* 18 U.S.C. § 1028A(b)(2)
[82] *See* 18 U.S.C. § 1028A(b)(4)
[83] *See* 18 U.S.C. § 1028A(b)(1)
[84] *See* 18 U.S.C. § 1028A(b)(3)

罪併罰」(concurrent sentencing)或「一罪一罰」(consecutive sentencing)裁量方式。我國刑法第五十一條規定，數罪併罰，於分別宣告其罪之刑後，再依該條各款，定其應執行刑。數罪併罰之方法的共通特徵為：就各種刑分別按其宣告刑加總之和，定其應執行刑時，該應執行刑沒有例外的皆至多等於，通常小於各罪宣告刑加總之和。美國聯邦法院定執行刑長短的方式和我國大致相同。[85]

第五項　2008 年《身分竊用執法及補償法》

現代的身分竊用以與電腦犯罪密不可分。身分竊用是電腦詐欺(computer fraud)最常見的手法之一。[86]為了進一步加強身分竊用法律的效能，美國於 2008 年通過施行《身分竊用執法及補償法》[87]。本法主要重點如下：

1. 在《美國聯邦法典》18 U.S.C. §3663 增加條文(b)，讓符合 18 U.S.C. 1028(a)(7) 或 1028A(a)的身分竊用受害者可以向法院請求向被告要求補償為彌補身分竊用所造成之實際或預期損失而花費的時

[85] 參考「釋字第六七九號解釋 大法官黃茂榮協同意見書」。頁 2-4；和美國法務網站：http://definitions.uslegal.com/c/concurrent-sentencing/ (Last visited on 2012/08/20)

[86] "Of the more than 400,000 complaints referred to the Internet Crime Complaint Center (IC3) since its opening in May of 2000, more than 100,000 were either characterized as Identity Theft, or involved conduct that could be characterized as Identity Theft." -- Steven M. Martinez, "Testimony Before the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census", Federal Bureau of Investigation, September 22, 2004. Source: http://www.fbi.gov/news/testimony/identity-theft-and-cyber-crime (Lasted checked on 2012/08/26)

[87] Identity Theft Enforcement and Restitution Act of 2008 (ITERA), Pub. L. No. 108-275, Tit. II (2008)

間費用；[88]此條中值得注意的是：18 U.S.C. 1028(a)(7)主要是定義「身分證明方式」，其涵蓋了 18 U.S.C. § 1029(e)(1)裡對「存取裝置」(access device)的定義。所以本法是另一個將身分竊用犯罪和電腦犯罪相關條文產生鏈節之處。有關 18 U.S.C. 1028(a)(7)的說明，請見本節第二項 1998 年《身分竊用嚇阻法》內「重要內容」分項之前段說明。

2. 降低檢察官起訴電腦駭客(hacker)和其它網際網路犯罪的門檻，讓聯邦檢察官可以起訴非跨州或和非跨國有關的電腦詐欺案件。[89]換言之，只要是電腦詐欺，就算是發生在單一州範圍內，聯邦檢察官都可行使聯邦司法管轄權；

3. 加重電腦犯罪罪責，使一年內破壞 10 台或以上的聯邦政府或任一金融機構的「受保護電腦」 (protected computer)的犯行，成為聯邦重罪(felony)。[90]這電腦包含前述組織直接使用的電腦，以及為其服務之其他組織所屬電腦；

4. 重新改寫《美國聯邦法典》18 U.S.C. §1030(a)(7)的條文，擴大「網路勒索罪」 (cyber-extortion)的定義；[91]

5. 處罰電腦犯罪的陰謀(conspires to commit)犯；[92]

[88] Ibid., Sec. 202 (3)
[89] Ibid., Sec. 203
[90] Ibid., Sec. 204(2)(C)
[91] Ibid., Sec. 205
[92] Ibid., Sec. 206

6. 擴大《美國聯邦法典》原 18 U.S.C. §1030(e)(2)(B)「受保護電腦」的定義範圍。讓原本的範圍只限於「使用」於聯邦政府或金融機構商務或通訊的電腦，擴及至「影響」前述的使用；[93]和

7. 增加電腦犯罪輔助物的沒收條款。[94]

第六項　身分竊用罪的起訴、裁判與量刑實務參考

起訴 - 《美國聯邦檢察官手冊》

在實務操作上，《美國聯邦檢察官手冊》(United States Attorneys' Manual)第九章第 1512 節[95]中根據《美國聯邦法典》18 U.S.C. § 1028(a)有關觸犯身分竊用罪行為的六項內容中，細分出下列 10 個符合身分竊用罪定義的構成要件，做為檢察官起訴之參考：

1. 未經合法授權製作或假造身分證明文件；[96]
2. 明知真實或假造之身分證明文件係經偷竊所得或未經合法授權製作所成，而仍移轉運輸之；[97]
3. 意圖非法使用而持有五份或以上的真實或假造之身分證明文

[93] Ibid., Sec. 207
[94] Ibid., Sec. 208
[95] *See* 1512 Prohibited Acts—18 U.S.C. § 1028, TITLE 9 CRIMINAL DIVISION, United States Attorneys' Manual, http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm01512.htm (Last checked on 2012/07/12)
[96] 原文 : Producing without lawful authority an identification document or a false identification document (*See* 18 U.S.C. § 1028(a)(1))
[97] 原文：Transferring an identification document or a false identification document knowing that such document was stolen or produced without lawful authority (*See* 18 U.S.C. § 1028(a)(2))

件（不包括持有者自己的合法身分證明文件）；[98]

4. 意圖非法移轉運輸而持有五份或以上的真實或假造之身分證明文件（不包括持有者自己的合法身分證明文件）；[99]

5. 意圖用以詐騙美國聯邦政府而持有真實或假造之身分證明文件（不包括持有者自己的合法身分證明文件）；[100]

6. 持有竊得或明知其為竊得之美國政府授發之身分證明文件；[101]

7. 明知而持有外觀上類似美國政府授發但實為未經授權製作之身分證明文件；[102]

8. 意圖製作偽冒身分證明文件，而生產、移轉運輸或持有文件製造相關應用工具材料；[103]

9. 意圖製作偽冒身分證明文件，而生產、移轉運輸或持有製造相關應用工具材料，以供進一步製成偽冒身分證明文件所需

---

[98] 原文：Possessing with intent to use unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor) or false identification documents (*See* 18 U.S.C. § 1028(a)(3))

[99] 原文：Possessing with intent to transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor) or false identification documents (*See* 18 U.S.C. § 1028(a)(3))

[100] 原文：Possessing an identification document (other than one issued lawfully for the use of the possessor) or a false identification document with the intent such document be used to defraud the United States (*See* 18 U.S.C. § 1028(a)(4))

[101] 原文：Possessing an identification document that is an identification document of the United States which is stolen, knowing that such document was stolen (*See* 18 U.S.C. § 1028(a)(6))

[102] 原文：Possessing an identification document that appears to be an identification document of the United States, which was produced without authority knowing that such document was produced without authority (*See* 18 U.S.C. § 1028(a)(6))

[103] 原文：Producing, transferring, or possessing a document-making implement with the intent that such document-making implement be used in the production of a false identification document (*See* 18 U.S.C. § 1028(a)(5))

之工具材料；[104]以及，

10. 試圖從事上述任一項行為。[105]換言之，即未遂犯罰之。

該手冊並無單獨章節針對利用電腦存取裝置(access device)進行身分竊用的犯行時的處理，而是在其第 9-49.000 章「和使用電腦存取裝置及信用卡有關之詐欺」(FRAUD IN CONNECTION WITH ACCESS DEVICES AND CREDIT CARDS)[106]中針對觸犯《美國聯邦法典》18 U.S.C. § 1029 的不同犯行，給予不同的起訴參考建議。並建議檢察官引用電腦犯罪(computer crime)相關規定，進行證據蒐集和起訴作業。

審理裁判-「聯邦陪審團指南」

美國法院在刑事審判案件的處理上使用了陪審團制度，為了讓陪審員能瞭解如何判斷案情的法律意義，進而決定被告是否有罪，美國聯邦第一、三、五、六、七、八、九、十和十三巡迴法院和除了西維吉尼亞州和德州外其餘的 48 州均設有可供一致參考使用的「陪審團指南」 (pattern/uniform Jury Instructions)。聯邦陪審團指南係由該聯邦巡迴法庭法官協會之模範陪審團指南委員會 (The Committee on Pattern Jury Instructions of the District Judges Association) 訂立，供轄

[104] 原文：Producing, transferring, or possessing a document-making implement with the intent that such document-making implement be used in the production of another document-making implement which will be used in the production of a false identification document (*See* 18 U.S.C. § 1028(a)(5))

[105] 原文：Attempting to do any of the above (*See* 18 U.S.C. § 1028(a))

[106] See http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/49mcrm.htm. Last checked on 2012/09/09.

區案件審理時陪審團員使用。[107]

以美國聯邦第六巡迴法庭所頒佈的「刑事案件陪審團指南」(Pattern Criminal Jury Instructions)[108]為例，在審理身分竊用案件所使用的是第 15.00 章「身分識別和存取裝置罪等」(Chapter 15.00 - Identity and Access Device Crimes)。這個章節提供詳細的指示以處理觸犯《美國聯邦法典》18 U.S.C. §1028、§1028A, 和 §1029 與身分竊用、加重身分竊用和使用存取裝置詐欺的刑事案件。

量刑 - 「美國聯邦量刑委員會」和《聯邦量刑基準》

如前述，1998 年的《身分竊用嚇阻法》引導美國聯邦量刑委員會，檢視並修正《聯邦量刑基準》，對於《美國聯邦法典》第 18 篇第 1028 條所列犯罪，訂定更為適當的罰則。而《身分竊用罪刑加重法》，針對若干罪行，當其有使用身分竊用為犯罪手法達成其犯罪目的，在量刑時，會在主罪所應負刑責之上，再針對其身分竊用行為予以加重刑期，也使加重身分竊用罪最成為美國聯邦法律中少數具有最低刑度要求(mandatory minimum penalty)的罪行。

聯邦量刑委員會是美國聯邦政府司法部門中的一個永久性的獨

[107] 參考 Jury Verdicts and Jury Instructions Research Guide, Georgetown University Law Library (http://www.law.georgetown.edu/library/research/guides/jury.cfm) 和 Federal Jury Instructions Resource Page, Federal Evidence Review (http://federalevidence.com/node/893), Last checked on 2012/08/12.

[108] See “PATTERN CRIMINAL JURY INSTRUCTIONS”, Committee on Pattern Criminal Jury Instructions District Judges Association of Sixth Circuit, Updated as of June 10, 2011 http://www.ca6.uscourts.gov/internet/crim_jury_insts.htm (Last Checked on 2012/09/09)

立機構。其成立的法源，來自於 1984 年之《綜合犯罪控制法》(*Comprehensive Crime Control Act of 1984*) ，該法亦被稱為《量刑改革法》(*Sentencing Reform Act of 1984*)。其成立之宗旨在於為聯邦法院決定量刑政策與形成量刑慣例，包括制訂詳細的量刑基準，以及對於違反聯邦法律之犯罪者給予適當之處罰。在發展、觀察、與修正量刑基準的過程中，量刑委員會針對與量刑有關的課題，提供相關之訓練與研究，並且向美國的國會、刑事司法實務界以及社會大眾，提供相關的資訊。[109]

在聯邦量刑委員會的研究中發現，在過去的量刑實務中，美國法院對於諸如竊盜、逃稅、反壟斷(anti-trust)、內線交易、詐欺以及侵佔公款等這些經濟性的犯罪，宣告緩刑之比例偏高，不過，聯邦量刑委員會則認為這些犯罪為嚴重的犯罪。為解決這些問題，聯邦量刑委員會在《聯邦量刑基準》中，將過去經常宣告緩刑的一些犯罪，規定成為科處短期監禁刑之犯罪。量刑委員會確信，一項明確的監禁刑，即使期間不長，仍會產生特別的嚇阻作用(deterrence)，尤其是與過去所量處的緩刑相較，更是如此。[110]

[109] 吳景芳，「美國之聯邦量刑改革法」，《刑事政策與犯罪研究論文集(三)02》，法務部犯罪研究中心編印，2000 年 11 月。頁 12 。全文見：http://www.criminalresearch.moj.gov.tw/ct.asp?xItem=170501&ctNode=27084&mp=301，(前次檢索日：2012/06/12)

[110] 同前註。頁 35

聯邦量刑委員會，每一年均出版一本《聯邦量刑基準手冊》(Federal Sentencing Guidelines Manual)[111]，最新的 2011 年版手冊其編排方式如下：第一章為「序論、授權及一般適用原則」(Introduction, Authority and General Application Principles)，第二章為「犯罪行為」(Offense Against the Person)，第三章為「調整」(Adjustments)，第四章為「犯罪前歷與犯罪生涯」(Criminal History and Criminal Livelihood)，第五章為「量刑」(Determining the Sentence)，第六章為「量刑程序與答辯協議」(Sentencing Procedures, Plea Agreements, and Crime Victims' Rights)，第七章為「保護觀察與釋放後之監督之違反」(Violations of Probation and Supervised Release)，第八章為「組織之量刑」(Sentencing of Organizations)。

聯邦量刑委員會還設計出一個包含「犯罪等級」(offense level)和「犯罪前歷種類」(Criminal History Category)的《量刑基準表》(Sentencing Table)。表中的垂直軸，區分為 43 種犯罪等級，每一個犯罪等級代表一種「量刑幅度」(Sentencing Range)，而表中的水平軸，區分為六種犯罪前歷種類，每一個犯罪前歷種類亦代表一種量刑幅度。垂直軸與水平軸二者所代表的量刑幅度，會在某一個位置相互重疊，這就是被告所應獲得之量刑。量刑委員會根據過去的量刑實務加以估

[111] 文件正式名為 United States Sentencing Guidelines (USSG)

算，求得其平均值，以決定每一種犯罪之適當的量刑幅度。量刑委員會同時亦檢查聯邦法律、假釋基準，以及其他有關的、類似的來源中有關量刑之特別規定。[112]

《聯邦量刑基準》中同時考量被告的定罪罪名與實際上真正的犯罪行為，藉由所犯罪行對應的「基本犯罪等級」(Base Offense Level)做為始點，去評估犯罪的嚴重性。根據各個案件的不同情況，犯罪等級可以增加也可以減少。這些可以修正犯罪等級（亦即：明確的犯罪特性）的因素，在量刑基準中加以列舉。犯罪等級經過明確的犯罪特性與相關考量加以修正調整後，形成為一項量刑表的垂直軸線，用來決定量刑的範圍。量刑表的犯罪垂直軸線，從最不嚴重的程度 1 到最嚴重的程度 43。

在進行量刑考量時，法官找出具體被告在垂直軸線中的犯罪等級，以及在水平軸線中的犯罪前歷種類，然後，此二者在量刑基準表中的交集部分所顯示出來之監禁月數，即是該名被告的實際量刑範圍。此外，為了使得量刑較有彈性，每個實際量刑範圍，並非採取唯一的刑期，而是仍有相當的彈性空間，實際量刑範圍的上限與下限之間，有不超過六個月的或二十五個百分點（不論何者較大）的彈性空間，法官可以在此範圍內有所裁量。同時聯邦「量刑改革法」中，允許法院

[112] 同前註。頁 38

可以例外的不適用此項量刑基準，亦即，當法院發現「某種惡化的或是緩和的情況，當初量刑委員會在制定量刑基準時並沒有充分加以考慮」[113]時，即可適用除外條款。

《量刑基準表》(Sentencing Table)之內容請參照下表 1：

[113] *See* 18 U.S.C. §3553(b)

表 1「美國聯邦量刑基準表」

SENTENCING TABLE
(in months of imprisonment)

	Offense Level	Criminal History Category (Criminal History Points) I (0 or 1)	II (2 or 3)	III (4, 5, 6)	IV (7, 8, 9)	V (10, 11, 12)	VI (13 or more)
	1	0-6	0-6	0-6	0-6	0-6	0-6
	2	0-6	0-6	0-6	0-6	0-6	1-7
	3	0-6	0-6	0-6	0-6	2-8	3-9
	4	0-6	0-6	0-6	2-8	4-10	6-12
Zone A	5	0-6	0-6	1-7	4-10	6-12	9-15
	6	0-6	1-7	2-8	6-12	9-15	12-18
	7	0-6	2-8	4-10	8-14	12-18	15-21
	8	0-6	4-10	6-12	10-16	15-21	18-24
	9	4-10	6-12	8-14	12-18	18-24	21-27
Zone B	10	6-12	8-14	10-16	15-21	21-27	24-30
	11	8-14	10-16	12-18	18-24	24-30	27-33
Zone C	12	10-16	12-18	15-21	21-27	27-33	30-37
	13	12-18	15-21	18-24	24-30	30-37	33-41
	14	15-21	18-24	21-27	27-33	33-41	37-46
	15	18-24	21-27	24-30	30-37	37-46	41-51
	16	21-27	24-30	27-33	33-41	41-51	46-57
	17	24-30	27-33	30-37	37-46	46-57	51-63
	18	27-33	30-37	33-41	41-51	51-63	57-71
	19	30-37	33-41	37-46	46-57	57-71	63-78
	20	33-41	37-46	41-51	51-63	63-78	70-87
	21	37-46	41-51	46-57	57-71	70-87	77-96
	22	41-51	46-57	51-63	63-78	77-96	84-105
	23	46-57	51-63	57-71	70-87	84-105	92-115
	24	51-63	57-71	63-78	77-96	92-115	100-125
	25	57-71	63-78	70-87	84-105	100-125	110-137
	26	63-78	70-87	78-97	92-115	110-137	120-150
Zone D	27	70-87	78-97	87-108	100-125	120-150	130-162
	28	78-97	87-108	97-121	110-137	130-162	140-175
	29	87-108	97-121	108-135	121-151	140-175	151-188
	30	97-121	108-135	121-151	135-168	151-188	168-210
	31	108-135	121-151	135-168	151-188	168-210	188-235
	32	121-151	135-168	151-188	168-210	188-235	210-262
	33	135-168	151-188	168-210	188-235	210-262	235-293
	34	151-188	168-210	188-235	210-262	235-293	262-327
	35	168-210	188-235	210-262	235-293	262-327	292-365
	36	188-235	210-262	235-293	262-327	292-365	324-405
	37	210-262	235-293	262-327	292-365	324-405	360-life
	38	235-293	262-327	292-365	324-405	360-life	360-life
	39	262-327	292-365	324-405	360-life	360-life	360-life
	40	292-365	324-405	360-life	360-life	360-life	360-life
	41	324-405	360-life	360-life	360-life	360-life	360-life
	42	360-life	360-life	360-life	360-life	360-life	360-life
	43	life	life	life	life	life	life

November 1, 2011

依照《聯邦量刑基準》，USSG §2B1.1.是專門處理偷竊(larceny)、貪瀆(embezzlement)和其他型態的不法取得(Other Forms of Theft)行為。這包含了如盜贓物(Stolen Property)、破壞財物(Property Damage or Destruction)、詐欺(Fraud and Deceit)、偽造(Forgery)、偽變造非美國政府負擔之證券(Offenses Involving Altered or Counterfeit Instruments Other than Counterfeit Bearer Obligations of the United States) 等罪行。有關「身分竊用罪」(18 U.S.C. §1028)的量刑參考是 USSG§2B1.1(b)和，「加重身分竊用罪」(18 U.S.C.§1028A)則參考 USSG §2B1.6.。

一般「身分竊用罪」的量刑基準：

一、 基本犯罪等級：視其所犯罪行種類，分別由 6 或 7 級為基礎起算。[114]

二、 考量被害人損失金額：當一犯罪行為造成被害人損失達 5000 美元以上時，則依照受害金額累加犯罪等級級數：[115]

(A)受害金額 5,000 美元或以下，不增加級數；

(B)受害金額達 5,000 美元時，增加 2 級；

(C)受害金額達 10,000 美元時，增加 4 級；

(D)受害金額達 30,000 美元時，增加 6 級；

[114] *See* United States Sentencing Guidelines (USSG) §2B1.1(a)
[115] *See* USSG §2B1.1(b)(1)

(E)受害金額達 70,000 美元時，增加 8 級；

(F)受害金額達 120,000 美元時，增加 10 級；

(G)受害金額達 200,000 美元時，增加 12 級；

(H)受害金額達 400,000 美元時，增加 14 級；

(I)受害金額達 1,000,000 美元時，增加 16 級；

(J)受害金額達 2,500,000 美元時，增加 18 級；

(K)受害金額達 7,000,000 美元時，增加 20 級；

(L)受害金額達 20,000,000 美元時，增加 22 級；

(M)受害金額達 50,000,000 美元時，增加 24 級；

(N)受害金額達 100,000,000 美元時，增加 26 級；

(O)受害金額達 200,000,000 美元時，增加 28 級；

(P)受害金額超過 400,000,000 美元時，增加 30。

三、 考量受害人數：當一犯罪行為受害者超過 10 人或使用大量行銷(mass-marketing)方式遂行時，增加犯罪等級級數 2 級；若被害人超過 50 人，增加犯罪等級級數 4 級；若被害人 250 人或更多，增加犯罪等級級數 6 級。[116]

四、 加計與身分竊用有關之犯罪行為：當犯罪行為涉及到未經合法授權而轉讓或使用任何方式的身分證明(mean of

[116] *See* USSG §2B1.1(b)(1)

identification)以非法製造或獲得其他形式的身分證明或握有 5 件或以上非法製造或獲得的身分證明時，增加犯罪等級級數 2 級。若加總後犯罪程度級數為達 12 級，則直接增加至 12 級。[117]

上述第四部分是因 1998 年的《身分竊用嚇阻法》而加入。有關其中的「身分證明」，係依照《美國聯邦法典》18 U.S.C. §1028(d)的廣義定義，所以除了一般身分證明文件外，還包括身分證明資訊，如社會安全號碼、信用卡號或貸款記錄等。《聯邦量刑基準》還特別提到，之所以會設計「若加總後犯罪程度級數為達 12 級，則直接增加至 12 級」的目的，是因為身分竊用行為讓被害人很難發現，一旦發現了，通常損失都已經嚴重，而且很多的損失是無形的，如名譽信用等，且其影響難以計量，所以在量刑時，針對使用身分竊用遂行的犯罪行為，加以較重的刑罰。[118]

換言之，犯罪行為人若是違反到「身分竊用罪」，其犯罪程度級數必然會達到 12 級或以上，即至少落至「聯邦量刑基準表」的 C 區間(Zone C)內。依照《聯邦量刑基準》第五章第 C 節內的規範，當量刑結果落入「量刑基準表」的 C 區間，犯罪人至少要在監獄中服宣判

[117] *See* USSG §2B1.1(b)(10)(C)
[118] *See* USSG §2B1.1, Background, at 102 (2011)

刑期的一半期間。[119]如前面所提到的，聯邦量刑委員會確信，一項明確的監禁刑，即使期間不長，仍會產生特別的嚇阻作用(deterrence)。而在《聯邦量刑基準》中特別設計「若加總後犯罪程度級數為達 12 級，則直接增加至 12 級」就是為了讓犯罪者必須在監獄服刑。由此可見，美國對於身分竊用罪重視的程度。

「加重身分竊用罪」的量刑基準

按照《美國聯邦量刑基準》§2B1.6.所規範，一旦所犯罪行為符合《美國聯邦法典》18 U.S.C. §1028A 的「加重身分竊用罪」之構成要件，其量刑即直接依照該法條之量刑規定處理，毋須參照《美國聯邦量刑基準》第三章「調整」和第四章「犯罪前歷與犯罪生涯」之規範。此即謂，若犯罪行為有：

一、意圖從事或幫助違反《美國聯邦法典》18 U.S.C. §1028A 所列一般罪行，而未經合法授權而轉讓或使用他人身分證明時，在其犯之罪本刑上，直接加重刑期 2 年。

二、意圖從事或幫助違反「聯邦恐怖活動罪」[120]，而未經合法授權而轉讓或使用他人身分證明或偽造之身分證明時，在其犯之罪本刑上，直接加重刑期 5 年。值得注意者為，本條之適

[119] *See* USSG §5C1.1(d)
[120] *See* 18 U.S.C. §2332b(g)(5)(B)

用範圍擴大到包括「偽造之身分證明」(false identification)，即行為人無論其所用來遂行「聯邦恐怖活動罪」的身分證明方式是否屬於某個真實存在的人所有，均可以本條論罪。

另外，在量刑時可否為緩刑宣告和刑度為合併考量或累加計算，亦特別規範法庭不得將「加重身分竊用罪」的被告予以緩刑宣告、不得因「加重身分竊用罪」之考量而減輕被告本罪之宣告刑；或將被告的「加重身分竊用罪」與其他的罪刑予以合併執行(concurrent)，除非是被告另有一個「加重身分竊用罪」，則法庭方始得行自由裁量。

《身分竊用罪刑加重法》針對案件有違反多次(multiple counts)「加重身分竊用罪」時，允許法庭可以依職權自由裁量，量刑考慮時得予以合併刑期或是累進(consecutively)刑期。《美國聯邦量刑基準》對此部分亦提供法院量刑的考量方向：(1)藉身分竊用行為所犯相關本刑的惡性程度；(2)前述本刑是否可依量刑指標準南予以群組化(to be grouped for guidelines purpose)，若可，即應考量合併刑期；(3)是否符合《美國聯邦法典》18 U.S.C. §3553(a)(2)的規範目的，適合予以合併刑期或是累進刑期。[121]

身分竊用罪的裁判量刑統計--以 2010 年為例

由聯邦貿易委員會主導設立的「消費者哨兵網」 (Consumer

[121] *See* USSG §5G1.2, comment. (n.2(B))

Sentinel Network)是專供各級執法機關查詢的加密線上資料庫，其中儲存的數以百萬計和詐欺、身分竊用和其他特定違法類型的申訴案件，以供執法機關進行調查和分析。[122]依據「消費者哨兵網」發布的統計資料，2010 年，收到超過一百卅餘萬件的申訴，其中身分竊用受害的申訴有 250,854 件[123]，位居所有申訴案件分類的第一位。這些案件中 71,940 件在申訴時表示他們同時有通知警方，但是正式做成報案紀錄的僅有 62,150 件。[124]

而依據聯邦量刑委員會在 2011 年 10 月呈報美國國會的報告書[125]中所示，在 2010 聯邦財政年度共有 73,239 個被告被裁判定罪，其中有 1,870 個被告是屬觸犯「身分竊用罪」，僅佔全年度總數的 2.6%。而在這 1,870 個被告中符合加重要件，即觸犯「加重身分竊用罪」者為 797 人。[126]案件看似不多，主要的原因是因為針對身分竊用罪的統計不易，且剛開始不久。雖然如此，聯邦量刑委員會已經發現，自開始針對本罪進行統計以來，身分竊用罪的裁判定罪數量有逐漸增加現象。[127]

統計結果顯示，觸犯一般「身分竊用罪」者(n=1,073)平均獲判徒

[122] *See* "Consumer Sentinel Network" website, available at http://www.ftc.gov/sentinel/ (Last checked on 2012/06/18)
[123] "*2010 Consumer Sentinel Network Data Book*", Federal Trade Commission, March 2011, at 6
[124] *Ibid*. at 12
[125] "*Report to Congress: Mandatory Minimum Penalties in the Federal Criminal Justice System*", United States Sentencing Commission, October 2011
[126] *Ibid*. at 329
[127] *Ibid*. at 330

刑 22 個月；觸犯「加重身分竊用罪」者(n=673)則平均獲判徒刑 50 個月；觸犯「加重身分竊用罪」但獲部分刑期赦免者(n=124)，其平均獲判徒刑 32 個月。[128]他們是因為在犯罪偵查及審判期間提供政府有效的協助或其他情狀而獲得部分赦免。[129]

對案件有違反多次「加重身分竊用罪」的統計部分，在 797 名「加重身分竊用罪」被告中，有 82 名屬本類。其中 69 名獲得合併刑期宣判，13 名則為累進刑期宣判。[130]

第二節　全國性個人身分證之相關法律

如本論文第一章所述，人們總是通過一些身分資訊(Identity Information)或識別憑證(Identifier)來證明自己或識別他人的身分。識別身分的方法主要有：(1)基於知識/資訊的識別：即判斷一個人「知道什麼」，例如密碼、口令、身分證號等；(2)基於憑證的識別：即判斷一個人「擁有什麼」，例如身分證，護照、信用卡、介紹信等；(3)生物性識別：即通過一個人的外貌、指紋、虹膜、聲音等生物性特徵以及一個人的行為資訊來識別身分。[131]

[128] *Ibid*. at 336
[129] *Ibid*. at 337
[130] *Ibid*. at 339
[131] CLARKE R. (1994)

美國並無一全國性的個人身分證制度。最接近我們所瞭解的「國民身分證」概念的是其「社會安全號碼」(Social Security Numbers: SSN)和各州所授發的「駕駛執照」(Driver's License)或「州居民身分證」(Identity Card)。個人的社會安全號碼就是前述(1)基於知識/資訊的識別的方式，而汽車駕駛執照或州居民身分證就是(2)基於憑證的識別和(3)生物性識別，因為其上之照片有持證人之外貌。

美國的社會安全號碼制度是依 1935 年發佈施行的《社會安全福利法》[132]而開始建立的。該法案授權社會安全局建立一套系統來管理各種社會福利救濟的工作。其中一項重要措施就是設立社會安全號碼制度。社會安全號碼發放給美國公民、獲永久居留權的外籍僑民和部分因工作或其他需要此號碼之外國公民[133]。這組號碼的最初是為了在社會安全計畫內追蹤個人的收支帳戶。因為社會安全號碼在美國個人識別資料中所具有的統一性和單一特性，雖然偶爾會有重複登錄的錯誤發生，但許多雇傭（工作）、醫療、教育、和信用記錄都使用社會安全號碼作為索引的依據。所以不久就被公部門和私部門廣泛被使用，讓它幾乎成為美國的「實質」(de facto)個人身分證號[134,135,136]。

[132] "Social Security Act of 1935", Pub.L. 74-271, 49 Stat. 620, enacted August 14, 1935, codified as 42 U.S.C. § ch.7

[133] *See* 42 U.S.C. § 405(c)(2)

[134] "社會安全號碼", 维基百科, 來源：http://zh.wikipedia.org/wiki/社會安全號碼, 檢查日 2012/05/05

[135] *See* Jim Kouri, "*Social Security Cards: De Facto National Identification*", American Chronicle, November 29, 2005, available at http://www.americanchronicle.com/articles/view/3911 (Last visited on 2012/04/05).

[136] "Social Security Number Chronology", U.S. Social Security Administration, available at http://www.ssa.gov/history/ssn/ssnchron.html, Last visited on 2012/05/12.

後來，鑑於公部門和私部門逐漸大量的使用社會安全號碼當作個人身分識別碼，因而讓人們產生了一些疑慮，國會亦要求要有行動，美國聯邦社會安全管理局於是在 1970 年成立了一個工作小組，專責調查社會安全號碼在社會安全管理計畫以外被使用的狀況[137]。1971 年報告出爐，其中很清楚的表示，社會安全號碼已經不只是原本的為了社會安全計畫目的號碼，它已經逐漸且大量的被社會公認而成為個人的「數字化識別」。本報告同時指出，美國社會已經進步到了每一個美國人都需要一個有效的個人識別碼[138]。

1974 年的《隱私權法》第七章(Section 7) ，規範美國聯邦及各州機關不得因人民拒絕提供其社會安全號碼而否准其依法享有之權利、福利或特權。同時，美國聯邦及各州機關若要求人民提供其社會安全號碼時，必須告知人民此要求係依何種法律要求之必要行為，或是其係屬可由人民選擇自願配合的項目。該法規範了公部門對社會安全號碼的使用限制，但對私部門則沒有直接規範限制。2007 年美國「政府責任辦公室」(GAO)公布了一份報告，指出私部門使用社會安全號碼的情況極其普遍[139]，包括用來做信用風險評估的資料交換、在多個醫療提供者間追蹤病友受照護的狀況、尋找破產剩餘資產，和用

[137] SWENDIMAN, Kathleen S., "*The Social Security Number- Legal Developments Affecting Its Collection, Disclosure, and Confidentiality*", CSR Report for Congress (Order Code RL 30318), 2008.

[138] "*Report to the Commissioner*", Social Security Number Task Force, Social Security Administration, 1971, at 4.

[139] "*Social Security Numbers: Use is Widespread and Protection Could be Improved*", (GAO-07-1023T), Government Accountability Office, June 21, 2007.

來進行新進員工背景查核等。

美國幅員廣大，公路網發達，其日常生活中，離不開汽車。駕駛執照之授發為各州之主管事務。美國居民每遷徙到新的州，就必須規定時日內（一般而言為 15 日）到該州的機動車輛監理機構（通常簡稱為 DMV）辦理住所登記和更換成該州的駕駛執照。對於沒有駕駛執照的居民，則辦理州居民身分證。由於駕駛執照通常是唯一隨身攜帶的有照片的官方授發之身分證明文件，無論是買汽車、辦保險，還是到銀行開戶頭、辦信用卡，都要出示駕駛執照，所以駕駛執照逐漸演變成為在日常生活中扮演著「身分證」的角色。

第一項 2004 年《情報改革與防範恐怖活動法》

在 2004 年的《情報改革與防範恐怖活動法》(*Intelligence Reform and Terrorism Prevention Act of 2004*) [140]通過之前，美國駕駛執照的規格和要求是由各州政府自行負責，並無一個全國一致的標準存在。事實上，在 2001 年的 911 恐怖攻擊之前，美國國會兩黨還一致的趨向立法，禁止全國有一致的標準產生，而且在當時的氣氛下還非常可能通過。

但是經過了 911 恐怖攻擊事件，這氣氛轉變了，大家都認為需要

[140] Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), P.L. 108-458 §§ 7211-7214, 118 Stat. 3638 (2004).

一個全國一致標準的身分證明文件，如駕駛執照和個人身分證。特別是在「美國受恐怖主義襲擊事件全國調查委員」(The National Commission on Terrorist Attacks Upon the United States，簡稱 911 委員會)，的最終報告書中提到假冒他人(impersonation)是恐怖份子實行活動的重要工具方法。旅行文件的重要性對恐怖份子而言就如武器一般[141]，911 事件中，19 名劫機者中就有 18 名使用假冒或非法取得的證件，讓他們得以在美國境內行動自如。911 委員會認為目前偽造、仿冒的假證件太浮濫，需要安全性更高的身分證件，因此建議將全美駕駛執照標準化，以增強駕駛執照和身分證件的安全性及可靠性。同時建議美國聯邦階層應該設立一套標準以規範出生證明、和證明文件的來源，如駕駛執照。[142]

因為 911 委員會的建議，美國國會起草通過了《情報改革與防範恐怖活動法》(IRTPA)。這個法案責成運輸部長(Secretary of Transportation)，並由國土安全部長(Secretary of Homeland Security)提供諮詢協助，授權他們制訂頒佈一份駕駛執照和個人身分證明文件的全國性最低標準，讓該文件為辦理聯邦管轄事務時接受為個人識別使用。[143]

[141] The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States (2004). at 384

[142] *Ibid.* at 390

[143] *See* IRTPA, § 7212: Driver's licenses and personal identification cards..

根據本法，運輸部長在法案生效後的 18 個月內要發佈相關的法規，規範為了任何與聯邦政府進行公務目的所使用的駕駛執照或州居民身分證必須要有該持證人的法律全名(full legal name)、出生日期、性別、駕駛執照號碼或身分證號碼、數位化照片、住址和簽名式樣。[144] 而且這新標準的卡必須要有實體的安全防偽功能，設計來避免竄改、偽造或複製，以防止詐欺使用。這證卡還要符合最低的可供機器辨識(machine-readable)的技術規範，供機器裝置得以閱讀該證卡資料。更進一步的，該法還要求各州在州法規上要明文規定若是發現上述證卡的安全防偽措施有破壞跡象，應將該證卡予以沒入。[145]

本法也要求各州訂立相關法規，規範各州駕駛執照和州居民身分證的授發。還特別強調，這些州法規必須要包含最低的標準，規範申請者應備之文件、驗證文件的程序、和處理申請的標準化程序。[146] 不過本法禁止侵犯到州在授發該州駕駛執照和州居民身分證的自主權限[147]。換言之，不論該州的規定核准授發給哪種人，不論是本國人、外國人；合法或非法居留，本法都必須尊重，無從強制要求其變更。另外，本法沒有規定駕駛執照和州居民身分證的統一式樣，並要求州法規中必須加入保護申請人隱私權的相關規範。

[144] *Ibid.* at § 7212(b)(2)(D)(i)-(vii).
[145] *Ibid.* at § 7212(b)(2)(G).
[146] *Ibid.* at § 7212(b)(2)(A)-(C).
[147] *Ibid.* at § 7212(b)(3)(B)- (C)

148

最後，本法要求各單位依據《行政程序法》(*Administrative Procedure Act*) [149]進行協商式規則訂定，產生出全國性的駕駛執照和個人身分證相關規則標準。。這是設計來將各機關(agency)的代表和相關的利益團體(interest group)聚在一起，共同磋商一體合用的規定內容。本規則制訂委員會被要求必須包括：(1)州和地方政府負責授發駕駛執照和州居民身分證的機關； (2) 州民選官員；(3) 國土安全部[150]，和 (4)利益團體。[151]

但本法還沒真正實施，美國國會在 2005 年就再度的對設立駕駛執照和個人身分證的全國標準著墨，並通過了《真實身分證法》(*REAL ID Act of 2005*) [152]。

第二項　2005 年《真實身分證法》(*REAL ID Act*)

依據 911 事件調查委員會的研究，對恐怖分子而言，旅行證件和武器一樣重要。911 事件中，19 名劫機者中有 18 名使用假冒或非法取得的證件，使他們行動自如。鑑於偽造、仿冒的假身分證件太浮濫，

148 *Ibid.* at § 7212(b)(3)(D)-(E).
149 *See* Negotiated Rulemaking Act of 1990, P.L. 101-648, 104 Stat. 4970 (1990) (codified as amended at 5 U.S.C. §§ 581 et seq.).
150 U.S. Department of Homeland Security
151 *See* IRTPA, supra note 1 at § 7212(b)(4)(A)-(B).
152 *See* Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, P.L. 109-13, §§ 201-207, 119 Stat. 231, 312-16 (2005). 法案在美國國會提案時的名稱叫做「移民安全標準法案」(Immigrant Security Standards bill)

需要安全性高的身分證件。因此 911 委員會建議將全美駕照標準化，以增強駕照和身分證件的安全性及可靠性。原 2004 年通過之《情報改革與防範恐怖活動法》還沒真正實施，美國國會在 2005 年就再度的對設立駕駛執照和個人身分證的全國標準著墨，並通過了《真實身分證法》。《真實身分證法》包含了一些與加強駕駛執照和州居民身分證安全防偽功能的規定，以及對未遵守本法的各州的指示。另外，《真實身分證法》也廢除了一些和《情報改革與防範恐怖活動法》重複和可能衝突的規定。

大體而言，雖然《真實身分證法》並沒有直接將聯邦所要求的標準強加在各州管理駕駛執照和州居民身分證相關的法律法規中，但是各州相關法律法規必須做出部分變更以符合聯邦的要求，用來交換能讓該州所核發的駕駛執照和州居民身分證能為聯邦所接受，讓持證人能據以進入聯邦管轄機構辦理公務和管轄事務範圍從事活動，如搭商業航線班機。[153]

《真實身分證法》明文定義了何謂聯邦「公務目的」(official purpose)。在本法係包括但不限於下列目的：使用聯邦設施服務、乘坐聯邦法管轄的商業航空航線班機、出入核能電廠和其他由國土安全部長依法令所宣布之區域。另外，《真實身分證法》特別廢除原《情

[153] TATELMAN, Todd B., "*The REAL ID Act of 2005: Legal, Regulatory, and Implementation Issues*", CSR Report for Congress (2008). at 3

報改革與防範恐怖活動法》裡§7212 有關要求各單位進行協商式規則訂定，產生出全國性的駕駛執照和個人身分證相關規則標準。《真實身分證法》包括下列重點：

一、訂定駕駛執照或州居民身分證之最低授發標準(Minimum Issuance Standards)：本法 Section 202(c)要求各州在授發駕駛執照或州居民身分證前必須要檢查並確認申請人的：(1) 有照片的身分證明文件或是無照片但同時有申請人的合法全名和出生日期；(2)出生日期；(3)社會安全號碼或確認其因資格問題無法獲得社會安全號碼，和 (4) 申請人姓名和其主要的住址。

二、申請人必須要提示其法律地位的證明(Evidence of Lawful Status)：本法 Section 202(c)(2)(B)要求各州在授發身分證件前必須確認申請者在美國的法律地位，如：(i)美國公民；(ii)合法永久或短起期居留之外國人；(iii)特殊條件限制的永久居民；(iv)獲准者或已以難民身分進入美國者;(v)持有未過期有效的美國非移民簽證或資格者；(vi) 申請政治庇護但能在審查中者；(vii)申請中或已獲得美國保護資格者；(viii)已獲得美國國土安全部同意不遣返[154]者，和(ix)申請調整成為合法永久居民或特殊條件限制的永久居民者。換言之，唯有符合上述條件者，方能申請駕駛執照和州居民身分

[154] IRTPA, Section 202(c)(2)(B)(viii) “has approved deferred action status”

證。

三、增加臨時駕駛執照和州居民身分證(Temporary Drivers' Licenses and Identification Cards)的設計：本法 Section 202(c)(2)(C)規定，若是申請人是依上述(v)到(ix)身分申請駕駛執照或州居民身分證，各州只能授發臨時證。其有效期限則是該申請人合法得在美國居留的期限為限，若原身分無居留期限限制，則該臨時證有效期以一年為限。臨時證之持有者得在提供有效證明文件後，申請延長期限。各州在臨時授發駕駛執照或州居民身分證前必須要檢查並確認申請人的美國政府核發給申請人的居留身分資格文件。除了正式護照外，各州不得接受申請者提供的外國授發之身分文件。

四、根據本法 Section 202 (d)的其他要求 (Other Requirements) ，各州必須要建立下列 13 項程序。其中除了第 11 項外，其他均與身分竊用防制目的有關。這些要求如下：

1. 建置相關技術，將申請者提示的原始證明文件予以數位影像化，使其得以保存並用於電子化傳遞；
2. 保存申請者提示的原始證明文件七年，其電子資料檔十年；
3. 拍攝申請者的面部相貌；
4. 建立有效的程序處理駕照或身分證申請更新時驗證申請者資訊；

5. 利用申請者提供的完整社會安全號碼向社會安全管理局進行確認。當發現該社會安全號碼已被申請者以外之人註冊使用，並用以申請該州的駕駛執照或州居民身分證時，該州必須予以改正或進行必要之行動；
6. 拒絕授發駕駛執照或州居民身分證給仍持有尚未註銷或尚未申請註銷之他州駕駛執照或州居民身分證；
7. 確保製作、處理和存儲駕駛執照或州居民身分證材料和成品卡處所的實體安全無虞；
8. 所有被授權製造或提供駕駛執照或州居民身分證卡的人員均需符合適當的安全等級(security clearance)要求；
9. 建立一套詐偽文件辨識訓練課程，提供給參與駕駛執照或州居民身分證授發作業的人員；
10. 限制駕駛執照或州居民身分證的有效期間到至多八年。
11. 若是該州決定不要依循該法的要求來管理授發其駕駛執照和州居民身分證，則須要在該州之駕駛執照和州居民身分證上要有獨特的顏色標誌和文字說明，讓持用人知道，該證件不得於聯邦公務目的時用為身分證明之用。
12. 各州的駕駛執照或州居民身分證資料庫必須要開放，供其他州得線上存取其資料。

13. 各州的車輛監理機關必須建立一個人資料料庫，用以存儲所有發證的內容資料，至少要包含那些在身分證件上出現的資料，如姓名、證號等；以及駕駛執照持證人之駕駛歷史，包括違規事件、吊銷或是違規記點資料。

上述 13 項要求，除了(11)外，其他均和防制身分竊用有關。

五、販運身分證明文件之防偽功能標章入罪化：本法 Section 203 修正的《美國聯邦法典》18 U.S.C. §1028(a)(8)，使實際或意圖運輸、移轉供製作身分證明文件的防偽功能標章成為一種聯邦罪行。由內文，此謂之身分證明文件並不限於各州發放駕駛執照或之個人身分證，只要是目的是或一般上用於作為身分證明的文件均屬之。而且在此之前，本條只規範只是用於「假的防偽功能」(false identification features)，易言之，必須係完全之偽造品。新法則增加「偽冒或真實的防偽功能」以對抗使用和真品相同的防偽技術，如特殊紙張、視覺變化膠膜(hologram)等，所製造出的身分證明文件贋品，其在外觀上和真品幾乎無異。使用的手段可能是完全重新製造新品，也可能是使用真品加以變造。現在只要是販運身分證明文件的防偽功能標章，不問其為真偽，均有可能觸犯聯邦罪。

另外，本法 Section 203 也要求並授權美國國土安全部，建立一

個適當的航空飛行安全篩選資料庫，存儲曾經在機場因使用偽冒變造身分證明文件，而遭到定罪者的相關個人資料。

第三項　2009 年《通行身分證法》草案 (*Pass ID Act*)

美國國會在 2005 年通過《真實身分證法》(*Real ID Act*)，要求各州政府在 2017 年前完成換發駕照及身分證件，但各州都以經費不足為由沒有在期限前執行完成。更甚者，在 2009 年底執行開始期限截止時，有 26 個州完全或部分拒絕執行《真實身分證法》[155]。於是，聯邦國土安全局提案，準備以《通行身分證法》(*Providing for Additional Security in States' Identification Act of 2009: Pass ID Act*)來取代《真實身分證法》，透過降低證件安全要求，鼓勵州政府加入。2009 年 6 月 15 日，新法案正式由參議員 Daniel K. Akaka (D-HI)和 George V. Voinovich (R-OH)送入美國國會進行討論。

美國國土安全部希望的目標是修正，而不是廢除有爭議的《真實身分證法》(*REAL ID Act*)。新提案的《通行身分證法》(*PASS ID Act*)，費用比較便宜也比較不嚴格，部分經費是由聯邦補助。此外，還加強了的隱私管控和限制。國土安全部將有 9 個月時間撰寫新的法規，各州將有 5 年期限重新印發所有的許可證，並預計在 2016 年完成。

[155] Summary of State Legislation Activity, Countdown to REAL ID, National Conference of State Legislation, available at http://www.ncsl.org/documents/standcomm/sctran/REALIDComplianceReport.pdf (Last visited on 2012/05/23)

但是這新計畫卻同時取消原先為打擊身分竊用的犯罪，要求汽車監理部門與原發證機構核實出生證件，以及讓各州能儲存和交叉檢查相關資料所設立的資料中心。讓原本期待藉由各州身分證授發前有確實文件認證，並有各州得共用之電子資料庫供查詢認證，來鑑別持證人正確身分，減少冒領事件，進而控制身分竊用問題的作法，在新計畫下恐無以實現。

第三節　消費者信用報告之相關法律

信用之使用，乃是人類歷史上之一大創舉，使得人們能夠以信用作為交易的媒介，兌換所需之商品與服務。同時因分期付款機制(installment plan)、循環信用(revolving credit)等之信用工具的革新，及信用來源的多元化，借貸於道德上之合理化的影響下，讓消費者信用的發展更加興盛。消費者信用的發展過程中，卻也因信用市場上之資訊不對等(asymmetric information)的情況，產生逆選擇(adverse selection)及道德危險(moral hazard)的問題。為了解決信用市場上的資訊不對等之情況，因而有信用報告機構的產生，提供消費者信用報告與借貸方，以解決逆選擇及道德危機的問題。[156]

[156] 馮聖中，「論金融服務與消費者保護之法律問題」，南台科技大學，財經法律研究所碩士論文（2007）。頁 48。

因為消費者信用資料對現代人的生活影響至劇，所以美國第一份針對個人資料保護的立法就和消費者信用報告有關，應不難理解。一般人所說的個人信用報告其實包含兩個意義：（一）狹義的個人「信用報告」(Credit Report)；和（二）「消費者報告」(Consumer Report)。「消費者報告」的內容會參考「個人信用報告」，但反之則不然。

個人「信用報告」(Credit Report)就是個人的信用消費活動和評分記錄。這報告條列出個人所有的信用卡或是貸款帳戶、餘額以及繳款和欠款記錄；還包括因為欠款而衍生的行動[157]，如債務協商、強制停卡等等。個人信用報告內的資料匯總自各金融借貸機構而成，其中內容僅與個人之財務資訊有關。[158]

依照《公平信用報告法》的定義，「消費者報告」(consumer report)是指的是書面、口頭或其它資料形式的報告，其內容含有關於消費者信用評價、信用狀況、信用能力以及個人消費特點、生活方式等。

第一項 1970 年《公平信用報告法》(*FCRA*)

隨著資料保存及通訊技術之發展，各界逐漸重視金融隱私之保護。美國於 1970 年所頒佈施行之《公平信用報告法》(*The Fair Credit*

[157] *See* "*Your Credit Report*", The Federal Reserve Bank of San Francisco, http://www.frbsf.org/publications/consumer/creditreport.html#what (Last visited on 2012/06/12)

[158] *See* "*Investigative Consumer Reports vs. Credit Reports*", February 16, 2009, http://www.gobankingrates.com/credit/investigative-consumer-reports-vs-credit-reports/ (Last visited on 2012/06/12)

Reporting Act of 1970: FCRA)[159]。公平信用報告法於 1971 年 4 月開始實施,所規範的主體是消費者信用報告機構和報告的使用者(如銀行、貸款商等)。

《公平信用報告法》主要在規範消費者對於使用其個人資料之行為享有知的權利,乃至於有權知悉政府機關或其他組織在未經其同意下,蒐集及傳輸信用資料及其他個人資料。此外,《公平信用報告法》除建立消費者報告機構(consumer reporting agency: CRA)[160]蒐集及儲存消費者信用及其他資料之標準外,尚限制消費者報告機構不得任意公開消費者報告資料,僅得於特定許可目的內進行資料之傳輸。[161]

對消費者而言,《公平信用報告法》保證了他們有權瞭解任何一家信用報告機構對自己信用狀況的評價及依據,並具有對不實負面資訊的申訴權利。對於消費者信用報告機構而言,《公平信用報告法》規範了消費者信用報告使用和傳播的範圍,明確了信用報告機構的經營方式。比如合法使用消費者資信調查報告的機構或人必須符合下列條件,否則即使當事人同意也屬違法行為:與信用交易有關、為雇傭目的、保險事務、與合法業務需要有關之需求、以及奉法院的命令或

[159] "The Fair Credit Reporting Act", P.L. 91-508 (Title VI § 601), October 26, 1970, 84 Stat. 1128, 15 U.S.C. § 1681 to 1681u

[160] *See* FCRA, Section 603(e): The term "consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

[161] *See* 15 U.S.C. § 1681B - PERMISSIBLE PURPOSES OF CONSUMER REPORTS

有聯邦陪審團的傳票等。

美國國會後於 1996 年通過《消費者信用報告改革法》(*Consumer Credit Reporting Reform Act of 1996*)大幅修正《公平信用報告法》，以界定消費者報告機構之義務及消費者報告之利用等。其中，最為重要者，在於擴大相關組織之權能，使其會員得共享消費者資訊。亦即在明確向消費者揭露之條件下，各會員間能彼此分享消費者資訊，並讓消費者有機會選擇退出，以拒絕各會員分享其個人資料。[162]之後的《公平正確信用交易法》(*Fair and Accurate Credit Transactions Act of 2003: FACT Act*) [163]則再度將《公平信用報告法》的 Section 605A、605B 和 609(a)(1)做大幅修正，並相對的更新了《美國聯邦法典》15 U.S.C. §1681c–1、§1681c–2 和§1681g (a)(1)。如後述。

《公平信用報告法》加諸於消費者報告機構(CRA)之義務

《公平信用報告法》發展迄今，其加諸於消費者報告機構(CRA)各項義務如下：[164]

1. 消費者報告機構必須在核准目的範圍內提供消費者報告(Section 604)；

[162] *See* Ireland, O. and R. Howell (2004), supra note 2, at 677.
[163] "The Fair and Accurate Credit Transactions Act of 2003", P.L. 108-159, Enacted H.R. 2622 / S. 1753, December 4, 2003, 117 Stat. 1952, U.S.C. § 1681 et seq.
[164] *See* "*40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations*", Federal Trade Commission, July 2011, at 28. Available at http://www.ftc.gov/os/2011/07/110720fcrareport.pdf (Last checked on 2012/07/29)

2. 實施打擊身分竊用的相關作為(Sections 605A, 605B)；
3. 避免提供過時的負面訊息於部分的消費者報告 (Sections 605, 607(a))；
4. 採用合理程序以確保消費者報告的隱私保護(Sections 604, 607(a))和正確性(Section 607(b)；
5. 揭露最低限度的資訊予政府機關(Section 608)，除非該案與反情報及反恐怖主義目的有關(Sections 625-626)；
6. 依消費者請求，揭露相關資訊 (Sections 609 and 610) 並在無償或支付合理之費用下進行(Section 612)；
7. 依照一定程序處理客戶抱怨其個人檔案的完整性或是正確性(Section 611)；
8. 依照一定程序提供公開訊息供聘僱目使用或當提供非公開資訊之負面訊息於消費者調查報告(investigative consumer report)內時(Sections 613, 614)；和
9. 對於消費者報告機構(CRA)轉手販售其他消費者報告機構所製作的消費者報告增列有額外的義務(Section 607(e))。

《公平信用報告法》之行政罰則

在行政罰則部分[165]，依 1996 年版本《公平信用報告法》Section 621(a)(2)(A)[166]，每一違規行為(violation)之罰鍰金額為$2,500 美元，聯邦貿易委員會在 2009 年依照《聯邦民事罰鍰通貨膨脹調整法》(*Federal Civil Penalties Inflation Adjustment Act of 1990*)的規定將其調高為$3,500 美元，並自該年 2 月 9 日起生效[167]。在決定實際罰鍰金額時，依《公平信用報告法》Section 621(a)(2)(B)法院必須考慮該事件的惡行程度、受罰者過去是否有類似之犯行、罰鍰償付能力、對持續其業務的影響和其他為實現正義的考量點。[168]

與身分竊用有關之處罰案例

迄 2011 年，在美國實施《公平信用報告法》的 40 年中，聯邦貿易委員會共執行了 87 件執法行動(enforcement actions)，處罰消費者報告機構、消費者信用報告使用者和信用報告機構的資料提供者(furnishers of information to CRAs)。

其中一個具指標性且與身分竊用有關的案例為 2006 年的 United States v. ChoicePoint, Inc. [169]案。在本案，聯邦貿易委員會指控

[165] *Ibid*, at 3-4.
[166] *See* also 15 USC § 1681S(2)(A): Knowing violations
[167] *See* 74 Fed. Reg. 857 (Jan. 9, 2009)
[168] *See* also 15 USC § 1681S(2)(B): Determining penalty amount
[169] *See* United States v. ChoicePoint, Inc., No. 1:06cv198 (N.D. Ga. Feb. 15, 2006) (consent order) as well as "*40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of*

ChoicePoint 公司提供信用報告給冒充為 ChoicePoint 客戶的身分竊賊。ChoicePoint 因而違反《公平信用報告法》的規定，提供消費者信用報告給不具合法使用目的的人，且未維持合理的程序驗證消費者信用報告的收受人和其使用目的。為解決本案，ChoicePoint 同意支付 $10,000,000 美元的罰鍰－在當時為聯邦貿易委員會歷史以來最大的罰鍰金額－以及支付$5,000,000 美元給身分竊用受害者。

第二項　2003 年《公平正確信用交易法》(*FACT Act*)

鑒於身分竊用案件因科技及資訊之發展而日益猖獗，美國於 2003 年 12 月 4 日公布《公平正確信用交易法》(*FACT Act*)，以協助消費者及金融機構共同打擊犯罪。

《公平正確信用交易法》的 Section 5 修正了之前的《公平信用報告法》，特別加入和身分竊用及其與消費者相關的事項。本法讓身分竊用受害者得以要求金融機構等借貸人(creditor)及信用報告機構(credit bureau)，將其個人信用記錄中因遭身分竊用犯罪受害影響而被註記的負面資訊予以移除。

《公平正確信用交易法》建立金融詐欺行為預警制度，如消費者發現其可能因身分遭冒用或金融詐欺而受損害時，得以通知消費者報

Interpretations", Federal Trade Commission, July 2011, footnote 19.

告之使用者，以降低消費者遭詐欺受害之機率。當消費者懷疑已經或即將成為身分竊用的犯罪被害者，他們可以通知信用報告機構，要求在其個人信用檔案中加入「初級警戒」(initial alert)註記[170]。當消費者確定成為身分竊用的受害者，而且已經向執法機關報案，隨後他可以要求信用報告機構在其個人信用檔案中加入「延長警戒」 (extended alert) 註記[171]。這「延長警戒」會在其個人信用檔案留存七年，且這受害人可以在 12 個月內要求信用報告機構免費提供他的個人信用報告兩次，以供其積極注意信用狀況的變化。對於信用報告機構端，一旦有客戶信用檔案註記上「延長警戒」，其必須在接來的五年中，要將該客戶資料自提供給信用或保險公司作事先篩選主動銷售的名單中移除[172]。另外，為了保護戎馬倥傯、為國征戰的軍方人員，本法特別設計讓他們在被徵召服現役或是被派往與原駐地相聚很遠的單位時，可以要求信用報告機構在其個人信用檔案加註「現役軍人警戒」(active duty alert)[173]。

《公平正確信用交易法》還讓身分竊用受害者在提供消費者信用報告機構必要的文件[174]後，該機構必須在四個工作日內封鎖該受害者之在該機構的相關檔案，不得再使用。同時，該機構必須通知其他消

[170] *See* 15 U.S.C. § 1681C–1(a)(1)
[171] *See* 15 U.S.C. § 1681C–1(b)
[172] 原文：…credit agencies must exclude the consumer's name from lists used to make pre-screened credit or insurance offers.
[173] *See* 15 U.S.C. § 1681C–1(c)
[174] *See* 15 U.S.C. § 1681C–2(a)(1)~(4)

費者信用報告機構，同時進行資料封鎖，以避免身分竊用受害影響擴大[175]。當然，信用報告機構也可以依法判斷是否給予封鎖或解除封鎖[176]。

《公平正確信用交易法》並設立相關的規定來防範身分竊用。如：要求商家不得將客戶的信用卡號碼資料印在收據上，也讓消費者可以要求信用報告機構，當被要求出具他們的信用報告時將其個人社會安全號碼自報告中移除等[177]。

聯邦貿易委員會透過《公平信用報告法》和《公平正確信用交易法》授與的權限，發佈過諸多命令：如要求金融機關與信用卡公司強化對民眾信用資料準確性的維護[178]、建立民眾對錯誤信用資料的回報和業者的快速處理機制[179]，並要求三家全國性的信用報告公司 Equifax、Experian 與 Trans Union 應免費提供消費者年度信用報告供查閱。[180]聯邦貿易委員會同時要求信用報告公司應在網站與新聞媒體上加強對消費者的教育，宣導信用報告「免費取得」的意旨，避免消費者被他人冒名開戶、信用受損而不自知[181]。

---

[175] *See* 15 U.S.C. § 1681C–2(b)
[176] *See* 15 U.S.C. § 1681C–2(b)
[177] *See* 15 U.S.C. § 1681g(a)(1)(A)
[178] Agencies Issue Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy, http://www.ftc.gov/opa/2007/10/redflag.shtm (Last visited on 2012/06/10)
[179] Agencies Issue Final Rules on Accuracy of Credit Report Information and Allowing Direct Disputes, http://www.ftc.gov/opa/2009/07/facta.shtm (Last visited on 2012/06/10)
[180] Agencies Issue Final Rules on Risk-Based Pricing Notices, http://www.ftc.gov/opa/2009/12/rbpricing.shtm (Last visited on 2012/06/10)
[181] 吳兆琰，「美國 anti-phishing 法制策略簡介」，《台灣電腦網路危機處理暨協調中心(TWCERT/CC)電子報》，2011 年 1 月號，http://newsletter.certcc.org.tw/epaper/201101/report3_1.html，(前次檢

第三項　1974 年《公平信用帳務法》

1968 年頒佈施行的《誠實借貸法》(*Truth in Lending Act*)[182]，立法宗旨在於規範授信機構公開揭露借貸期限與信用成本等資訊，以利消費者瞭解各授信機構提供之信用條件，並幫助消費者比較授信單位提供信用條件之優劣。美國於 1974 年頒佈施行《公平信用帳務法》(*Fair Credit Billing Act*)[183]，則部分修正了《美國聯邦法典》15 U.S.C. §1601(a)，於其後段文字加入「…並保護消費者不被不正確和不公平的信用帳務所害。」

《公平信用帳務法》建立了一連串的程序要求，讓消費者得以收到其信用卡消費帳單後，在一定時間範圍內，得以向其信用卡機構以書面形式檢附理由，呈報未經其授權的信用卡消費活動並要求更正其信用消費記錄[184]。如此的規定能讓消費者在被身分竊用受害，信用卡被冒用盜刷時，獲得財務保護（只需負擔 50 美元的債務責任）[185]，並得以更正其信用記錄。

因為本法，信用卡機構必須要更正消費者被冒名盜刷的信用消費和記錄，信用卡機構也要先承擔因之而生的財務損失，所以信用卡機構為了保障自己的權益，就必須建置一套程序機制確定交易指示的人

索日：2012/06/10）

[182] Truth in Lending Act, P.L. 90-321 (Title I § 104), May 29, 1968, 82 Stat. 147, 15 U.S.C. § 1601

[183] Fair Credit Billing Act, P.L. 93-495 (Title III), October 28, 1974, 88 Stat. 1511, 15 U.S.C § 1666 et seq.

[184] *See* 15 U.S.C. § 1666 - CORRECTION OF BILLING ERRORS

[185] *See* 15 U.S.C. § 1666(e)

確為本人授權，而非冒名者，從而防止或抑制身分竊用事件發生。

第四項　1978 年《電子化資金移轉法》

美國於 1978 年頒佈施行《電子化資金移轉法》(*Electronic Fund Transfer Act*)，用來規範客戶與金融服務提供者間在電子化交易環境下的權利義務關係，依賴詳盡告知原則(comprehensive disclosure)來分配消費者與金融服務提供者間的危險與責任，並賦予消費者在使用信用卡或簽帳卡時獲得有限責任的保護，並由金融機構來負舉證責任[186]。

因為本《電子化資金移轉法》規定電子化金融交易服務提供者必須要證明交易的存在並提供記錄文件[187]，所以金融服務提供者為了保障自己的權益，也如同對《公平信用帳務法》般，必須建置一套程序機制確定交易指示的人確為本人授權，而非冒名者，從而防制身分竊用事件發生。

第四節　隱私權及個人資料保護之相關法律

由於美國之國家體制為聯邦制，相較於其他國家，並未制定全國

[186] "Electronic Fund Transfer Act", P.L. 95-630 (Title IX § 2001), November 10, 1978, 92 Stat. 3728, 15 U.S.C. § 1693 et seq. /

[187] *See* 15 U.S.C. § 1693D - DOCUMENTATION OF TRANSFERS

統一適用之《隱私權法》,而是由各州及聯邦政府基於權力分立原則，分別立法規範[188]。其中，在聯邦立法層次，除關注個人健保資料(healthcare privacy)之保護外，更特別重視消費者金融隱私(consumer financial privacy)之保護[189]。雖然美國國會先後制定通過許多與個人資料保護相關之隱私權法案，而金融主管機關亦對於個人金融資料之保護，頒訂相關行政命令，但國會似乎不願意制定一部足以包羅所有個人資料之隱私權法案[190]；相對地，美國是依其社會經濟之各個發展階段，建構出各種錯落分散之隱私權法制。

依據美國學者 William L. Prosser 之整理[191]及《美國侵權行為法論》之對照[192]，隱私權受侵害之類型主要有下列四種：(1)個人獨居之不合理入侵[193]；(2)個人姓名或肖像之竊用[194]；(3)個人私密生活之不合理公開[195]；(4)將個人置於公眾之錯誤觀感下而為不合理公開[196]。又觀諸美國聯邦最高法院之諸多判決，亦試圖採取各種不同之方法，以勾繪出隱私權之基本特徵。例如所謂「不受干涉之權利－最廣泛及最受文

[188] *See* Nojeim, G. T.(2000), "*Financial Privacy*", N.Y.L. Sch. J. Hum. Rts., 17, 81, at 90.

[189] *See* Ireland, O. and R. Howell (2004), "*The Fear Factor：Privacy, Fear, and the Changing Hegemony of the American People and the Right to Privacy*", N.C.J. Int'l L. and Com. Reg., 29, at 671, 673.

[190] *See* Sammin, K. T. (2004), "*Note: Any Port in a Storm: The Safe Harbor, the Gramm-Leach-Bliley Act, and the Problem of Privacy in Financial Services*", Geo. Wash. Int'l L. Rev.,36, at 653, 657.

[191] *See* Prosser, W. L. (1960), "Privacy," Cal. L. Rev., 48, at 383-419. 轉引自劉佐國，「我國個人資料隱私權益之保護—論『電腦處理個人資料保護法』之立法與修法過程」，《律師雜誌》，第 307 期，2004 年一月，42-51 頁。

[192] "*Restatement of Torts*", American Law Institute, 2nd edition (1977), 652A-652I

[193] *Ibid.* 652A(2)(a), 652B: unreasonably intrudes upon an individual's seclusion

[194] *Ibid.* 652A(2)(b), 652C: appropriates an individual's name or likeness

[195] *Ibid.* 652A(2)(c), 652D : unreasonably publicizes an Individual's private life

[196] *Ibid.* 652A(2)(d), 652E: unreasonably publicizes an individual to place him or her in a false light before the public

明人類重視之權利」[197]、「避免個人資料公開」及「作成特定類型重要決定之獨立性」之結合[198]。

關於隱私利益之內涵[199]，美國學者 Judith W. Decew 認為包括：資訊隱私(information privacy)、接觸隱私(accessibility privacy)和表達隱私(expressive privacy)，其中資訊隱私是指對個人資料的控制。除了公眾人物，一般人的個人資料，無須接受公眾檢視。一個人的日常活動、個人的生活方式、財務狀況、醫療歷史及學術成就等，不論形於文字與否，也不管為公共記錄之一部分，均可被個人視為無須揭露予他人之資訊，且應當受到保護。其雖非隱私之全部意涵，但以構成隱私課題之基本核心。

基本上個人資料「資料外洩」(data breach)可以被瞭解是某機關組織未經授權或是不經意的暴露、揭露或是遺失重要敏感的個人資訊。這個人資訊可能包括足供識別為個人資料(individual identifiable data)的資訊，如姓名、住址、社會安全號碼或財務資訊，如信用卡卡號等。資料外洩的形式有很多種，但是它並不必然會造成身分竊用事件[200]。

---

[197] *See* "Olmstead v. United States", 277 U.S. 438, at 475(1928)(Brandeis, J., dissenting)，轉引自劉佐國(2004)。原文為："the right to be let alone – the most comprehensive of rights and the right most valued by civilized men".

[198] *See* Whalen v. Roe, 429 U.S. 589, at 599-600(1977). 原文分別為：" avoiding disclosure of personal matters"和" independence in making certain kinds of important decisions".

[199] Judith Wagner Decew, "*Pursuit of Privacy. Laws, Ethics and the Rise of Technology*", 1997。轉引自陳起行，「隱私權法理之探討-以美國法為中心」，《政大法學評論》，2000 年 12 月。頁 297-341。

[200] "*Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*" (GAO-07-737), United States Government Accountability Office, June 4 2007, at Hightlines page

據美國政府責任辦公室(Government Accountability Office: GAO)[201]在2007 年發佈的報告表示：因為資料外洩而造成身分竊用的影響範圍尚難清楚得知，絕大部分的原因是無法知道是哪些資料外洩事件對應造成哪些身分竊用事件。不過，從已知的資料和研究學者、執法機關人員以及業界代表的訪談中可以探知，絕大部分資料外洩事件並沒有找到可以直接對應的身分竊用事件，特別是如同時間有未經授權開立的帳戶等。雖然現階段無足夠資料證明在資料外洩事件和身分竊用的事件發生有正相關，但不可否認的，依通念，個人資料的安全和隱私管理是防制身分竊用的重要手段之一。

一直以來，美國在個人資料保護作為上比較傾向建置一個結合法規、命令和自我管理的架構，而非由政府制訂的單一法規，如前面章節所述之《公平信用報告法》等之消費者信用資料保護等。美國前總統 Bill Clinton 和副總統 Al Gore 曾清楚明白的在他們所提議的「全球電子商業架構」(Framework for Global Electronic Commerce)中提倡私部門必須領導和實行自我管理來應對網際網路科技所帶來的各種問題[202]。迄今，美國並無單一的個人資料保護法規可以和歐盟的「個人

[201] 在 2004 年由 General Accounting Office 「審計總署」改名為 Government Accountability Office，「政府責任辦公室」。

[202] *See* William J. Clinton & Albert Gore, Jr., "*A Framework for Global Electronic Commerce*", July 1, 1997, available athttp://www.technology.gov/digeconomy/framewrk.htm; *See* also Robert R. Schriver, You Cheated, You Lied: the Safe Harbor Agreement and Its Enforcement By the Federal Trade Commission, 70 Fordham L. Rev. 2777, 2779 (2002)，轉引自劉佐國(2004)。

資料處理保護指令」(EU Data Protection Directive) [203]直接對應。

惟美國因為受到歐盟的經貿壓力，美國與歐盟為解決跨國個人資料流動之問題，由美國商業部(U.S. Department of Commerce)與歐盟執行委員會(E.U. Executive Commission)在 1998 年開始進行協議，試圖建立遵守個人資料保護之機制。最後，雙方在妥協之下，簽訂一項「安全港計畫」(U.S.-EU Safe Harbor program) [204]，並於 2000 年 11 月 1 日正式生效[205]。基本上，「安全港計畫」為一自願性計畫(voluntary program)[206]，明定舉凡聯邦貿易委員會及運輸部(U.S. Department of Transportation)所管轄之企業或組織，得主動申請加入「安全港計畫」，並遵守聯邦貿易委員會之規定，以取得認證。[207]

第一項 1974 年《隱私權法》

在公布制定《公平信用報告法》後，美國衛生、教育及福利部之 Elliot L. Richardson 部長，隨即於 1972 年組成「個人資料自動化系統部長諮詢委員會」(下稱「個資系統諮委會」) [208]，以因應及解決因不

[203] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[204] "U.S.-EU Safe Harbor Overview ", U.S. Department of Commerce, Available at http://export.gov/safeharbor/eu/eg_main_018476.asp (Last checked on 2012/06/20)

[205] *See* Safe Harbor Overview, available at http://export.gov/safeharbor/eu/eg_main_018365.asp, last checked on 2012-05-04

[206] *See* DiLascio, T.(2004), "*Note: How Safe Is the Safe Harbor? U.S. and E.U. Data Privacy Law and the Enforcement of the FTC's Safe Harbor Program*," B.U. Int'l L. J., 22, at 399, 415(2004).

[207] *See* Safe Harbor Workbook, available at http://export.gov/safeharbor/eg_main_018238.asp, last checked on 2012-05-12.

[208] The Secretary's Advisory Committee on Automated Personal Data Systems

當運用電腦及通訊科技蒐集、儲存及利用個人資料，而與日俱增之隱私權侵害案件。個資系統諮委會於分析當時之問題後，並建議採取相關措施。個資系統諮委會所提出之「市民之紀錄、電腦及權利」報告(HEW Report)[209]，不僅納入「公平資訊交易規範」(Code of Fair Information Practice)中，且其所歸納出之五項公平資訊隱私原則，則整合成為 1974 年公布之《隱私權法》(*Privacy Act of 1974*)[210]，並成為美國隱私及資訊政策之重要基礎[211]。

美國 1974 年《隱私權法》主要是讓個人有更多的選擇和管制政府蒐集和使用個人的識別資訊。本法規範聯邦政府所搜集的個人資料公布於眾時，應該通知當事人該情事，且政府機關只得蒐集為達成其業務所需的必要個人資料[212]。同時，聯邦機構並被限制揭露其所蒐集之個人資料的限度和條件，且其揭露必須要有個人之書面揭露同意函、正式收達之法院命令、或符合本法所列之除外條件等，方能為之。而按上開法律之規定，所謂的「個人資料」意指，包含個人之教育、金融交易、醫療紀錄、犯罪前科及受雇紀錄之中關於個人之姓名、識別號碼、象徵或其他足以辨識個人如指紋、聲紋或相片之資料[213]。

---

[209] *See* "*Records, Computers and Rights of Citizens*", Health, Education, and Welfare Secretary's Advisory Committee on Automated Personal Data Systems, 1973 , available at http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm，轉引自劉佐國(2004)。

[210] "Privacy Act of 1974", P.L. 93-579, Enacted S.3418, December 31, 1974, 88 Stat. 1896, Codified 5 U.S.C. § 552a

[211] *See* Ireland, O. and R. Howell(2004), at 674.，轉引自劉佐國(2004)。

[212] *See* 5 U.S.C. § 552a(e)(1)

[213] *See* 5 U.S.C. § 552a(a)(4)

在以個人之社會安全號碼為識別索引的管理上，依照本法第七章(Section 7)[214]，美國聯邦及各州機關不得因人民拒絕提供其社會安全號碼而否准其依法享有之權利、福利或特權。又，美國聯邦及各州機關若要求人民提供其社會安全號碼時，必須告知人民此要求係依何種法律要求之必要行為，或是其係屬可由人民選擇自願配合的項目。在實務判例上，有私人公司員工因為拒絕向雇主提供其個人之社會安全號碼而遭到開除，在上訴至聯邦巡迴法庭後敗訴。聯邦法官認為雇主要求其雇員提供社會安全號碼並未違反雇員在憲法上之權利。[215] 該雇員聲稱如果她提供其個人之社會安全號碼給雇主，將使得她遭受到身分被竊用的可怕危險(dire jeopardy)中。[216] 不過，聯邦法院判決認為，美國憲法所保護的隱私權不及於個人的社會安全號碼，且法律要求雇主要取得其雇員的社會安全號碼有其正當性。[217]

1974 年的《隱私權法》在個人隱私權的保障上是一個里程碑，但是它卻沒有規範到如個人資料販賣商、蒐集機構或是消費者信用報告機構等私部門進行的個人資料蒐集運用時對個人隱私權的保護責任。《隱私權法》第七章(Section 7)並沒有限制私部門對於社會安全號碼的利用限制。於是，私人商業和機構仍要求相對人提供其個人之社

[214] *See* 5 U.S.C. § 552a (note), Sec. 7(a) ,(b), available at http://www.justice.gov/opcl/privstat.htm, Last visited on 2012/05/04

[215] 436 F.3d 74 (2nd Cir. 2006): Dianne W. Cassano, Plaintiff-appellant, v. Allen Carb, Arnold Lessor, North Shore Veterinary Surgery, Defendants-appellees, twelve John and Jane Does, Individually, Defendants. docket No. 04-6712-cv.

[216] *Ibid*.

[217] *Ibid.*, at 75-6

會安全號碼以交換貨品或服務，而且基本上沒有聯邦法規規範那些交易。[218]

第二項　1994 年《駕駛人資料隱私保護法》

在 1997 年以前，在很多的州，任何人只要向當地的汽車監理機關(Department of Motor Vehicles)付少許費用可以輕易的購買到他人的駕照資料。區區的幾美元，個人資料如持照人的全名、住址、出生日期、和駕照號碼。特別值得一提的是，當時在不少的州，駕照的號碼就是直接用持照人的社會安全號碼[219]。所以，政府的汽車監理機關成為有心進行身分竊用行為人一個最簡單且最便宜獲得他人個人資料的地方。

因為 Rebecca Schaeffer 的謀殺案[220]所引起的重視，美國國會於 1994 年通過《駕駛人資料隱私保護法》(*Driver's Privacy Protection Act, DPPA*) [221]，限制了政府汽車監理機關對駕駛人資料得揭露的範圍[222]，

[218] *Ibid.*, SWENDIMAN (2008)

[219] 在台灣，汽（機）車駕駛執照證號就是持照人的國民身分證號。又如，作者所持有的美國聯邦航空總署(FAA)飛行員執照原本的證號也是個人的 SSN。2002 年六月後該總署停止使用 SSN 為證號，改用序號為新證號，同時通知各原持證人，可以自由選擇是否將 SSN 移除，並改為新證號。

[220] Rebecca Schaeffer 是一位知名演員，有一位瘋狂愛慕者 Robert John Bardo 依當時的規定，在加州汽車監理機關處輕易獲得 Rebecca Schaeffer 的住址，因而得以埋伏在其住處並進而殺害 Rebecca Schaeffer。這案件間接催生了 DPPA 法案。

[221] "Drivers Privacy Protection Act of 1994", P.L. 103-322 (Title XXX), amended by 106-69, Enacted, as amendment to H.R. 3355, September 13, 1994, 108 Stat. 2099, 18 U.S.C. §§ 2721-2725。

[222] 18 U.S.C. § 2721 - PROHIBITION ON RELEASE AND USE OF CERTAIN PERSONAL INFORMATION FROM STATE MOTOR VEHICLE RECORDS

讓不法人士從政府汽車監理機關處獲得他人個人識別資料更加的困難。

不過這法案的施行也不是一帆風順，在 2000 年 Reno v. Condon[223] 的案件中，南卡羅來納州(South Carolina) 的法院就認為《駕駛人資料隱私保護法》違反了美國的聯邦體制，一路纏訟至美國聯邦最高法院。最後美國聯邦最高法院認為美國國會所立的《駕駛人資料隱私保護法》因符合《美國聯邦憲法》中的「商務條款」(Commerce Clause) [224]而判決合憲。

第三項　1996 年《健康保險可攜性及責任法》(HIPPA)

1996 年之《健康保險可攜性及責任法》(*Health Insurance Portability and Accountability Act of 1996, HIPAA*)[225]要求醫療照護機構和保險公司為增加保密性和效率必須建立和維持電子化的病友病歷資料庫。在其保密性原則的要求下，限制了醫師、健康保險計畫、藥師、醫院和醫療照護單位等可以使用病友病歷資料庫的方式。《健康保險可攜性及責任法》(HIPPA)將所有來自醫療照護機構、健康保險計畫、公共衛生部門、雇主、人壽保險、學校或醫療資料清算服務單位

[223] "Reno v. Condon", 528 U.S. 141, 120 S.Ct. 666 145, L.Ed.2d 587
[224] United States Constitution, Article I, Section 8, Clause 3
[225] "Health Insurance Portability and Accountability Act of 1996 (HIPAA)", P.L. 104-191, Enacted H.R. 3103, August 21, 1996, 110 Stat. 1936, codified 42 U.S.C. § 1320

等的病友可供識別為個人的健康和病歷資料都納入保護範圍[226]。

本法也要求醫療照護機構必須要有隱私權保護宣言，清楚說明該機構不會在未獲得病友的同意前將其可供識別為個人的健康和病歷資料分享給其他人。換言之，醫療照護機構必須先獲得病友之同意才可以揭露其健康病歷資訊。而且，本法也加入了一旦該等資料的安全性被破壞時，醫療照護機構通知受影響病友的義務。

在身分竊用的各種影響中，「醫藥身分竊用」(medical identity theft)是其中一種不容忽視的現象。犯罪者利用不法獲得的他人身分資訊和病史健康資訊冒名對醫療機構進行詐騙，以獲得醫療照護、藥品或保險給付。而醫藥身分竊用被害人會因此背負額外的費用、不正確的醫療使和額外增加的醫療保險費用等。[227]病友病歷資料庫的保護除隱私權考量外，尚有防制身分竊用之目的。

為了嚇阻犯罪者利用身分竊用手法詐騙醫療照護機構，致使病友病歷資料庫之內容外洩，美國司法部亦在2005年六月做出函令解釋，明白定義此行為違反《健康保險可攜性及責任法》(HIPPA)規定。美國司法部發佈關於 HIPPA 的法令解釋，清楚的定義其刑罰的適用範圍。[228] 本法涵蓋人士若故意非法獲得或揭露可供識別為個人的健康資料，

[226] *See* 42 U.S.C. § 1320d(4)

[227] 參考自 FTC 網站 http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt10.shtm. (Last visited on 2012/06/17))

[228] "SCOPE OF CRIMINAL ENFORCEMENT UNDER 42 U.S.C. § 1320d-6", MEMORANDUM OPINION, U.S. Department of Justice, June 1, 2005, available at http://www.justice.gov/olc/hipaa_final.htm (Last

可處 1 年以下有期徒刑，得併科 50,000 美元以下罰金。若是以身分竊用手段，偽冒為本法涵蓋人員而從事上述不法行為，則可處 5 年以下有期徒刑，得併科 100,000 美元以下罰金。最嚴重者，若故意非法獲得或揭露可供識別為個人的健康資料之目的係企圖為商業營利、個人利益或惡意破壞等，則可處 10 年以下有期徒刑，得併科 250,000 美元以下罰金。[229]

第四項　1999 年《金融服務現代化法》(*GLBA*)

美國於 1999 年 11 月 12 日制定公布《金融服務現代化法》(*Financial Services Modernization Act of1999*)，一般又稱為 *Gramm-Leach-Bliley Act* (*GLBA*)，部分規範了金融機構在銷售消費者財務金融資訊應有的保護作為。本法立法目的係為取消銀行法(*The Banking Act of 1933*)以及銀行控股公司法(*Bank Holding Company Act of 1956*)對銀行、證券、保險業透過合併從事跨業經營的障礙，以容許設立「金融超級市場」(financial supermarket)，一方面加強金融服務業的競爭，以造福消費者，另一方面用以提高美國金融服務業之國

checked on 2012/06/20)

[229] "HIPAA Violations and Enforcement - Failure to comply with HIPAA can result in civil and criminal penalties (42 USC § 1320d-5)", American Medical Association website. Available at http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page (Last checked on 2012/06/20)

際競爭力[230]。

金融業者認為該法案得以提高金融業競爭的原因之一，在於金融業跨越原本銀行、證券、保險業分立的藩籬後，合併經營後，得以產生更具效益的經濟規模，降低提供金融商品和服務的平均成本。尤其該法案容許金融集團內之關係企業交互運用其客戶資料，將其視為一體之資產，更有助於提高經營效率。但此提供金融集團處理其客戶資料的便利時，同時亦引起對顧客隱私權侵犯的隱憂。隱私權保護團體因此提議應對金融集團之顧客個人資料運用及流通設立合理的限制[231]。因此美國國會順應此種發展和要求，遂訂定資訊隱私權的保護規定。

《金融服務現代化法》有關金融客戶資訊隱私權的規範被編入《美國聯邦法典》第 15 篇第 94 章第 1 分章「非公共個人資料之揭露」[232]，以及第 2 分章「以詐欺手法獲取財務資訊」[233]。在這兩個分章中均含有關於禁制利用身分竊用手法，冒名蒐集或揭露消費者金融財物資訊的規定。

---

[230] Edward J. Janger & Paul M. Schwartz, “The Gramm-Leach-Biley Act, Information Privacy, and the Limits of Default Rules”, 86 Minn L. Rev. 1219, 1222-1223 (2002) 轉引自陳妍沂，「美國財務資訊隱私權保護規定之研究」，國立政治大學法學院碩士在職專班碩士學位論文，2008 年 5 月。

[231] Jolina C. Cauaresma, “The Gramm-Leach-Biley Act”, 17 Berkley Tech. L.J. 497, 501-502 (2002), 轉引自陳妍沂(2008)

[232] *See* 15 U.S.C. CHAPTER 94, SUBCHAPTER I - DISCLOSURE OF NONPUBLIC PERSONAL INFORMATION (15 U.S.C. § 6801-6809)

[233] *See* 15 U.S.C. CHAPTER 94, SUBCHAPTER II - FRAUDULENT ACCESS TO FINANCIAL INFORMATION (15 U.S.C. § 6821-6827)

《金融服務現代化法》還指示八個聯邦金融監管機關[234]和各州要管理和執行(enforce)其中之財物隱私規則(Financial Privacy Rule)和保護規則(Safeguards Rule)，確認各金融機構建有避免未經授權揭露金融消費者的金融財物資訊的相關政策、程序和內部控制措施。此處之「未經授權揭露」包含金融機構因受騙而揭露。

另外，為解決美國與歐盟間跨國個人資料流動之問題，美國商業部與歐盟執行委員簽訂「安全港計畫」。基本上，「安全港計畫」為一自願性計畫，明定舉凡美國聯邦貿易委員會及運輸部所管轄之企業或組織，得主動申請加入計畫，並遵守聯邦貿易委員會之規定。但美國與歐盟於所簽訂之「安全港計畫」，並未涵蓋有關金融服務業及相關行業之個人資料處理[235]。

雖然《金融服務現代化法》將隱私權法制加於金融服務業之內容，並非與「安全港計畫」完全相同，但形式上與歐盟「個人資料處理保護指令」(EU Data Protection Directive) [236]及「安全港計畫」加於其他產業並無不同。基本上，《金融服務現代化法》所建立之金融隱私權

[234] 分別為：聯邦貿易委員會 (Federal Trade Commission, FTC)、聯邦儲備理事會 (Federal Reserve Board, FRB)、財政部貨幣監理局 (Office of the Comptroller of the Currency, OCC), 聯邦存款保險公司(Federal Deposit Insurance Corporation, FDIC)、證券交易委員會(Securities and Exchange Commission, SEC)、全國信用合作社管理局(National Credit Union Administration, NCUA)、儲蓄機構管理局(Office of Thrift Supervision, OTS)和商品期貨交易委員會(Commodity Futures Trading Commission, CFTC)

[235] *See* Safe Harbor Workbook, available at http://export.gov/safeharbor/eg_main_018238.asp, last checked on 2012-05-12.

[236] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

法制，可以歸納成下列五項原則：（一）通知(notice)；（二）選擇(choice)；（三）市場公開(marketing disclosure)；（四）安全(security)；（五）執行(enforcement.)[237]。應注意者，雖然其用語與美國與歐盟所簽訂之「安全港計畫」部分相同，但其意義卻並非完全一致[238]。

在 2010 年 7 月 21 日通過施行的《多德・法蘭克華爾街改革及金融消費者保護法》(*Dodd–Frank Wall Street Reform and Consumer Protection Act*)[239]中，此部分被劃歸為新成立的「消費者財務保護局」(Bureau of Consumer Financial Protection)所管轄。相關條文亦被改編入美國聯邦規則彙編第 12 篇 1016 章(12 C.F.R. Part 1016)中。

《金融服務現代化法》將隱私權法制加於金融服務業之內容，讓美國在各產業的個人資料保護嚴謹程度整體提昇；又，本法很清楚的將對金融機構的任一職員、主管、代理人或是其客戶，使用任何虛偽證明方式獲得客戶資料的行為入罪化[240]。觸犯者處五年以下徒刑，得併科罰金。前項之未遂犯罰之。[241]。若觸犯者同時亦觸犯其他法律或者其身分竊用行為係其他任何慣常不法行為模式之一部，且於 12 個月期間內其犯罪金額超過 100,000 美元，則處十年以下徒刑，得併科

[237] *See* Swire, P. P.(2002), at 1265-1273. 轉引自王志誠(2004)，「金融商品共同行銷與公平競爭(上)」，《台灣本土法學》，58，16。

[238] *See* Sammin, K. T. (2004), at 663. 轉引自王志誠(2004)

[239] Dodd–Frank Wall Street Reform and Consumer Protection Act, P.L. 11-203, H.R. 4173, July 21, 2010

[240] *See* 15 U.S.C. § 6821 - PRIVACY PROTECTION FOR CUSTOMER INFORMATION OF FINANCIAL INSTITUTIONS and§ 6823 - CRIMINAL PENALTY

[241] *See* 15 U.S.C. § 6821(a)

罰金。若併科罰金時，其罰金金額加倍。前項之未遂犯罰之。[242]此兩者均對防制身分竊用產生助益。

第五項　2000 年《社會安全號碼保密法》

2000 年公佈施行的《社會安全號碼保密法》[243]，修定了《美國聯邦法典》31 U.S.C. §3327，要求美國財政部要建立必要的措施，讓寄送支票或其他匯票時，不會在未經開啟郵件的情況下即顯露出社會安全號碼。本法的目的是為了不讓身分竊用犯輕易獲得被害人的社會安全號碼，進而減少被害的機會。

第六項　2001 年《愛國者法》(*USA PATRIOT Act*)

觀諸美國個人資料保護之聯邦立法，遠從 1945 年制定公布《麥卡倫・佛格森法》(*McCarran–Ferguson Act*)[244]開始，乃至於其後制定公布之《公平信用報告法》、《金融隱私權法》[245]、《知悉客戶規則》提案、《金融服務現代化法》、《愛國者法》及《公平正確信用交易法》等，皆是與個人金融隱私相關。其中《麥卡倫・佛格森法》主要在於限制聯邦政府對保險業管理之權限，《公平信用報告法》則在於限制

[242] *See* 15 U.S.C. § 6821(b)
[243] Social Security Number Confidentiality Act of 2000, P.L. 106-433, Enacted H.R. 3218, November 6, 2000, 114 Stat. 1910, 31 U.S.C. § 3327
[244] *See* McCarran-Ferguson Act, Pub. L. No. 79-15, 59 Stat. 33 (1945), codified at 15 U.S.C. §§ 1011–1015
[245] *See* Right to Financial Privacy Act of 1978 (RFPA), Pub. L. No. 95-630, § 1114, codified at 12 U.S.C. §3401 et seq. (1978).

行政機關及私人部門蒐集及傳輸消費者信用資料及其他個人資料之權限。至於《金融隱私權法》則偏重在規範金融機構將客戶之金融資訊，不當向行政機關傳輸或揭露之行為。相反地，鑒於國際洗錢、金融詐欺及恐怖攻擊事件之嚴重性，美國從金融主管機關於 1998 年公布「知悉客戶規則」提案後，即先後因金融整合及社會發展之需要，先後制定公布《金融服務現代化法》、《愛國者法》及《公平正確信用交易法》，而逐漸調整金融隱私權之保護政策，試圖在隱私權保護與國家利益間取得平衡。

雖然自《金融隱私權法》制定後，各界對於個人金融資訊保護之爭論稍歇，但其後因洗錢問題叢生，致使金融主管機關必須採取必要措施，以免社會大眾之金融資訊隱私受到不法侵害。美國聯邦儲備理事會(Board of Governors of the Federal Reserve System)、聯邦存款保險公司(Federal Deposit Insurance Corporation)、金融管理局(Office of the Comptroller of the Currency) 及儲貸監理局(Office of Thrift Supervision)等金融主管機關，隨即在社會輿論之壓力下，於 1998 年 12 月 7 日提案訂定「知悉客戶規則」(Know Your Customer Rule)[246]，期能落實《美國聯邦法典》12 U.S.C. §1818(s)之執行[247]。

[246] *See* 63 Fed. Reg. 67,536 (proposed Dec. 7, 1998, withdrawn Mar. 23, 1999).

[247] *See* 12 U.S.C. § 1818(s) Compliance with monetary transaction recordkeeping and report requirements. 即要求聯邦金融主管機關必須訂定各金融機構維持一套合理程序的規範，確保其在重要交易記錄上的資訊正確。

觀諸「知悉客戶規則」提案之內容，主要責成金融主管機關應訂定一套規則， 確保存款機構建立及維持符合《銀行秘密法》(*Bank Secrecy Act*)[248]之程序，以嚇阻可能對金融機構之誠信造成重大威脅的違法行為，例如洗錢或金融詐欺行為。此外，金融機構應確認其客戶身分及判定其交易是否正常，並監控是否有不正常及可疑之轉帳行為。申言之，藉由確認其客戶身分及判定其交易是否正常，金融機構可以確保其誠信，並協助金融主管機關及執法機關嚇阻違法行為[249]。本案後來因當時社會輿論龐大壓力而撤回，但隨後通過之《愛國者法》則讓它復活。

美國於 2001 年 9 月 11 日發生 911 恐怖攻擊事件後，群情激憤。因此，美國國會於 2001 年 10 月 26 日閃電通過《愛國者法》(*USA PATRIOT Act*)[250]，期能有效防範恐怖攻擊行動之再度發生。《愛國者法》不僅授權聯邦政府有權追蹤及截取恐怖主義者之通訊，並擴大聯邦調查局及執法機關取得商業紀錄、醫療紀錄、教育紀錄、圖書館紀錄及所儲存之電子資料及通訊。此外，就個人金融資訊之處理而言，《愛國者法》明文要求金融機構執行更嚴格及詳盡之「知悉客戶規則」。相較於金融主管機關先前於 1998 年 12 月 7 日提案訂定「知悉客戶

[248] *See* Bank Secrecy Act, Pub. L. No. 91-508, § 221, 84 Stat. 1122 (1970), codified as amended at 31 U.S.C. § 5313(a) (2006)

[249] *See* Ireland, O. and R. Howell (2004), at 677-678.

[250] "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001", Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001).

規則」，因社會輿論龐大壓力而撤回，《愛國者法》明定金融機構應建立「知悉客戶規則」之要求，並未遭到社會大眾之質疑，其目的在於確認及認證客戶身分，並提供有效方法使政府機關取得該項資料[251]，以防制洗錢活動的相關作為。亦即，金融機構應實施一項符合其商業規模之「客戶確認計畫」(Customer Identification Program)[252]。

「客戶確認計畫」基本上由三個部分組成：(一)客戶身分確認、(二)客戶資料檔案管理，存儲客戶開戶身分證明資料和交易資訊等；和(三)進行客戶背景查核，查核確認客戶不在政府資料庫內恐怖或非法份子的黑名單內。其中，第一項之客戶身分確認和防制身分竊用有最直接之關係。《愛國者法》第 326 條亦增修《銀行秘密法》規定[253]，要求金融主管機關訂定金融機構辦理開戶時應確認客戶身分之最低標準，其內容包括下列幾項：(1)姓名；(2)出生日期；(3)地址。亦即應確認個人之居所及營業場所；如無居所或工作場所，則應確認其郵編地址、其家屬之居所、工作場所或其他連絡方式；如非個人則應確認其主營業所、分支機構地點及其他座落地點；(4)身分證字號、稅籍編號、護照號碼及發行國家、外國人身分證字號或其他由政府發行而足以顯示國籍或居所之文件號碼及發行國家，並附有照片或類似安全

[251] *See* Ireland, O. and R. Howell(2004), at 677-678. 轉引自王志誠(2004)

[252] *See* Financial Recordkeeping and Recording of Currency and Foreign Transactions, 68 Fed. Reg. 25109 (May 9, 2003), codified at 31 C.F.R. pt. 121(b)(1).

[253] *See* 31 U.S.C. § 5318.

措施[254]。

本法要求金融機構必須依法訂立和施行「客戶確認計畫」驗證客戶身分，原為防制洗錢和打擊資助恐怖主義目的，設計藉由「客戶確認計畫」的進行，確認客戶身分，排除已知罪犯和恐怖份子使用金融服務網絡，並減少冒名戶頭的產生，增加罪犯和恐怖主義份子在從事洗錢活動的難度。但也因此，同時有效防制身分竊用事件於金融端發生，對人民有最實際感受和直接影響的個人財務信用安全上的保障產生相當程度的正面助益。而金融機構也樂於告訴客戶，其依《愛國者法》所施行的「客戶確認計畫」係為防制身分竊用目的之用，以獲得客戶之支持與配合。同時，不少專業人士或單位的意見亦抱持相同看法。[255]

第七項　個人資料保護的「合理安全標準」

消費者個人資料保護標準的要求法源，主要來自《聯邦貿易委員會法》 (Federal Trade Commission Act)的 Section 5[256]規範禁止企業以不正當(unfair) 或欺罔(deceptive)之行為或方法從事州際商務。聯邦

[254] *See* Financial Recordkeeping and Recording of Currency and Foreign Transactions, 68 Fed. Reg. 25109 ,May 9, 2003, codified at 31 C.F.R. pt. 121(b)(2)(i)(A).

[255] 作者以" USA PATRIOT Act identity theft"做關鍵字在 Google 搜尋引擎進行搜尋，發現前 30 個結果中，就有 24 個結果是金融機構對外說明《愛國者法》係為防制身分竊用目的。其他 6 個網站亦直言《愛國者法》具協助防制身分竊用功能，(前次檢索日：2012/06/17)

[256] Section 5 of the Federal Trade Commission Act (FTC Act), Ch. 311, §5, 38 Stat. 719, codified at 15 U.S.C. §45(a)

貿易委員會在眾多的案件中靈活運用該原則，成為主要要求企業要進好個人資料保護責任的法源。該委員會在 2012 年 3 月發表的《在快速變遷下保護消費者隱私：對企業及政策制訂者的建言》[257]中表示：聯邦貿易委員會認為公司必須提供消費者保證該公司已遵照合理的安全措施保護其資料安全。聯邦貿易委員會會依照合理的基礎以及其他的考量，含法規等，依照所蒐集資料的敏感度、該公司已施行之資訊保護措施，以及該公司是否已經針對大眾所熟知及容易預防的安全弱點進行相對應防護行動。在該報告中，聯邦貿易委員會實際上解釋了何謂「合理安全標準」(reasonable security standards)，也標定了各業最佳實踐典範(best practices)的標準。聯邦貿易委員會建議公司必須建立隱私權保護架構(Privacy Framework)[258]、並提供合理的安全措施以保護消費者資料。[259]所謂合理的安全標準，包括要遵照聯邦貿易委員會主管的相關聯邦法規以外，還有該公司所要遵守的特定聯邦法和州法，以及所屬業種(industry)，所需遵守的特別法令規範。

以金融機構為例，相關可參照的標準有聯邦金融檢查局[260]的《資訊安全技術檢查手冊》[261]、聯邦儲備銀行發佈的函令有關《打擊假託

[257] "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers", Federal Trade Commission, March 2012, at 21
[258] *Ibid*., at 15
[259] *Ibid*., at 24
[260] Federal Financial Institutions Examination Council (FFIEC)
[261] Information Security IT Examination Handbook (July 2006), available at http://ithandbook.ffiec.gov/it-booklets/information-security.aspx (Last checked on 2012/07/29)

和身分竊用方針》[262]和證券交易委員會[263]的《企業金融揭露基準：網際安全議題二》[264]等。在資訊安全管理標準上，聯邦金融檢查局明言目前並無一個正式可供業界遵守的標準，但是其建議金融機構和主管機關可以參照下列標準來實施或制訂資訊安全管理標準[265]：美國國家標準局(National Institute of Standards and Technology: NIST)頒佈的 NIST 800-33 資訊技術安全基礎技術模型(Underlying Technical Models for Information Technology Security)；國際標準組織(International Organization for Standardization: ISO)頒佈的 ISO/IEC 27000 資訊安全管理體系(Information Security Management System)和 ISO/IEC 15408 資訊技術安全評估準則(Security techniques-Evaluation criteria for IT security)；以及國際電腦稽核協會(Information Systems Audit and Control Association: ISACA)制訂的 CobiT 資訊技術控制目標(Control Objectives for Information Technology: CobiT)。

[262] Letter from Richard Spillenkothen, Dir., Div. of Banking Supervision & Regulation, Bd. of Governors of the Fed. Reserve Sys., SRO1-11: Identity Theft and Pretext Calling (Apr. 26, 2011), available at http://www.federalreserve.gov/boarddocs/srletters/2001/sr0111.htm (guidance on pretexting and identity theft) (Last checked on 2012/07/29)

[263] Securities & Exchange Commission

[264] Securities & Exchange Commission, CF Disclosure Guidance: Topic No. 2, on Cybersecurity (Oct. 13, 2011), available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (Last checked on 2012/07/29)

[265] Information Security IT Examination Handbook, July 2006. at 3

第五節　小結

美國在身分竊用預防和抑止的相關立法環繞於個人資料中重要的財務金融交易記錄、消費者信用記錄報告和健康病歷資料的保護和正確性；個人資料的合法使用和驗證；身分遭冒用後的損害控管和回復；以及身分竊用的偵查和訴追。有關身分竊用定義中的身分證明不只侷限於實體文件，重要的還有身分資訊。而此身分證明則是隨著時代的進步和社會的變化，由實體書面身分證明文件，進步到電子身分證明，一直到現在的各種形式的身分證明資訊。也因此，要保護的身分證明標的物也由實體文件擴大到任何形式的資訊。

在個人資料的保護上，美國是由隱私權出發，限制政府對於人民個人資訊的運用和課以保護責任，然後發展到保護個人的金融和健康資訊隱私。之後，隨著身分竊用問題的被重視，開始針對性的對於常被拿來作主索引的身分證明資訊加以限制運用。

在身分辨識上，美國要求金融機構要在開戶和交易各階段做好客戶的身分確認。也嘗試藉由規範各州政府，建立一套全國性的身分證體系。不過到目前為止，建立身分證體系的進展並不是相當順利。這應是美國聯邦體制和歷史國情所致，另外也是人們對個人資料置於集中資料庫所產生的疑慮，不但不認為其為解決身分竊用問題上提供身分確認的工具方法，甚至是認為其之建立，反而會增加身分竊用受害

機率。重要的論點是：一、不可能有完全安全的資料庫；二、內部濫用資料比資料外洩的機率更高，危害也更大。[266]

美國由其聯邦貿易委員會負責主導全國的身分竊用預防抑制工作，如一、執行提升全民身分竊用危害警覺教育計畫；二、建立協助受害者呈報被害、回復信用和減少受害擴大機制；三、建立身分竊用受害資料庫，供執法機關分析使用，俾能有效訴追身分竊用犯。

最後，在身分竊用的執法訴追上，為了有效的懲治嚇阻身分竊用犯，美國國會立法，清楚將身分竊用入罪化。在一些利用身分竊用為手段的特定的犯罪行為上，則針對其身分竊用行為予以加重處罰，使其成為美國為數不多具罪低刑期的犯罪行為之一。而且藉由讓各級聯邦法院對各罪行量刑有相同基準的《聯邦量刑基準》之規範， 讓身分竊用犯無法逃脫牢獄之罰，以達懲戒和嚇阻之效。

[266] Bruce Schneier, Testimony of, "Will REAL ID Actually Make Us Safer? An Examination of Privacy and Civil Liberties Concerns", U. S. Senate Judiciary Committee, May 8, 2007. Available at http://www.judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862f735da127b2f0&wit_id=e655f9e2809e5476862f735da127b2f0-0-4 (Last checked on 2012/06/22)

(空白頁)

第四章 現行我國對身分竊用問題的處理

我國針對身分竊用問題並無任何專法處理，而是散見於各法律中，而且《刑法》上也沒有身分竊用罪名，亦無將身分竊用列為加重要件之法條。目前身分竊用本身不是一個單獨的罪行，大多是以「冒用他人身分」過程時會產生之「偽造私文書」加以處理。而「冒用他人身分」手段，在現實生活中以偽、變造他人身分證明文件為大宗。在網際網路上，常見的則是被稱為「網路釣魚」(Phishing)的詐騙方法詐取重要個人資料，進而取得被害人的帳號控制權，進行交易，或冒其名，再擴大詐取其社交網路上其他人的個人資料。

第一節 我國個人身分識別制度

第一項 我國戶籍制度與個人身分識別制度的發展

在傳統社會之中，每一個人都是以戶籍身分存在於國家之中，並無現代意義的個人身分存在。這一情形隨著商品經濟的發展、戶籍賦役功能的逐步弱化而開始發生變化。

我國戶籍制度起源很早。中國古代歷代政府用以稽查戶口、徵收賦稅、調派徭役、維護統治秩序的制度。戶籍是登記、管理人戶的冊

籍，亦稱籍帳。春秋時發展為書社制度，25 家為社，「社之戶口書於版圖」，版即戶籍。秦國商鞅變法後，嚴格戶籍管理，又將之與軍事編組相結合。秦統一後，使黔首自實田，遂系田畝於戶籍。漢代定戶律，作為徵收人口稅和分派兵役、力役的依據。戶籍這時是人口、土地、賦役三種冊籍的合一。唐代也是三年一造戶籍，每年做異動登記，戶籍制度趨於完備。 宋代，土地私有制進一步發展，徵收賦稅漸以田畝為主，戶籍遂按有無土地分為主戶、客戶，並按土地多少分別戶等（農村分五等）。同時，設置各種單行的田畝帳冊圖簿，地籍逐漸從戶籍中分離出去。宋以後，金的戶籍登記包括男女老少，較宋為全面。元代則戶類、戶等複雜，戶籍制度頗亂。明初整理戶籍，進行人口普查，頒發戶帖，登記戶種（民戶、匠戶等）、原籍貫、現籍貫、居住地、各口姓名、性別、年齡、與戶主關係等，相當完備。

清初，戶籍散失。順治初，為徵收丁銀，行戶籍人丁編審制度：將戶籍分為軍、民、灶、匠四類，以戶為單位核登丁口，造丁冊，其他人口不備載。康熙五十一年(1712)丁銀全部併入田賦，人丁編審作用消失。乾隆五年(1750)首令歲奏民數，次年規定通過保甲系統統計男女老少全部人口，保甲成為戶籍管理的基礎，一直沿用下來。此時，戶籍已與賦役無關了。[267]

[267] http://www.hudong.com/wiki/中國古代戶籍制度，（前次檢索日： 2012/06/22）

清末民初，中國的門戶被西方列強強行打開之後，傳統社會自己自足的自然經濟遭到徹底破壞。19 世紀後半葉出現了資本主義經濟形態，社會經濟結構的變遷導致傳統戶籍網路的破壞，也使得建立在傳統戶籍基礎上的社會與國家的關係發生了急劇變化。順應這一歷史潮流，晚清政府起草了歷史上第一部戶籍單行法規。這部法規雖然沒有頒佈，但它打破了傳統戶籍理念，解除了封建社會長期束縛在人們身上的戶籍繩索，為民國戶籍法律體系的構建奠定了基礎。1911 年，晚清政府在考察歐美各國之後，認識到「憲政之進行無不以戶籍為依據，而戶籍法編訂又必由民法與習俗而成」，在參考東西各國之良規的基礎上制定了中國歷史上第一部《戶籍法》單行法規。該法規共八章、184 條，其內容可分為戶籍的管理、人籍、戶籍、罰則四個部分。該部法規的主要特點在於：首先，將戶籍吏、戶籍局置於法規的第一章和第二章，突出了戶籍管理機構的地位，反映了政府在觀念上仍視戶籍為管理人口統制的手段，強化戶籍統制功能。其次，法規區分了人籍和戶籍。人籍主要是關於個人出生、死亡、婚姻、繼承、國籍等比較個人化的資訊資料，戶籍則是以家庭為單位，關於移籍、入籍、就籍、除籍等家庭資訊資料。法規將表現歐美個人主義的個人身分證書和體現中國家族主義的傳統戶籍相結合，剔除了傳統戶籍中資產登記專案。戶籍開始成為傳遞人口資訊、個人私權保障的工具，而不再

純粹是國家管制人口的工具。但，《戶籍法》制定後未及頒佈，晚清政府便滅亡了，《戶籍法》隨之擱淺。因此，晚清政府戶籍制度實際上仍沿襲了清中後期的保甲制度的一些做法，將人戶「編牌入甲」。

南京國民政府成立以後，在推行鄉自治的基礎上，參照英、美、德、日等國戶籍及人事登記的法律制度，於 1931 年正式頒佈了中國歷史上第一部《戶籍法》。1934 對該法修正，並于同年施行，1946 年對該法進行了第二次修正，並公佈並施行。該法分通則、籍別登記、身分登記、遷徙登記、變更登記、登記申請、罰則、附則，共八章 61 條。與晚清的《戶籍法》相比，具有把人事登記與戶籍登記合二為一、推行身分證制度、確立了「以戶立戶」的編戶原則等。不過，在實踐中，因國內外局勢動盪，南京國民政府《戶籍法》並未得到很好實施。[268]

中華民國台灣戶籍制度可溯及自日治時代，當時的日本政府為順利統治台灣，便利用戶籍制度蒐集台灣人民的個人資訊，以做為社會控制的工具。直到二次大戰結束，國民政府接收台灣，戶籍制度的地位仍未改變。直到終止戒嚴，恢復戶警分立的正常狀態，戶籍制度的地位才逐漸轉換成國家為遂行社會福利的工具。現行的戶籍制度係依《戶籍法》之規定辦理，主管機關為中華民國內政部，主要分為身分

[268] 窦希铭，《民国初年户籍制度变迁研究——行政立法的社会效应浅析》，法律图书馆 法律论文数据库，2009-3-12，來源：http://www.law-lib.com/lw/lw_view.asp?no=9750，（前次檢索日：2012/07/01）

登記及遷徙登記。舉凡出生、死亡、結婚、離婚等涉及身分變更者，皆屬身分登記之範圍。[269]《戶籍法》是在台灣個人身分證明的來源。除了中華民國國民身分證以外，現行戶籍制度衍生出來的戶籍謄本、戶口名簿是公、私機構經常要求個人提供，以茲核對的有效身分證明文件。

第二項　國民身分證沿革

中華民國國民身分證是《戶籍法》的產物，主管機關為內政部。

1946 年內政部公布《國民身分證實施暨公務員首先領證辦法》，率先由中央及省級公務員於 1946 年 10 月領發國民身分證，民國 36 年開始普發國民身分證，之後經過 1954 年、1965 年、1975 年、1986 年以及 2005 年 12 月 21 日共計 5 次全面換發國民身分證。歷代的身分證無論在格式、註記事項、紙張顏色、男女證分色上均有所不同，身分證之註記欄由全面開放改為正面膠封，到 2005 年則採用膠膜雙面護貝，每一張身分證的變革都象徵著社會的變遷與時代的進步。

第 1 代國民身分證：抗戰勝利後，政府於 1947 年 5 月初次發行身分證。臺灣地區自 1946 年全面清查戶口結束，1947 年 5 月開始依照戶籍法規定製發國民身分證。第 1 代國民身分證採雙頁折疊式，紙

[269] 參考自：http://zh.wikipedia.org/wiki/戶籍，（前次檢索日：2012/07/01）

張為白色，發給對象為 18 歲以上的國民。特別的是，身分證欄位中有項「指紋符號」,「◯」、「∨」記錄每人手指的指紋；類似同心圓的「斗」狀紋路，以「◯」記錄，有如畚箕紋路狀的「箕」狀紋路，則以「∨」記錄。不過，登錄指紋的工作，因戰亂緣故並未確實執行。

1954 年第 1 次全面換發國民身分證。配合整理戶籍，政府於 1954 年 5 月第 1 次全面換發國民身分證，將領證年齡由 18 歲降為 14 歲，並刪除指紋箕斗及公民資格等欄位。

第 2 代國民身分證：係 1954 年換發，仍採雙頁折疊式，紙張為藍色，發給對象為 14 歲的國民，配賦個人「口號」，桃溪(5)口字第 0013 號，刪除指紋符號、公民資格、寄籍、義務勞動，另增加蓋戳記、戶籍記事等欄位。

第 3 代國民身分證：1965 年 4 月至 1966 年 5 月係第 2 次換發國民身分證，將國民身分證格式改為單頁，面積較舊證小 2 分之 1。改採單頁式，男女分色，男為淺綠色、女為淺紅色，正面上加封透明膠套，欄位增加血型、家中排行，共計 14 項欄位。1969 年 7 月起，配合電腦作業，自出生登記即配賦統一編號（即現行的身分證統一編號）。

第 4 代國民身分證：1975 年 10 月至 65 年係第 3 次全面換發國民身分證，1976 年為加強偽造措施，並於正面套印內政部大印，以

示適用於全國。最大變革是廢除「口號」，完全採統一編號，男為淺藍色、女為奶油色，採單面式，證內計有 14 項欄位。

第 5 代國民身分證：1986 年 1 至 12 月係第 4 次全面換發國民身分證，1986 年因改註及人貌改變等因素再次全面換發，該新證特點如下：1、證面縮小便利攜帶；2、欄位精簡，減少出生別、血型、教育程度（因教育程度可透過教育主管機關調查取得，教育程度登記非絕對必要，故於 1997 年修正戶籍法時，刪除該規定，廢止教育程度登記）、戶口校正、備蓋戳記、戶籍記事等 6 欄位；3、擴大封膠面積，以防偽變造，正面封膠，背面除住遷註記、役別、職業欄外均封膠；4、照片加大，以利識別；5、增列出生地，以彌省籍隔閡。第 5 代國民身分證採取正面全封，背面半封，男為土黃色、女為桃紅色，證內計有 11 項欄位。使用期間，廢除本籍登記（為根本解決省籍問題，進一步避免地域偏狹觀念，加強國家認同，於 1992 年 6 月 29 日修正公布戶籍法，刪除有關本籍規定之相關條文，廢止本籍登記，戶籍法第 16 條配合修正為出生地登記）、職業（1997 年修正戶籍法，有鑑於行職業登記與個人權利義務無實質關係，且異動頻繁申報意願低，資料不完整，爰廢止行職業登記）等欄位。

第 6 代國民身分證：自 94 年 12 月 21 日起至 95 年 12 月 31 日止，辦理第 5 次換發。新證格式採取以紙卡製作，全面封膠安全設計，

規格為橫 8.57 公分、直 5.4 公分，大小與一般信用卡、健保卡相同，攜帶更為簡便。男女不分色，均以淺紫、淺咖啡漸層隔色方式呈現，採用橫式印刷，相片透過掃瞄方式製作。第 6 代國民身分證最大的不同，其具有 21 種防偽功能，希望能有效遏阻不法、偽變造國民身分證猖獗的情形。[270]

至此，我國的身分證已具有兩個重要特色：（一）統一的國民身分識別證明文件；（二）個人的專屬身分證號碼。因為身分證的普及運用，此證號也實質上成為全國性單一的個人身分識別號碼。又因為公務和非公務機關絕大部分均使用個人身分證上之基本資料進行建檔索引，所以當面臨到身分證遭到偽冒用時，只要聯絡當地戶政事務所和警察機關，證明是本人身分遭到偽冒用，就可以開始啟動更正的作業。

第二節　身分竊用犯行的刑事法律

我國《刑法》並沒有直接針對身分竊用行為行入罪化，而是利用偽造私文書罪、偽造公印文罪等的方式處理。在《戶籍法》內，也有因應進行身分竊用時偽造、變造國民身分證或使用他人交付或遺失之

[270] 參考整理自「桃園縣大溪鎮戶政事務所」網頁 http://www.tachi-house.gov.tw/file2_08-4-5.php，（前次索引日：2012/07/01）

國民身分證遂行冒用身分的行為訂有刑事處法規定。

因為我國所使用的個人身分識別方式中以利用國民身分證為最主要之方式，而國民身分證之相關授發及管理規定係訂在《戶籍法》內，所以我國在處理人頭帳戶氾濫問題時，由於過去並沒有針對國民身分證借予他人使用所生之損害訂定罰則，而申請補發也只需工本費200 元，導致許多民眾貪圖小利，故意將身分證以數千元賣給不肖份子，再來申請補發。為有效嚇阻不法行為，維護人民權益、公眾利益及國民身分證公信力，嚇阻偽變造及冒用身分證，故在 2008 年 5 月份通過公布增列刑事處罰於《戶籍法》第 75 條。[271]

與身分竊用有關之刑事判決

本研究蒐集分析臺灣臺北地方法院刑事判決中與身分竊用有關之判決，嘗試找出我國法庭實務上，法官處理身分竊用的論罪量刑模式。摘錄與身分竊用有關之刑事判決共 15 例請見下「表 2」。[272]

[271]中華民國 97 年 5 月 9 日於立法院通過，同年 5 月 28 日以總統華總一義字第 09700061901 號令修正公布。新增《戶籍法》第 75 條的立法理由為：「國民身分證為法定個人身分證明文件，人民日常社會生活行使權利及負擔義務不可或缺之重要基本身分證明。偽造、變造及冒用國民身分證者，侵害人民個人權益，甚至有不法人士利用偽（變）造國民身分證，申請護照、簽證或信用卡等牟利，紊亂國家社會秩序，造成國家與人民權益嚴重損害。刑法第二百十二條、二百十六條等，雖有相關處罰規定，惟刑責過輕，難以達到嚇阻犯罪之作用。為有效嚇阻上開不法行為，維護人民權益、公眾利益及國民身分證公信力，爰參考行政院九十七年二月二十五日函送立法院審議之「護照條例」修正案修正條文第二十七條及第二十八條（現行條文第二十三條及第二十四條）規定，增訂本條。」參見立法院資訊網 http://lis.ly.gov.tw/lghtml/lawstat/reason2/0111997050900.htm，（前次索引日 2012/07/01）

[272] 資料來源：作者自行蒐集分析。使用資料庫：司法院法學資料檢索系統-判決查詢；使用全文檢

表 2 「臺灣臺北地方法院刑事判決中與身分竊用有關之判決」

臺灣臺北地方法院刑事判決中與身分竊用有關之判決					
項次	裁判字號/日期	裁判案由	身分竊用有關之犯罪事實	論罪法條	判決
1	93,易,196 93/04/27	違反電腦處理個人資料保護法	未經甲之同意，擅自冒用甲之電子郵件信箱以電腦網路寄發販售廣告傳單暨客戶訂購表單予不特定之多數人，向收信者行使上開偽造之電腦文書，致使該收件者均誤以為上開信件為本人所寄發、販售。	刑法第 216 條（行使偽造變造或登載不實之文書罪）；第 200 條；第 220 條第二項之行使偽造準私文書罪。 （原起訴引電腦處理個人資料保護法第 34 條，當庭更正起訴罪名為行使偽造私文書罪）	連續行使偽造私文書，足以損害於他人，處有期徒刑 6 月。
2	101,審訴,440 101/05/15	偽造文書等	冒用他人身分證至銀行開戶	戶籍法第 75 條(冒用身分證) 刑法第 216 條（行使偽造變造或登載不實之文書罪） 刑法第 212 條（變造特種文書罪） 刑法第 339 條（詐欺取財罪）	共同犯行使偽造私文書罪，累犯，處有期徒刑 6 月
3	101,訴,112 101/04/30	偽造文書	冒用他人身分訂購火車票	刑法第 210 條、第 216 條	犯行使偽造私文書罪，處有期徒刑 3 月，
4	100,訴,869 101/04/27	偽造文書等	使用他人交付之國民身分證，以冒用身分申辦行動電話預付卡門號	刑法第 216 條；戶籍法第 75 條	行使偽造私文書罪，累犯，處有期徒刑陸月。（宣告刑）
5	101,易,181 101/04/27	偽造有價證券等	行使意圖冒用身分使用而變造之國民身分證，行使變造特種文書、意圖供行使之用而偽造有價證券	刑法第 201 條（有價證券之偽造變造與行使罪） 刑法第 212 條（偽造變造特種文書罪） 刑法第 216 條（行使偽造變造或登載不實之文書罪）	偽造有價證券，處有期徒刑 1 年 10 月，緩刑 3 年。
6	100,審訴,372 101/02/23	護照條例等	分別偽造他人(共二人)之國民身分證以冒用身分申辦護照，一次未遂，一次既遂。	刑法第 210 條（偽造變造私文書罪） 刑法第 216 條（行使偽造變造或登載不實之文書罪） 護照條例第 23 條偽造、變造國民身分證以供申	行使偽造私文書，處有期徒刑 8 月，減為有期徒刑 4 月；共同行使偽造私文書，處有期徒刑 1 年，減為有期徒刑 6 月；又偽造署押，處有期徒刑 4 月，減為有期徒刑 2 月。又明知為不實之事項，而使公務員登載於職務上所掌之公

索語詞檢索：「冒用身分」。其中裁判日期格式為中華民國年月日。最近檢索日：2012/07/07。

				請護照及行使。	文書，處有期徒刑 1 年。應執行有期徒刑 1 年 10 月。緩刑 5 年，並應於本判決確定後 6 個月內，向公庫支付新臺幣 20 萬元。
7	99,訴,878 101/02/15	毒品危害防制條例等	為隱匿身分，冒用他人身分，偽造及行使他人國民身分證及汽車駕駛執照，並用以開立銀行帳戶使用。	偽造公印文、偽造國民身分證、偽造特種文書三罪，為想像競合犯，應依刑法第 55 條之規定，應從一重以偽造公印文罪處斷。	偽造公印文罪。累犯，量處有期徒刑 5 月之刑。
8	100,訴,1062 101/02/07	偽造文書等	變造他人（共二人）身分證影本及外國駕照，以冒用身分，申請並使用行動電話門號、美國運通卡、設立公司等，進而進行詐欺取財等其他犯行。	戶籍法第 75 條第一、二項 商業會計法第 75 條第一款 刑法第 210 條、第 212 條、第 216 條、第 220 條第二項、第 339 條第一、三項	多次行使偽造私文書，申請行動電話門號及美國運通簽帳卡部分，分別處有期徒刑 4 月、1 年 1 月及四月。 合併其他行使偽造文書詐欺取財犯行，應執行有期徒刑 6 年。
9	98,訴,1648 98,訴,1859 100/12/30	傷害致死等	被告因前案遭通緝，偽造他人身分證進而冒用他人身分，以逃避查緝。	刑法第 218 條（偽造盜用公印或公印文罪）、第 216 條（行使偽造變造或登載不實之文書罪）、刑法第 212 條（偽造變造特種文書罪）； 戶籍法第 75 條	共同偽造公印文，足以生損害於公眾及他人，累犯，處有期徒刑 5 月。
10	100,簡,4370 100/12/15	偽造文書	酒駕被警攔檢，冒用他人（其兄廖○○）名義由員警進行酒測及其後受偵訊等。	刑法 217 條第 1 項之偽造署押罪、 刑法第 216 條（行使偽造變造或登載不實之文書罪）、第 210 條（偽造變造私文書罪）	行使偽造私文書，足以生損害於公眾及他人，處有期徒刑 3 月 本案被告雖有持用廖○○國民身分證以冒名使用，惟並無證據證明被告取得廖○○國民身分證之原因係廖○○交付被告、或被告拾得廖○○所遺失之國民身分證，與戶籍法第 75 條第 3 項後段「冒用身分而使用他人交付或遺失之國民身分證」之要件不符，就此部分尚不構成本條項之罪，附此敘明。
11	100,簡,777 100/05/06	偽造文書	大陸人士偽冒他人身分（不確定是否為真人之大陸地區人民），使用偽造之大陸身分證件，申請入境來台許可，自大陸地區來台賣淫。	刑法第 216 條（行使偽造變造或登載不實之文書罪）、第 210 條（偽造變造私文書罪）	行使偽造私文書，處有期徒刑 5 月
12	100,金訴緝,9 100/11/30	銀行法等	擔任詐欺集團之開戶車手，持偽冒之多名他人身分證件，冒用身分開設銀行帳戶後，供詐欺集團使用。	刑法第 216 條（行使偽造變造或登載不實之文書罪）、第 210 條（偽造變造私文書罪）；戶籍法第 75 條(冒用身	共同行使偽造私文書，處有期徒刑 3 月

				分證)	
13	100,審訴,172 100/11/25	違反戶籍法等	使用竊得之他人國民身分證，冒用他人身分、偽造文書而販賣物品	刑法第 216 條（行使偽造變造或登載不實之文書罪）、第 210 條（偽造變造私文書罪）; 戶籍法第 75 條(冒用身分證)	共同犯行使偽造私文書罪，處有期徒刑 2 月。 身分被冒用人陳○○國民身分證既係因竊盜而喪失持有，即非屬遺失之國民身分證。是被告 2 人冒用陳○○身分而使用竊得之陳○○國民身分證之行為，即不構成戶籍法第 75 條之犯罪。
14	95,訴,1801 980610	電信法等	連續冒名辦理行動電話易付卡門號。	刑法第 216 條（行使偽造變造或登載不實之文書罪）、第 210 條（偽造變造私文書罪）	共同行使偽造私文書罪，共 16 罪，各罪處宣告刑 3 月。甲應執行有期徒刑 6 月；乙應執行有期徒刑 4 月。
15	100,訴,1073 100,訴,1101 100,訴,1127 100/11/21	違反戶籍法等	偽造他人之國民身分證、汽車駕駛執照、全民健康保險卡。用他人名義向汽車出租業者以假租車之方式詐取車輛後，持以典當或變賣以獲取現金。	刑法第 216 條（行使偽造變造或登載不實之文書罪）、第 210 條（偽造變造私文書罪）; 戶籍法第 75 條(冒用身分證)	兩個共同行使偽造私文書犯罪行為，累犯，分處有期徒刑 8 月及有期徒刑 10 月。

綜合分析發現，實務上對於身分竊用的刑事責任問題基本上的處理方式分為兩種：

第一項　偽造、變造他人之身分證件

使用偽造、變造國民身分證者

《戶籍法》第 75 條（偽造變造國民身分證之處罰）：意圖供冒用身分使用，而偽造、變造國民身分證，足以生損害於公眾或他人者，處 5 年以下有期徒刑、拘役或科或併科新臺幣 50 萬元以下罰金。行使前項偽造、變造之國民身分證者，亦同。將國民身分證交付他人，

以供冒名使用，或冒用身分而使用他人交付或遺失之國民身分證，足以生損害於公眾或他人者，處 3 年以下有期徒刑、拘役或科或併科新臺幣 30 萬元以下罰金。

實務上在操作《戶籍法》第 75 條時，其構成要件的要求是行為人或得他人之身分證必須具冒用其身分之意圖，單純之偽造、變造國民身分罪尚不觸犯此條。又，本條第三項之構成要件係國民身分證本人交付或使用他人交付或遺失之國民身分證，以行冒用身分行為。故若係「竊取」他人國民身分證，再行冒名使用，因為此非屬他人「遺失」，故其冒用身分證行為，不構成《戶籍法》第 75 條之犯罪。[273]

偽造、變造其他身分證件者

《刑法》第 212 條（偽造、變造特種文書罪）：偽造、變造護照、旅券、免許證、特許證及關於品行、能力服務或其他相類之證書、介紹書，足以生損害於公眾或他人者，處 1 年以下有期徒刑、拘役或 3 百元以下罰金。《刑法》第 210 條（偽造變造私文書罪）偽造、變造私文書，足以生損害於公眾或他人者，處五年以下有期徒刑。

若偽造國民身分證、汽車駕駛執照等公文書特種身分證明文件時有同時偽造公印文時，實務上的論罪如下：「按國民身分證、汽車駕

[273] 參考：臺灣臺北地方法院刑事判決：100 年度審訴字第 172 號

駛執照均屬《刑法》第 212 條之特種文書。又偽造公印文，《刑法》第 218 條第 1 項既有獨立處罰之規定，且較《刑法》第 212 條之處罰為重，則於偽造《刑法》第 212 條之特種文書同時偽造公印文者，即難置《刑法》第 218 條處刑較重之罪於不問，司法院大法官解釋釋字第 82 號解釋參照。又《戶籍法》第 75 條於 95 年 5 月 28 日修正公佈，第 1、2 項規定「意圖供冒用身分使用，而偽造、變造國民身分證，足以生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科新臺幣五十萬元以下罰金。行使前項偽造、變造之國民身分證亦同。」，《戶籍法》第 75 條係針對國民身分證之偽造、變造犯行予以明文規定，相較於《刑法》第 212 條係針對所有一般特種文書之偽造、變造行為之處罰規定，《戶籍法》之規定應屬於特別規定，依特別法優於普通法及從重處斷之原則，應優先適用《戶籍法》之規定。惟《刑法》第 218 條第 1 項之偽造公印文罪，並未修正，且與《戶籍法》第 75 條第 1 項之構成要件不同，自難謂《戶籍法》第 75 條第 1 項係《刑法》第 218 條第 1 項之特別法，況偽造國民身分證，並不當然需要偽造國民身分證上之公印文，是偽造國民身分證，自不能當然包括偽造公印文在內；而偽造公印或公印文，《刑法》第 218 條既有獨立處罰規定，且較《戶籍法》第 75 條第 1 項規定之處罰為重，則於偽造國民身分證同時偽造公印或公印文者，即難僅論以《戶籍法》第 75 條

第 2 項、第 1 項之罪，而置《刑法》第 218 條第 1 項處刑較重之罪於不問（最高法院 97 年度台上字第 5114 號判決參照）。是《戶籍法》之上揭規定與《刑法》第 218 條規定為想像競合關係，依《刑法》第 35 條第 2 項主刑輕重標準之比較規定,《刑法》第 218 條較《戶籍法》第 75 條為重，應從較重之《刑法》第 218 條之偽造公印文罪論處。」

第二項　僅利用他人身分資料

此類型的犯罪手法，常見應用於在網際網路上。如被稱為「網路釣魚」(Phishing)的詐騙方法詐取重要個人資料，進而取得被害人的帳號控制權，進行交易，或冒其名，再擴大詐取其社交網路上其他人的個人資料或作其他運用。另一種則是利用網頁設計的身分證檢測漏洞，輸入可通過程式檢核的身分證字號，行為人通常不知道其輸入冒用之身分證字號真實的擁有者為何人。此種方法之所以容易進行是因為我國身分證號碼的檢索碼驗證公式是公開的，網路上隨處均可獲得所謂的「身分證號產生器」。

我國刑法處理此類型之犯行係以偽造文書罪論之。《刑法》第 210 條的偽造變造私文書罪：「偽造、變造私文書，足以生損害於公眾或他人，處五年以下有期徒刑。」本罪的行為有二個，一個是偽造私文書，另外一個是變造私文書，且要足以生損害於公眾或他人，始可能

構成本罪。本罪之成立要件為：

1. 偽造私文書：偽造私文書是指沒有製作權的人，製作虛偽的私文書。所謂「虛偽的私文書」是指非出於私文書上所示的作成名義人的文書，也就是說對外足以詐騙別人，使別人認為此虛偽的文書，是與作成名義人具有同一性的文書。
2. 變造私文書：是指無權修改私文書內容之人，擅自更改真實文書的內容，故原本變造行為的客體必須是真實的私文書。真實私文書的內容精行為人竄改後，其證明資格和文書品質，並沒有因此而完全消失，始屬變造。如果已經完全消失的話，則屬偽造。
3. 變造或偽造私文書的結果，必須足以生損害於公眾或他人者，才可能成立本罪。足以生損害並不以實際上真的發生損害為必要，只要有足生損害之可能，即可。
4. 行為人主觀上必須具備偽造或變造私文書的故意。

而在電腦上輸入處理的資料，因為《刑法》第 220 條：「在紙上或物品上之文字、符號、圖畫、照像，依習慣或特約，足以為表示其用意之證明者，關於本章及本章以外各罪，以文書論。錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，亦同。稱電磁紀錄，指以電子、磁性或其他無法以人之知覺直接認識之方式所製成之紀錄，而供電腦處理之用者。」

故亦屬《刑法》偽造文書罪定義的一種文書，所以其論罪方式與實體文書無異。

第三節　個人資料保護法律

第一項　1995 年《電腦處理個人資料保護法》[274]

1990 年 9 月間，行政院鑑於政府機關與民間企業開始大量使用電腦儲存、處理所蒐集的個人資料，並廣泛予以利用，其流通與運用得當者，對於交易安全保障、整體經濟發展、社會秩序維護與學術研究均有助益；然如有誤用或濫用情事，勢必嚴重侵害個人隱私權益，爰指示法務部研擬相關法律，作為利用個人資料與保護隱私權益的基本規範。是時我國正積極推動加入國際貿易組織(World Trade Organization: WTO)，而歐盟各國一向對個人資料之保護十分重視，為避免在加入WTO組織協商過程中，被指摘我國對個人資料保護不力，法務部乃擬定立法計畫積極進行研擬法案工作。經先後邀請學者專家與機關團體，舉行數十次研商會議後，法務部於 1992 年 6 月間研擬完成《電腦處理個人資料保護法草案」，報請行政院審查後函請立法

[274] 參考自劉佐國，「我國個人資料隱私權益之保護—論『電腦處理個人資料保護法』之立法與修法過程」，律師雜誌，第 307 期，，2004 年一月，42-51 頁。

院審議，於 1995 年 7 月完成三讀立法程序，並經　總統於同年 8 月 11 日公布施行，在我國法制史上有關保護個人資料隱私權益方面，建立一重要之里程碑。

1995 年公布施行之《電腦處理個人資料保護法》（以下簡稱本法）係參照經濟合作開發組織(Organisation for Economic Co-operation and Development: OECD)所揭示的保護個人資料八大原則（即限制蒐集原則、資訊內容完整正確原則、目的明確化原則、限制利用原則、安全維護原則、公開原則、個人參加原則與責任原則）所制訂，其立法目的在於避免人格權受侵害及促進資料之合理利用。由於本法嚴格規範有關個人資料之蒐集、處理及利用行為，為避免對民間衝擊過大，並考量執法之效能與社會各界接受之程度，爰參酌當時日本之《行政機關計算機處理個人資料保護法》（*行政機関の保有する個人情報の保護に関する法律*）與英國之《資料保護法》(*Data Protection Act*)立法例，僅將經電腦處理之個人資料納入保護範疇，至於一般未經電腦處理或儲存之資料（亦即人工資料）則不適用本法予以保護。另考量個人資料蒐集之數量與利用情形，除公務機關外，僅限制大量蒐集個人資料作成個人資料檔案，以供利用之徵信業及以蒐集或電腦處理個人資料為主要業務之團體或個人(例如「財團法人金融聯合徵信中心」)、醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業等八類

事業，為適用本法之非公務機關。另為怕掛一漏萬，爰授權法務部會同中央目的事業主管機關指定特定之事業、團體或個人亦得適用本法。迄今，業經指定適用者計有：期貨業、台北市產物人壽保險商業同業公會、中華民國產物保險商業同業公會、中華民國人壽保險商業同業公會、財團法人台灣更生保護會、財團法人犯罪被害人保護協會、不動產仲介經紀業、利用電腦網路開放個人資料登錄之就業服務業（人力銀行）、百貨公司業及零售式量販業、除語文類科外之文理類補習班、無店面零售業、錄影節目帶出租業、運動場館業等十三個事業或團體。非屬上開法定之八類事業或經指定適用本法者，則均不受本法規範。

因為《電腦處理個人資料保護法》適用行業限制較知名的案例為：國內知名的「博客來網路書店」網站，2007 年發生民眾購買金馬影展套票，回覆會員註冊成功的電子郵件，夾帶其餘 477 位註冊成功之會員資料含會員帳號、姓名、地址、電話、手機、電子信箱資料，外流到其他數百人之信箱之中。曾某等十七位受害人，為此提起損害賠償訴訟，要求博客來依個資法及侵害隱私權，賠償各人九至十萬元。台北地方法院 2008 年 11 月 18 日 97 年度訴字第 1683 號判決博客來必須賠償每人二千四百元至一萬一千九百元不等。法官審理認為，本案確實是因為被告人員業務處理疏失，才將原告曾某等十七人的姓名

等個人資料，無端附加在購票確認系統回覆電郵，公開揭示和購票目的無關的第三人，自屬侵害隱私權，原告主張受有非財產上的損害有理由。至於違反個資法部分，法官認定博客來網站不是《電腦處理個人資料保護法》規定的非公務機關，原告不能依該法求償。

另外，對於違反本法規定，侵害個人資料隱私權益之行為人，僅限意圖營利者始有刑事責任。違法蒐集、處理或利用個人資料，對個人權益的侵害不可謂不大，但依《電腦處理個人資料保護法》第 33 條規定，需具有意圖營利的主觀構成要件，始能科處刑事責任。以臺灣臺北地方法院為例，摘錄違反《電腦處理個人資料保護法》之刑事有罪判決 5 例供參，如「表 3」[275]。如未有營利的意思或意圖，即使故意洩漏了大筆個人資料，亦無法追究其刑責[276]，如其亦非為蒐集機關之負責人，則無法課以行政責任（罰鍰），而民事損害賠償責任，本法則規定應由蒐集機關本身負責。因此，如有不肖員工違法洩漏個人資料，只要聲稱未有營利之意圖，又無具體事證可資證明其有獲利之事實，幾乎無法可罰而殊有不公，對於惡意的資料外洩者，亦缺乏儆戒的效果。[277]

[275] 資料來源：作者自行蒐集分析。使用資料庫：司法院法學資料檢索系統-判決查詢；案由檢索字詞：「個人資料保護」。資料庫回傳查詢結果僅 13 筆，經檢視內容，其中 5 筆與違反《電腦處理個人資料保護法》有關。裁判日期格式為中華民國年月日。最近檢索日：2012/07/09。

[276] 實務上曾查獲某中學老師長期將學生個人資料提供給經營補習班之友人，由於該老師堅稱未收受報酬，又無其他意圖營利之具體事證，致無法追究渠本法規定之刑事責任。轉註自劉佐國(2004)。

[277] 同前註。

《電腦處理個人資料保護法》刑事判決-以臺灣臺北地方法院為例

表 3「臺灣臺北地方法院刑事判決-違反《電腦處理個人資料保護法》」

臺灣臺北地方法院刑事判決			
項次	裁判字號/日期	裁判案由	違反電腦處理個人資料保護法部分之判決
1	93,易,1755 94/06/28	意圖營利，非公務機關對個人資料為蒐集及電腦處理，致生損害於他人。	累犯。 被告前因違法蒐集並販售個人資料，經法院以背信罪判處罪刑確定並甫於93年4月13日易科罰金執行完畢，被告竟於該案執行完畢後，旋觸犯本件犯行，足見其未因前受科刑、執行而記取教訓，毫無悔意，及被告犯罪之動機、目的、手段、所生危害等一切情狀，處有期徒刑8月。
2	95,易緝,7 95/03/08	同上	處有期徒刑3月。緩刑2年。
3	95,簡,620 95/06/30	同上	處有期徒刑4月。緩刑2年。
4	94,易,2121 95/08/18	同上	處有期徒刑3月。
5	99,訴,47 100/10/27	同上	累犯，同手法共三罪，各罪處有期徒刑3月。應執行有期徒刑7月。

《電腦處理個人資料保護法》訴訟原告勝訴案

在《電腦處理個人資料保護法》時代發生之個人資料外洩事件，以本法作為請求權基礎之訴訟案，自 2004 年至今約僅有兩百多件，而原告勝訴可據以參酌賠償金額之案件 7 年來約僅有 9 件，詳參「表 4」。[278]

[278] 達文西個資暨高科技法律事務所彙整。葉奇鑫、李相臣(2012)。頁 44。原文中有將臺灣臺北地方法院 97 年度訴字第 1683 號民事判決，即「博客來網路書店」網站個人資料外洩案列入。惟經作者查詢原判

表 4 「《電腦處理個人資料保護法》原告勝訴賠償金額之案件」

《電腦處理個人資料保護法》原告勝訴賠償金額之案件				
裁判案號	被告行業別	請求權基礎	事實摘要	賠償金額
臺灣高等法院 98 年度上易字第 1229 號民事判決	銀行	電腦處理個人資料保護法第 18 條、第 28 條、民法第 184 條第 1 項前段、第 188 條第 1 項、第 195 條。	原告未曾向被告申請信用卡，然被告於民國 97 年間誤向聯合徵信中心申報原告持用之信用卡遭強制停卡致原告之名譽、信用受有損害。	25 萬元
臺灣板橋地方法院 99 年度重勞訴字第 10 號民事判決	證券商離職員工	民法第 153 條、第 199 條、第 184 條第 1 項前段、營業秘密第 12 條第 1 項前段。	被告藉職務上之機會，取得原告未授權被告查閱之客戶資料後離職。	21 萬 4,500 元
臺灣臺南地方法院 94 年度訴字第 121 號民事判決	個人、電信業者及其員工	電腦處理個人資料保護法第 28 條、民法第 184 條第 1 項前段、第 188 條第 1 項、第 195 條。	被告甲為利用職務之便，受被告乙之請託擅自進入電腦系統查詢電話使用人即原告之姓名、住址相關資料，並告知被告乙藉以確定原告之身分。	個人：15 萬元 電信業者及其員工：8 萬元
臺灣臺中地方法院 94 年度重訴字第 196 號民事判決	銀行及其員工	電腦處理個人資料保護法第 6 條及第 18 條、第 28 條及民法第 188 條之規定。	被告甲利用任職被告公司業務之機會，取得原告申辦現金卡之個人資料，進而利用此一資料，冒用原告名義，辦理變更住址及掛失補發現金卡。	10 萬元
臺灣臺北地方法院 93 年度訴字第 2455 號民事判決	徵信業者、資訊業者	電腦處理個人資料保護法第 27、28 條規定。	被告乙違法蒐集原告之個人資料，又與被告甲共同意圖營利，提供被告甲之付費會員，得透過網路超連結方式，以每筆資料 200 元之價格付費查詢。	徵信業者：10 萬元 資訊業者：10 萬元
臺灣基隆地方法院 93 年庭訴字第 82 號民事判決	證券商	電腦處理個人資料保護法第 27、28 條規定。	未經原告同意蒐集其姓名、地址等資料並發送廣告信函。	3 萬元
臺灣宜蘭地方法院羅東簡易庭 99 年度羅小字第 56 號民事小額判決	網購賣家	民法第 184 條第 1 項前段、第 195 條。	原告於網拍上購買被告商品，被告於評價留言公開原告家中之系爭家用電話號碼，使原告之家用電話號碼遭第三者知悉。	2 萬元
臺灣臺北地方法院簡易庭 99 年度北國簡字第 16 號民事判決	公務機關	國家賠償法第 5 條、民法第 195 條。	被告將原告之個人資料公布於薪給發放標準之陳情函並予以張貼。	5,000 元

由此 8 件案例分析，被告之行業別因現行《個人資料保護法》之限制，不脫離現行法下規範之八大行業，分別為：銀行（2 件，1 件含員工）、證券商（2 件、1 件含離職員工）、電信業者（及其員工）、

決書發現，法官審理認為，本案確實是因為被告人員業務處理疏失，才將原告曾某等十七人的姓名等個人資料，無端附加在購票確認系統回覆電郵，公開揭示和購票目的無關的第三人，自屬侵害隱私權，原告主張受有非財產上的損害有理由，依民法第 184 條第 1 項前段及第 195 條，判被告賠償原告等共 13 萬 7,900 元。至於違反個資法部分，法官認定博客來網站不是《電腦處理個人資料保護法》規定的非公務機關，原告不能依該法求償。故作者將該判決自本表中刪除。

徵信業及資訊業者、網購賣家及公務機關。大部分案例引用現行個人資料保護法第 18 條或第 28 條作為請求權基礎，此兩條文在新法依然存在，僅有賠償額度自每人每事件 2 萬元以上 10 萬元以下，修正為 500 元以上 2 萬元以下；而同一原因事實合計最高賠償額，則由 2,000 萬元提高至 2 億元，如該原因事實所涉利益超過 2 億元，以該所涉利益為限，是如當事人能證明超過外洩者獲有超過 2 億元之利益時，其賠償額將會更高。

實際判賠之金額部分，唯一一件公務機關為被告之案件（臺灣臺北地方法院 99 年度北國簡字第 16 號判決）遭判賠 5,000 元，與現行個人資料保護法規定下限 2 萬元不符。由該判決析之，似與原告並未主張法院應適用現行個人資料保護法第 27 條規定作為損害賠償額度審酌之標準有關，並非係參酌新個人資料保護法規定降低賠償額度，始作為賠償額度僅有 5,000 元之決定因素。其他 8 件賠償案例，賠償金額均自 2 萬元起跳，除有 2 萬元、3 萬元及 8 萬元案件各一件以外，有三位被告被判應賠償 10 萬元，超過 10 萬元則有 13 萬 7,900 元、15 萬元、21 萬 4,500 元及 25 萬元者。

新《個人資料保護法》有關民事損害賠償規定之構成要件，規定於第 28 條（針對公務機關）：及第 29 條（針對非公務機關）：「違反本法規定致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利」

者。條文規定較舊《電腦處理個人資料保護法》更為詳盡，當事人得據此加以求償之範圍，不僅僅止於個人資料被洩漏情形，舉凡違法蒐集、應告知當事人而未告知、應通知而未通知、逾期保存或利用個人資料、當事人請求更正或刪除卻未為之等等，均可能符合求償之構成要件。而其他各種違反個人資料保護法要件的情狀，如個人資料外洩、應通知未通知、逾期保存資料等侵害權利之行為，當事人勢將難以證明其實際損害額之多寡，如此皆可適用新個人資料保護法第 28 條第 3 項規定，由法院以自由心證方式，酌定賠償金額。此時審判者究應如何衡量其損賠金額之高低？判斷標準為何？勢必將成為攻防焦點與審判爭議。[279]

影響層面極廣的新《個人資料保護法》，幾乎涉及所有的企業、團體，以及個人，然而在立法過程中，由於欠缺充分討論，立委又各自提出不同版本，以致通過條文完全脫離行政院版本，發生窒礙難行的情形，業界為此也抱怨連連，認為不宜貿然實施，以避免對社會造成衝擊。縱觀個資法條文，也確實有若干內容不合時宜之處，諸如 2010 年主要是參考歐盟 1995 年的指令，相關規範已過於陳舊，歐盟執行委員會已考慮全面檢討修正，我國似也應納入參考。又第 6 條對

[279] 葉奇鑫、李相臣，「淺談個人資料保護法民事賠償責任及數位鑑識相關問題」，《司法新聲》，第 101 期，2012 年一月。頁 45。資料來源：ja.lawbank.com.tw/pdf/司法新聲 101 期_第 3 篇.pdf，（前次檢索日： 2012/06/22）

於敏感性個人資料，包括醫療、基因、性生活、健康檢查及犯罪前科等個人資料蒐集、處理或利用之限制過於嚴苛，完全違背現況；第54 條對於間接蒐集個人資料，必須在一年內告知才能處理或利用，執行上確有困難。另新法刑責過重，違反個資法動輒面臨刑事責任，這些問題確實有檢討修正的必要。[280]

第二項　2010 年《個人資料保護法》

我國對於個人資料之保護規範，始於 1995 年頒布之《電腦處理個人資料保護法》，後於 2010 年 4 月 27 日經立法院三讀修正通過，並於同年 5 月 26 日經總統公布之新《個人資料保護法》，為該法第一次且大幅度修法。本次修正之主要內容為：

一、擴大法律適用範圍：公務和所有非公務機關，包括自然人、法人或其他團體，不分行業，均納入個人資料保護法適用對象。任何有關個人資料之蒐集、處理、利用及相關之檔案安全維護措施，皆須符合新法之規定，並同時取消原先需事前取得執照與登記等規定。

二、擴大個人資料之範圍：將護照號碼、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式及其他得以直接或間接方式識別個人

[280] 何展旭，「個人資料保護法施行不宜再拖」，國家政策研究基金會，2012/07/05。來源：http://www.npf.org.tw/post/1/10994 ，（前次索引日 2012/07/08）

資料，均納入個人資料之範圍。

三、增加特種個人資料定義：除符合法律規定外，任何人不得蒐集、處理或利用醫療、基因、性生活、健康檢查、犯罪前科等個人資料。[281]縱依法可蒐集、處理或利用上開個人資料，亦應遵守中央目的事業主管機關及法務部所訂定資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法。

四、增訂非由當事人提供個人資料之處理方式：公務機關及非公務機關向當事人蒐集個人資料時，應告知其名稱、蒐集之目的、個人資料之類別、利用個人資料之期間、區域、對象及方式、當事人得行使之權利及方式，及不提供資料對其權益之影響。[282]於非由當事人提供個人資料之情形，公務機關及非公務機關於處理或利用個人資料前，除前述告知事項外，原則上應告知當事人資料來源。[283]就使用個人資料，原則上應經當事人同意，但若使用個人資料與公共利益有關，或個人資料取自於一般可得來源，且使用該資料有比保護個人資料更重大利益，則不在此限。此例外規定係為保障新聞自由所定。

五、明訂安全維護責任：公務機關保有個人資料檔案者，應指定

[281]《個人資料保護法》第 6 條

[282]《個人資料保護法》第 8 條

[283]《個人資料保護法》第 9 條

專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏[284]。非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏[285]。

六、提高民事賠償責任金額：如有不法蒐集、處理、利用或其他侵害當事人權益之情形，縱當事人不能證明其實際損害額時，當事人仍得請求法院依侵害情節，以每人每事件新台幣五百元以上二萬元以下計算，請求損害賠償。對於同一原因事實造成多數當事人權利受侵害之事件，合計最高損害賠償總額為新台幣二億元；但所涉利益超過新台幣二億元時，則以所涉利益為最高損害賠償額，且每人每事件之最低賠償額則不受最低新台幣五百元之限制。其名譽被侵害者，並得請求為回復名譽之適當處分。[286]

七、增加公益團體代表訴訟：當事人行使權利，得授與訴訟實施權予財團法人或公益社團法人，由該等法人向違反個人資料保護法者，提起訴訟，請求損害賠償。

八、提高刑事責任：違法蒐集、處理或利用有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料；公務及非公務機關對個人資料

[284] 《個人資料保護法》第 18 條。

[285] 《個人資料保護法》第 27 條第 1 項。

[286] 《個人資料保護法》第 28、29 條

之蒐集或處理無特定目的或對個人資料之利用與蒐集之特定目的不相符;或違反中央目的事業主管機關限制國際傳輸之命令或處分，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。[287]意圖營利犯前項之罪者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。[288]意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。[289]公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。[290]

九、增加非告訴乃論部分:意圖營利犯罪者或非法妨害公務機關個人資料檔案之正確者，為非告訴乃論。[291]

新舊個人資料保護法內容比較

新舊個人資料保護法內容比較請參見「表 5」[292] 。

---

[287]《個人資料保護法》第 41 條第 1 項

[288]《個人資料保護法》第 41 條第 2 項

[289]《個人資料保護法》第 42 條

[290]《個人資料保護法》第 44 條

[291]《個人資料保護法》第 45 條

[292] 參考自:「機不可失—保護企業資料 為新版個資法作好準備」,台灣微軟,2010 年 5 月。頁 4。以及顧振豪,「業者因應新修個資法之調整」,資訊工業策進會科技法律中心,簡報檔,2010 年 5 月。頁 23。資料來源:http://download.microsoft.com/download/5/4/C/54CC1721-F3F6-4F79-8221-52428FB27669/PrivacyIs

表 5 「新舊個人資料保護法內容比較」

新舊個人資料保護法內容比較		
	舊版 《電腦處理個人資料保護法》	新版 《個人資料保護法》
適用行業	政府機構、徵信、醫院、學校、電信、金融業、證券、保險及大眾傳播及經法務部會同中央目的事業主管機關指定適用本法之特定事業、團體，	全體適用。
個人資料定義	以電腦處理之個資為限 僅包括足資識別個人之資料	不以電腦處理個資為限 包括直接、間接識別個人之資料
新增特種資料	無	除符合法定要件外，原則上不得蒐集、處理或利用關於個人的醫療、基因、性生活、健康檢查及犯罪前科....等 5 項資料。
行為規範	蒐集、電腦處理、利用的行為(含國際傳遞) 。	應明確告知當事人蒐集者名稱、目的、資料類別、利用方式...等相關事項。 如需以超出原目的之方式使用個人資料，應另外單獨徵求當事人書面同意，不得以概括方式處理。 公務機關可主動或依當事人請求，停止資料相關處理單位的違反行為。 該資料若用於產品行銷，應於首次使用時免費提供客戶表示拒絕的方式。 若發生個人資料外洩事件，應主動即時告知當事人。
行政監督	中央目的事業主管機關	相關主管機關若認為有必要，或發現非公務機關違反事項時，得派員依法檢查，並採取必要處分。
其他公務機關行為規範調整	特定目的外利用必須符合法定要件 保有個人資料需公告法定事項於政府公報或其他適當方式	特定目的外利用刪除「有正當理由且僅供內部使用」 修訂學術研究必要範圍與限制利用方式(以無從識別當事人為原則) 公告方式改為公開於電腦網站或其他適當方式
其他非公務機關行為規範調整	特定目的外利用必須符合法定要件 行政檢查配合義務	學術研究機構於公共利益下利用個資為統計或學術研究以無從揭露當事人之方式為原則 對於行政檢查之要求、強制扣留等行為得聲明異議需採取適當安全措施 配合裝樣目的事業主管機關之指定訂定個資檔案維護計畫等事宜
損害賠償	同一事實上限新臺幣 2,000 萬。 無團體訴訟規定。	同一事實上限新臺幣二億，若不法獲利超過該上限者，以不法獲利金額為限。 財團法人或公益社團法人若符合規定者，得代受害當事人提起團體訴訟。 二十人以上之團體訴訟，且其訴訟標的價額超過新臺幣 60 萬元者，超過部分免徵裁判費。
罰責	2 年以下有期徒刑，得併科新臺幣 20 萬元以下之罰金。	行政罰之罰鍰，依據事實可罰 2 萬～50 萬元以下之罰鍰 非公務機關之代表人、管理人或其他有代表權人，除能證明已盡防止義務，應並受同一罰鍰處罰。 加重「意圖營利」者的處罰。刑責提高為 5 年以下有期徒刑及新臺幣 100 萬元以下罰金。且提升為非告訴乃論罪。

sue_0520.pdf 及 http://www.cnra.org.tw/cnraDoc/2010-6-7-16-09-15-990525 無店面零售業因應新修個資法.pdf ，(前次檢索日： 2012/06/22)

第四節　金融機構配合規定

為研究整理方便，作者將本節所提各法規分為三部分，分別為「警示聯防，阻絕不法使用」、「認證身分，減少偽冒開戶」目的相關規定，和「金融聯合徵信中心」

第一項　「警示聯防，阻絕不法使用」相關規定

2005 年增修《銀行法》第四十五條之二

我國於 2003 年間因為新興詐騙問題嚴重，冒用他人身分至金融機構開立帳戶或是自願提供帳戶供他人使用的人頭戶的情況氾濫，為維護各銀行經管財務之安全，提高金融從業人員之警覺，減低銀行營運上之風險，並為貫徹政府打擊詐欺犯罪及國際間反洗錢與反恐政策，政府於 2003 年 4 月 8 日召開「行政院強化社會治安第十八次專案會議」進行討論，並於 2005 年 4 月依據結論增修《銀行法》第四十五條之二，增訂銀行安全維護相關行政命令之法律授權依據。即增訂第二項「銀行對存款帳戶應負善良管理人責任。對疑似不法或顯屬異常交易之存款帳戶，得予暫停存入或提領、匯出款項。」及第三項「前項疑似不法或顯屬異常交易帳戶之認定標準，及暫停帳戶作業程序及辦法，由主管機關定之。」之後並衍生出一系列與打擊詐騙和偽冒身

分開戶的法規命令。

由系列法規及作為觀之，其主要的兩個目標手段是：一、警示聯防，阻絕不法使用：定義「警示帳戶」和「衍生管制帳戶」並規定相關的處理辦法，防止此等帳戶遭到歹徒繼續利用；以及二、認證身分，減少偽冒開戶：加強要求金融機構採取更嚴謹的開戶身分查驗認證工作，以預防及嚇阻偽冒身分開戶的情事。

2005 年《一人持有多個金融機構存款帳戶，其中一帳戶經通報為警示帳戶，其餘帳戶之通報及控管作業程序》

在作業面上，「行政院金融監督管理委員會」（以下簡稱「金管會」）於 2005 年 8 月 16 日以金管銀（一） 字第 0948011044 號函准予備查，「中華民國銀行公會」（以下簡稱「銀行公會」）訂立之《一人持有多個金融機構存款帳戶，其中一帳戶經通報為警示帳戶，其餘帳戶之通報及控管作業程序》要求會員金融機構於接獲警調機關通報警示帳戶後，即終止該帳號使用提款卡、語音轉帳、網路轉帳及其他電子支付轉帳功能。為防止歹徒利用同一存款人之其他尚未遭警示通報之帳戶繼續進行詐騙，特訂定本作業程序。金融機構所有分支單位於接獲「警示帳戶」通報後，應立即向金融機構總行通報，金融機構總行於接獲所屬分支單位之「警示帳戶」通報後，應立即向「金融聯合徵

信中心」(以下簡稱「聯徵中心」)通報。聯徵中心接獲警政署刑事警察局及金融機構總行(含聯徵中心會員及非聯徵中心會員)所通報「警示帳戶」資料，應每半小時將資料轉入「信用資料庫」。金融機構總行應於每營業日上午 10 時及下午 5 時各一次主動至聯徵中心「信用資料庫」中擷取「警示帳戶」資料。擷取方式則依聯徵中心通報方式為之，如未申請檔案加密系統之非會員金融機構，則由聯徵中心以書面傳真「警示帳戶」通報案件。金融機構 (含所有分支單位) 亦得隨時至「信用資料庫」查詢所通報「警示帳戶」資料。

金融機構總行於擷取或收到聯徵中心之「警示帳戶」通報資料後，應即時查證比對金融機構所有分支單位是否有「警示帳戶衍生之管制帳戶」，若發現有此等帳戶應即予註記，限制存戶使用提款卡、語音轉帳、網路轉帳及其他電子支付之轉帳交易（不含臨櫃交易及自動扣款轉帳等情形），並循金融機構內部通報系統轉知所屬分支單位。該「警示帳戶衍生之管制帳戶」雖非屬警示帳戶，但如屬「金融同業間遭歹徒詐騙案件通報要點」所列之「歹徒詐騙案件」者，則仍應依該要點向聯徵中心通報。「警示帳戶衍生之管制帳戶」如經各金融機構研判無詐騙之虞者，金融機構應即解除限制。

2006 年《銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法》

金管會於 2006 年 4 月 27 日以金管銀(一)字第 09510001640 號令訂頒《銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法》，以有效遏止詐欺犯罪所衍生之人頭帳戶過於氾濫，以確保金融體系運作之完整與消費者權益。本法定義「警示帳戶」指法院、檢察署或司法警察機關為偵辦刑事案件需要，通報銀行將存款帳戶列為警示者。此機制係為配合警調機關查緝電話詐欺恐嚇案件需要，暨維護民眾權益，於 2002 年 10 月建立之通報、支付方式變更及協助還款機制，明訂於本辦法以提升其法律位階；另為強化該機制功能，將其適用範圍擴大至偵辦刑事案件需要。「衍生管制帳戶」指警示帳戶之開戶人所開立之其他存款帳戶。此本法同時也回應了《洗錢防制法》等對可疑交易和開戶身分認證的要求。

2006 年《金融機構辦理警示帳戶聯防機制作業程序》

另，為迅速協助民眾通報警示帳戶以即時攔截財損款項，金管會特督促銀行公會依據《銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法》第七條第四項之規定，及金管會 2006 年 7 月 26 日金管銀(一)字第 09510003090 號函頒《金融機構辦理警示帳戶聯防機制作業程序》，規定金融機構在接獲「檢警調通報設定警示帳戶」或「金融機

構協助受詐騙民眾通報疑似警示帳戶通報單」時，經查詢帳戶內之詐騙款項轉出至其他金融機構帳戶時，應立即啟動聯防機制，通報下一受款之金融機構，以遏止不法資金流出。

第二項　「認證身分，減少偽冒開戶」相關規定

除《銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法》第五條第一項第二款訂有規定：「存款帳戶如屬偽冒開戶者，應即通知司法警察機關、法務部調查局洗錢防制處及金融聯合徵信中心…」以通報建立偽冒身分資料庫外，作業面上尚有《金融機構開戶作業審核程序暨異常帳戶風險控管之作業範本》以及《防杜人頭帳戶範本》。

2006 年《金融機構開戶作業審核程序暨異常帳戶風險控管之作業範本》

為提升金融機構辦理開戶作業之嚴謹性及對異常帳戶之風險控管，並加強防杜異常帳戶之開立或進行詐欺、洗錢等不法行為，銀行公會依據《銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法》第十二條及相關規定訂定《金融機構開戶作業審核程序暨異常帳戶風險控管之作業範本》[293]。規範金融機構辦理開立銀行法第六至第八條所

[293] 行政院金融監督管理委員會銀行局中華民國 95 年 6 月 30 日金管銀(一)字第 09585013680 號函准予備查

稱之支票存款、活期存款及定期存款帳戶，其開戶作業程序應依下列方式辦理：

一、應指派資深行員辦理開戶審核工作。

二、受理開戶時應查核客戶身分：雙重身分證明文件查核，以確認係其本人。使用聯徵中心「Z 系統通報案件紀錄資訊」功能查詢「Z21 國民身分證領補換資料查詢驗證」、「Z22 通報案件紀錄及補充註記資訊」。另，各金融機構可依其使用需求，選擇是否查詢「Z07 通報案件紀錄資訊」「Z13 補充／註記資訊」及「 Z18 通報案件紀錄資訊—受通報者統計資訊」等資訊。

三、受理開戶時應向客戶宣導，如提供帳戶供非法使用應負法律責任。

四、採用「開戶檢核表」輔助工具，嚴格審核申請新開戶案件，以防杜利用人頭申請開立帳戶。

五、建立「拒絕開戶資料庫」。

六、受理個人開立活期性存款戶（支票存款除外），應確實依據銀行公會訂立之《國內金融機構受理存戶新開戶建立影像檔注意事項》[294]採錄影或拍照方式建立開戶影像檔案。

[294] 中華民國 93 年 3 月 31 日中國銀行商業同業公會全國聯合會全一字 第 0790 號令訂定發布

2007 年《防杜人頭帳戶範本》

2007 年 1 月銀行公會訂定的《防杜人頭帳戶範本》[295]則是提供了更詳盡的開戶作業參考，提供金融機構人員在臨櫃面判斷可疑人頭或冒名開戶的觀察表徵，及在資訊面、管理面、交易面和教育宣導等的加強作為。

第三項　金融聯合徵信中心

金融聯合徵信中心是台灣地區目前唯一蒐集金融機構間信用資料的信用報告機構，也是亞洲地區第一家蒐集並建置個人與企業之正面與負面信用資料的信用報告機構。該中心之前身為「台北市銀行公會聯合徵信中心」，創始於 1975 年，為銀行公會體系下負責公會會員機構間授信資料蒐集、處理及交換之資料處理中心，後於 1992 年以原組織營運剩餘，以台北市銀行公會名義，全數捐助成立為公益性財團法人「金融聯合徵信中心」。

聯徵中心被指定為前述「警示帳戶」和「衍生管制帳戶」的資料庫管理單位，提供及時提供給所有會員機構使用。

在個人方面，被害當事人可以利用的服務項目有申請「信用報告」、「信用註記」和「解除警示」。

[295] 行政院金融監督管理委員會銀行局中華民國 96 年 1 月 11 日銀局(一)字第 09500553460 號函准予備查

信用報告

當當事人的國民身分證遺失時，除應該盡快親自向全國各地任何一個戶政事務所，或是用電話向其戶籍所在地的戶政事務所辦理掛失，並申請補發新的身分證外，如果擔心身分證會被有心人士冒名開戶或申請貸款、現金卡、信用卡，當事人可以向聯徵中心申請一份綜合信用報告書加以核對，如有可疑記錄，再盡快向報送的金融機構接洽釐清。

信用註記

更進一步的保護方式，可利用聯徵中心之「當事人辦理註記申請」，要求聯徵中心在當事人之電腦檔上擇一註記下列選項：1, 金融機構核貸核卡，當事人特別要求須確認係本人辦理；2, 即日起不再申請貸款、信用(現金)卡；3, 限定日期內不再申請貸款、信用(現金)卡；或4, 限與國內金融機構業務有關者的其他事項。用以通知金融機構，在接到以當事人為名義新申請的金融服務時能與當事人聯絡或逕行其他交付事項，以避免身分被冒用。

解除警示

當身分竊用被害人之存款帳戶被設定為「警示帳戶」，可備妥身

分證明文件，向聯徵中心申請取得載有「詐騙通報案件紀錄資訊」的「當事人綜合信用報告」，然後親赴距離個人最近的警察機關，向偵查隊詐欺案件承辦人索取申請書填寫，請求協助調查及解除事宜。

第五節　小結

我國因為歷史及國情因素具有一完整之國民身分證體系。我國的身分證具有兩個重要特色:(一)統一的國民身分識別證明文件;(二)個人的專屬身分證號碼。因為身分證的普及運用，此證號也實質上成為全國性單一的個人身分識別號碼。又因為公務和非公務機關絕大部分均使用個人身分證上之基本資料進行建檔索引，所以當面臨到身分證遭到偽冒用時，只要聯絡當地戶政事務所和警察機關，證明是本人身分遭到偽冒用，就可以開始啟動更正的作業。被害當事人還可以利用聯徵中心的服務項申請「信用報告」、「信用註記」或「解除警示」，解決金融上的冒用問題。在某一程度而言，因為具有統一身分證體系和相對資料庫的運用，大幅降低了身分竊用危害的蔓延。

在金融機構配合部分，主管機關頒佈一系列的法律、法規、命令和作業規章，以警示聯防，阻絕冒名戶頭的不法使用和認證身分，減少偽冒開戶，加強要求金融機構採取更嚴謹的開戶身分查驗認證工作，

以預防及嚇阻偽冒身分開戶的情事。

在個人資料保護上，係以「個人資料自主權」為出發點的個人隱私權保護目的。雖非以身分竊用為主要保護目標，但當個人資料保護機制實施得當避免洩漏，再加上對不法使用個人資料施以刑罰的嚇阻，其對身分竊用防制必然產生正面的功效。不過自之前的《電腦處理個人資料保護法》包含的範圍過窄，以至效果不彰，至 2010 年公布《個人資料保護法》，因為內容爭議性過大，迄 2012 年仍尚未施行，且已有要修法的呼聲，我國在個人資料保護法制和實務的完備上尚待進一步的努力。

在刑法部分，我國雖然沒有將身分竊用單獨入罪，但有相關法律條文可被應用來間接處理身分竊用的犯罪行為。但是，是否有清楚的參酌到身分竊用受害者的法益侵害，並在整體論罪量刑上予以呈現，以符合現在社會的進程改變和人民的期待，則待觀察。

(空白頁)

第五章 美國與我國身分竊用問題法律比較分析

本章基於前面數章所蒐集整理之資料，進行美國與我國身分竊用問題法律的比較分析。

第一節 身分識別制度與實務比較分析

美國在個人身分識別制度上和我國相當的不同，美國目前為分散式的身分識別方式，而我國則是集中統一。

美國一方面發佈一系列法令，希望能減低公、私部門對其社會安全號碼的應用，企圖消除全國性單一的身分識別號碼。但同時嘗試藉由規範各州政府，建立一套全國性的身分證體系。不過到目前為止，進展並不是相當順利。這應是美國聯邦體制和歷史國情所致，另外也是美國人民對個人資料置於集中資料庫所產生的疑慮，不但不認為其為解決身分竊用問題上提供身分確認的工具方法，甚至是認為其之建立，反而會增加身分竊用受害機率。其重要的論點是：一、不可能有完全安全的資料庫；二、內部濫用資料比資料外洩的機率更高，危害也最大。

我國因為歷史及國情因素具有一完整之國民身分證體系。我國的身分證具有兩個重要特色:(一)統一的國民身分識別證明文件;(二)

個人的專屬身分證號碼。因為身分證的普及運用，此證號也實質上成為全國性單一的個人身分識別號碼。又因為公務和非公務機關絕大部分均使用個人身分證上之基本資料進行建檔和各資料庫間的連線索引，所以我國在個人資料庫的型態上，具有雖分散建立儲存，但可集中運用的功能。

美國雖然在建立一套各州經營的全國性的身分證體系遇到一些挫折，但是就其進程看來，似乎計畫推動者看到我與我國類似的集中統一身分識別方式的優點，所以才有這些作為。

第二節　刑事制度與實務比較分析

美國訂有專法將身分竊用單獨入罪，有「身分竊用罪」和「加重身分竊用罪」；我國則無身分竊用罪名，視其犯行，一般常見係包括在「偽造文書罪」上處理。

美國對身分竊用的問題很早就注意到，主要是因為因身分竊用所致生的或是為手段的詐騙事件頻傳，而且影響又因為資通科技的發達而迅速擴大，迫使美國政府必須拿出對應政策，加以控制。雖然在州法階層，1996 年亞利桑納州(Arizona)就已經成為第一個將身分竊用立法定義為刑事罪。 但將身分竊用定義成是一種 1998 年的《身分竊用

嚇阻法》是第一部專門針對身分竊用問題而立的法。這也是第一次讓身分竊用成為一個正式的聯邦罪名方便讓各級執法單位可以起訴罪嫌。

在 2004 年又通過了《身分竊用罪刑加重法》，擴大既有的身分竊用的涵括範圍，針對若干罪行，當其有使用身分竊用為犯罪手法達成其犯罪目的，在量刑時，會在主罪所應負刑責之上，再針對其身分竊用行為予以加重刑期。

美國在偽造身分證明文件上係由《身分竊用嚇阻法》處理。《身分竊用嚇阻法》特別對有關「身分證明文件」、「身分證明方式」等做定義性之規範。 如「身分證明方式」係指當單獨或與其他資訊一併使用，可證明特定人之身分，包括：姓名、社會安全號碼、生日、駕照號碼、外國人登記號碼、護照號碼、獨特電子身分證明號碼、地址、密碼等。不論是為、變造實體和非實體的身分證明方式均屬之。還有「身分證明方式」，即係指當單獨或與其他資訊一併使用，可證明特定人之身分的證明方式均屬之。包括：姓名、社會安全號碼、生日、駕照號碼、外國人登記號碼、護照號碼、獨特電子身分證明號碼、地址、密碼等。因此，本法所定義之「身分證明方式」包括了《美國聯邦法典》18 U.S.C. § 1029(e)(1)裡對「存取裝置」(access device)的定義，即：「任何卡(card)、版(plate)、碼(code)、帳號號碼(account number)、

電子化序號(electronic serial number)、移動識別碼(mobile identification number)、個人識別碼(personal identification number)或其它電信服務、設備或儀器識別器(identifier)、或其他方式單獨或與其他任何存取裝置配合使用而控制帳戶，以用來獲得金錢、貨品、服務或任何其他有價值之事物，或可以用來啟動資金轉移者。」這讓一些電腦犯罪(computer crime)行為，也納入身分竊用罪的範圍內。

《身分竊用嚇阻法》法亦引導「美國聯邦量刑委員會」，檢視並修正《美國聯邦量刑基準》(Federal Sentencing Guidelines)，對於身分竊用犯罪，訂定更為適當的罰則。「身分竊用罪」是被放在《聯邦量刑基準》USSG §2B1.1 來參考量刑。該章是專門處理偷竊、貪瀆和其他型態的不法取得行為。這包含了如盜贓物、破壞財物、詐欺、偽造、偽變造非美國政府負擔之證券等罪行。除了「加重身分竊用罪」原本就具備的最低刑期，因聯邦量刑委員會確信，一項明確的監禁刑，即使期間不長，仍會產生特別的嚇阻作用(deterrence)。而在《聯邦量刑基準》中特別設計「若加總後犯罪程度級數為達 12 級，則直接增加至 12 級」就是為了讓犯罪者必須在監獄服刑。

相較於美國，在身分證明文件上，因為我國有國民身分證制度，故在《戶籍法》上有專門條文處理偽造、變造身分證。但我國戶籍法第 75 條只處理偽造、變造國民身分證和進而行使，遂行冒用身分

的犯行；而偽造、變造其他身分證明文件，係由《刑法》第 212 條偽造特種文書罪處理。而其使用以遂行冒用身分的犯行則係《刑法》第 216 條所言之「行使第二百十條至第二百十五條之文書者，依偽造、變造文書或登載不實事項或使登載不實事項之規定處斷。」

值得注意的是，因為《戶籍法》第 75 條第三項的構成要件僅有他人交付或遺失之國民身分證，不包括被竊，故與美國在身分竊用概念上的「竊用」包括偷竊個人身分證明文件而冒名使用不同。在我國此行為不違反《戶籍法》第 75 條，但是會因為使用他人身分證而觸犯了《刑法》第 210 條的行使偽造私文書罪。雖然如此，但因為我國處理身分竊用問題本就將其納入偽造文書罪內，故無太大差異。

我國在論罪上，因為身分竊用通常是為達犯罪目的的其中一種行為手段，在罪數論中常被視為「包括一罪」，故實務上處理常見運用到《刑法》第 55 條想像競合，即「一行為而觸犯數罪名者，從一重處斷。」所以常見到的是以較重之「行使偽造文書罪」處斷。

至於在量刑部分，我國並無類似美國的《量刑基準手冊》臚列包含被告的犯罪前歷、犯罪涉及之被害人人數、犯罪所涉及偽造或非法取得之身分證明文件（方式）、犯罪導致受害者損失金額之多寡等各項考慮因子，並有《量刑基準表》可供法官於量刑時參考。我國的實務操作則是依《刑法》第八章「刑之酌科及加減」進行，輔以參考類

似判決進行量刑。

第三節　個人資料保護制度與實務比較分析

每個國家對個人資料隱私權保護的法律和實務都有所不同。在歐洲則有長遠的歷史，歐盟對人權的保護是採取從上而下立法的方式，供大家遵守。但是，美國卻是相反，是由下而上。美國沒有單一的個人資料保護法，也不認為有其需要。然而，觀察美國的發展，其對於一些重要的諸如兒童的隱私和電子商務或其他等領域，已慢慢地形成一些規範出來。

一直以來，美國在個人資料保護作為上比較傾向建置一個結合法規、命令和自我管理的架構，而非由政府制訂的單一法規。由於美國之國家體制為聯邦制，相較於其他國家，其並未制定全國統一適用之個人資料保護法，而是由各州及聯邦政府基於權力分立原則，分別立法規範。其中，在聯邦立法層次，除關注個人健保資料之保護外，更特別重視消費者金融隱私之保護。雖然美國國會先後制定通過許多與個人資料保護相關之隱私權法案，而金融主管機關亦對於個人金融資料之保護，頒訂相關行政命令，但美國國會似乎仍未頃向於制定一部足以包羅所有個人資料之隱私權法案；相對地，美國是依其社會經濟

之各個發展階段，建構出各種錯落分散之隱私權法制。

美國在推動其個人資料保護的進程中，以對個人影響最大的金融財務相關的領域為先。美國在這方面的立法始自於 1970 年的《公平信用報告法》。而 1974 年的《隱私權法》，其主要目的則是限制政府使用人民的個人資訊。之後完成立法的幾乎都集中在信用報告和帳務及交易等領域。其中也穿插對個人的社會安全號碼以及駕駛執照資料的保護，因為此兩者為美國人們大量用來作身分識別的號碼及文件資訊。但因為美國身分識別方式的方散，被用來做身分識別資料多樣且多元，造成身分識別資料的管理更加複雜，保護更不易。

雖然美國散見在如《公平信用報告》等各目的專法上對個人資料保護和正確性的維護相關的要求相當的多。不過，迄今，美國並無單一的個人資料保護法規可以和歐盟的「個人資料處理保護指令」直接對應。惟美國因為受到歐盟的經貿壓力，美國與歐盟為解決跨國個人資料流動之問題，由美國商業部與歐盟執行委員會進行協議，試圖建立遵守個人資料保護之機制。最後，雙方在妥協之下，簽訂一項「安全港計畫」。基本上，「安全港計畫」為一自願性計畫，明定舉凡美國聯邦貿易委員會及運輸部所管轄之企業或組織，得主動申請加入「安全港計畫」，並遵守聯邦貿易委員會之規定，以取得認證。至此，雖尚未及於美國之聯邦法地位，但美國的個人資料保護確實已藉由商業

運作開始向其他世界接軌，其未來發展是否會向歐盟靠攏，值得觀察。

我國對於個人資料之保護規範，則始於 1995 年頒布之《電腦處理個人資料保護法》，因我國於 1990 年左右積極推動加入國際貿易組織(World Trade Organization: WTO)，而歐盟各國一向對個人資料之保護十分重視，為避免在加入 WTO 組織協商過程中，被指摘我國對個人資料保護不力，法務部乃擬定立法計畫積極進行研擬法案工作。係參照經濟合作開發組織(OECD)所揭示的保護個人資料八大原則所制訂。為避免對民間衝擊過大，僅將經電腦處理之個人資料納入保護範疇。另考量個人資料蒐集之數量與利用情形，除公務機關外，僅限制大量蒐集個人資料作成個人資料檔案，以供利用之徵信業及以蒐集或電腦處理個人資料為主要業務之八類事業，為適用本法之非公務機關。另為怕掛一漏萬，爰授權法務部會同中央目的事業主管機關指定特定之事業、團體或個人亦得適用本法。

實行之後，因舊法無法應對社會發展的狀況和對個人資料保護的呼聲，後於 2010 年修正公布之新《個人資料保護法》，為該法第一次且大幅度修法。本次修正擴大了法律適用範圍：公務和所有非公務機關，包括自然人、法人或其他團體，不分行業，均納入個人資料保護法適用對象；擴大個人資料之範圍：將護照號碼、醫療、基因、

性生活、健康檢查、犯罪前科、聯絡方式及其他得以直接或間接方式識別個人資料，均納入個人資料之範圍；增加特種個人資料定義；明訂安全維護責任;提高民事賠償責任金額;增加公益團體代表訴訟；提高刑事責任;增加意圖營利犯罪者或非法妨害公務機關個人資料檔案之正確者，為非告訴乃論等。

但此影響層面極廣的新《個人資料保護法》，幾乎涉及所有的企業、團體，以及個人，卻在立法過程中，由於欠缺充分討論，立委又各自提出不同版本，以致通過條文完全脫離行政院版本，發生窒礙難行的情形，各界為此也抱怨連連，認為不宜貿然實施，以避免對社會造成衝擊。本法迄今（2012 年 9 月）尚未施行。

相較於美國，我國在個人資料保護的體制和施行遵循的是如歐盟般的由上而下模式，但爭議似乎自始就不間斷。法務部法律事務司科長黃荷婷在公開演講時就曾表示：「有些國際的學者在比較歐盟、APEC[296]和美國的情形，諸如這種從上而下或者是由下而上的模式，他們的結論認為較有效率的，應屬美國由下而上的模式，因為只有如此，才能真正做出實際管理面的流程，而且並不重視立法模式，而是重視執行的層面。因而，美國的動向值得注意，將來對於隱私權的保護做得會更好。歐盟的標準很高，而實際上做得更好的，有可能是美國。」

[296] Asia-Pacific Economic Cooperation 亞洲太平洋經濟合作會議

[297]作者的觀察研究則以為，美國之個人資料保護若有較他國更好的成效，並非其分散式的立法模式所致，而是其對於實務面上的保護目標明確和重視執行手段以求實行效果而來。

第四節　消費者信用報告制度與實務比較分析

因為個人信用資料對現代人的生活影響至劇，所以美國第一份針對個人資料保護的立法就和個人信用報告有關，應不難理解。可能是習稱，也可能是被法案名稱所侷限，一般人所說的個人信用報告其實包含兩個意義：（一）狹義的「個人信用報告」(Credit Report)；（二）「消費者報告」(Consumer Report)。「消費者報告」的內容會參考「個人信用報告」，但反之則不然。

美國的信用報告產業(credit reporting industry)係配合消費金融之發展而產生。最早期之消費者信用報告是地區性且內容較為單純，所蒐集資料較少，且格式並未標準。各信用報告機構(credit bureau, credit reporting agency 或 consumer reporting agency)以人工處理信用資料，不定期更新，保管期限不確定。隨著時間經過，這些小型消費者報告

[297] 參見法務部法律事務司科長 黃荷婷，於 2011/05/17「個人資料保護法規對金融業影響之探討」研討會之發言。會議實錄來源：http://www.tfsr.org.tw/uploads/個人資料保護法規對金融業影響之探討研討會實錄_1000609.pdf ，（前次檢索日：2012/07/07）

機構逐漸蛻變為大型個人資料庫。目前消費者報告體系主要由 Equifax、Experian、以及 Trans Union 等三大消費者信用報告機構組成,保管為數達 15 億之信用帳戶資料，帳戶所有人達 1. 9 億人。隨著資料保存及通訊技術之發展，各界逐漸重視金融隱私之保護。美國於 1970 年所頒佈施行之《公平信用報告法》所規範的主體就是消費者信用報告機構和報告的使用者（銀行、貸款商）。美國的金融消費隱私權保護濫觴即是來自此法的施行。

鑒於身分竊用案件因科技及資訊之發展而日益猖獗,美國於2003年公布《公平正確信用交易法》，以協助消費者及金融機構共同打擊犯罪。《公平正確信用交易法》的 Section 5 修正了之前的《公平信用報告法》，特別加入和身分竊用及其與消費者相關的事項。本法讓身分竊用受害者得以要求金融機構等借貸人(creditor)及信用報告機構(credit bureau)，將其個人信用記錄中因遭身分竊用犯罪受害影響而被註記的負面資訊予以移除。

《公平正確信用交易法》建立金融詐欺行為預警制度，如消費者發現其可能因身分遭冒用或金融詐欺而受損害時，得以通知消費者報告之使用者，以降低消費者遭詐欺受害之機率。當消費者懷疑已經或即將成為身分竊用的犯罪被害者，他們可以通知信用報告機構，要求在其個人信用檔案中加入「初級警戒」註記。當消費者確定成為身分

竊用的受害者，而且已經向執法機關報案，隨後他可以要求信用報告機構在其個人信用檔案中加入「延長警戒」註記。這「延長警戒」會在其個人信用檔案留存七年，且這受害人可以在 12 個月內要求信用報告機構免費提供他的個人信用報告兩次，以供其積極注意信用狀況的變化。《公平正確信用交易法》還讓身分竊用受害者在提供消費者信用報告機構必要的文件後，該機構必須在四個工作日內封鎖該受害者之在該機構的相關檔案，不得再使用。同時，該機構必須通知其他消費者信用報告機構，同時進行資料封鎖，以避免身分竊用受害影響擴大。當然，信用報告機構也可以依法判斷是否給予封鎖或解除封鎖。

《公平正確信用交易法》並設立相關的規定來防範身分竊用。如：要求商家不得將客戶的信用卡號碼資料印在收據上，也讓消費者可以要求信用報告機構，當被要求出具他們的信用報告時將其個人社會安全號碼自報告中移除等。

聯邦貿易委員會透過《公平信用報告法》和《公平正確信用交易法》授與的權限，發佈過諸多命令：如要求金融機關與信用卡公司強化對民眾信用資料準確性的維護、建立民眾對錯誤信用資料的回報和業者的快速處理機制，並要求三家全國性的信用報告公司 Equifax、Experian 與 Trans Union 應免費提供消費者年度信用報告供查閱。聯

邦貿易委員會同時要求信用報告公司應在網站與新聞媒體上加強對消費者的教育，宣導信用報告「免費取得」的意旨，避免消費者被他人冒名開戶、信用受損而不自知。

相較於美國，我國的「聯合徵信中心」係非營利的財團法人機構，並無專法規範該機構，因其已屬《個人資料保護法》涵蓋的消費者信用報告產業。聯徵中心只提供個人的財務金融「信用報告」，而無提供像美國般的「消費者報告」，其敏感度和涵蓋度與應用度上與美國之消費者信用報告產業有相當程度上的不同。

在應對身分竊用問題上，我國聯徵中心被指定為「警示帳戶」和「衍生管制帳戶」的資料庫管理單位，提供及時提供給所有會員機構使用，以避免冒名和人頭帳戶繼續被利用，降低負面影響。在個人方面，身分竊用被害當事人可以利用的服務項目有申請「信用報告」、「信用註記」和「解除警示」。基本上和美國的相近。

在提供免費年度個人信用報告上，美國的信用報告機構有數家，所擁有的個人資料範圍較我國為廣，且申請單份個人信用報告費用從 9.95 至 20 美元不等，美國人為了解自己身分竊用受害的程度，所需要的費用相較我國高出甚多，故其採取免費提供年度個人信用報告制度，有其背景。相較於美國，我國的聯徵中心為我國目前唯一個人信用報告機構，申請一般個人信用報告每次僅為新台幣 100 元，且每人

均可於每年免費申請一次個人之年度信用報告，[298]並不限於必須是身分竊用受害本人，故更較美國為優。

第五節　金融機構配合規定比較分析

在個人身分識別碼方面，美國希望各金融機構能減少利用客戶的社會安全號碼來作識別，而我國則不限制使用國民身分證號。美國和我國均要求金融機構要在開戶和交易各階段做好客戶的身分確認。美國的著眼點比較是來自洗錢防制和打擊資助恐怖主義，而我國比較是來自防詐騙，但同時也符合了洗錢防制和打擊資助恐怖主義的要求。在身分竊用防制的部分，兩國的金融機構所進行的努力方向基本上是一致的。

[298] 參見 金融聯合徵信中心網站：當事人查詢信用資料辦理程序，http://www.jcic.org.tw/doc/personal_credit_1010701.pdf，(前次檢索日：2012/09/09)。

第六章 結論與建議

我國和美國雖然均面臨到身分竊用的問題，但因為國情和制度的不同，所受到的影響程度和所採取對應問題的方式也因此不同。例如：我國和美國在對個人識別號碼的態度和處理不同，美國是盡量打破個人利用單一獨特號碼進行識別的機制，但是我國則是大量的使用。在個人身分證明文件上，我國較為統一，美國較為分散，迄今尚未有全國統一性的身分識別證。在個人識別資料庫的建置和運用上，我國相對集中，美國重分散。再美國加上國土遼闊、人口眾多、商務交通繁榮和聯邦體制的特殊性，因此在身分竊用問題的處理上，困難度遠較我國為大。本研究認為下列發現值得提出：

我國現在使用的國民身分證和身分證號在實體世界所建構的通用身分識別體系，因為個人資料庫雖分散但可集中連線查詢管理的特性，其在身分竊用防制機制的優勢因此建立。惟一方面在享受其優勢外，必須持續注意並加強個人資料庫的資訊安全管理。由於現在社會的演進已由實體世界擴張深入至以網際網路建構的網路世界，而此網路世界也和實體世界緊密相合，美國和我國所面臨的身分竊用威脅事實上是完全的相同，更有可能因為我國國民的生活習慣，讓我們對於網路世界的接受度和利用度更不下於美國，所面臨身分竊用的威脅也難謂較美國為輕。在網路世界中的身分識別係以個人身分資訊識別

(PII)為主體，我國現在的實體身分識別體制不見得能著力太多，必須輔以其他機制，加強網路世界和實體世界在個人識別上的連結，但同時又要避免個人隱私權的可能侵害和商務通訊等的便利性。為了保護個人資料和符合歐盟個人資料保護指令，我國很早就訂頒了《電腦處理個人資料保護法》，現又修訂了新《個人資料保護法》，除了增加適用範圍外，也加重了民事責任和刑事罰則。方向上可以看出對個人資料保護及其影響的重視，但未來實際運作上，效果如何，仍待觀察。作者以為，主要影響民眾和企業對身分竊用問題和個人資料保護的認知和施行是來自行政機關對個人資料保護相關事件的處理態度和法院的審理結果。如，雖個人資料保護法訂有罰則，但是否會因為我國刑法論罪的方式，因法院操作時被其他犯罪行為「吸收」，所得到最後的判決結果和現在的一樣，當犯罪者所受的後果小和所得大，因而出現嚴重失衡，更難彰顯出嚇阻效果。

我國對個人資料的保護是遵循歐盟模式，採取從上而下立法的方式；相反的，美國在個人資料保護作為上比較傾向建置一個結合法規、命令和自我管理的架構，而非由政府制訂的單一法規，是採由下而上模式。而且並不重視立法模式，而是重視執行的層面。美國由下而上的模式，其缺點是體系較為鬆散複雜，掛一漏萬的機會較多，但優點則是能真正做出實際管理面的流程，有助於落實特定的範圍的個人資

料保護工作。作者的觀察研究則以為，美國之個人資料保護若有較他國更好的成效，並非其分散式的立法模式所致，而是其對於實務面上的保護目標明確和重視執行手段以求實行效果而來。

根據美國聯邦貿易委員會(FTC) 的報告指出，要清楚界定資料外洩和身分竊用之間的關連是相當困難的，因為身分竊用的受害者常常不知道他們的個人資料何時被他人不法使用，而且身分竊用被害人往往無法得知自己已經被害。因此，美國對身分竊用的法律策略重點，不再只針對個人隱私權和資料的保護，規範個人資料的蒐集、處理和保管人的責任義務，且在個人資料外洩事件時加諸保管人通知個別個人的責任，更進而加強對個人資料的不法利用的防制，特別是將身分竊用行為明確入罪化。此身分竊用之入罪化不止包含傳統實體身分識別證明文件資料的偷竊和冒用，還有「身分證明方式」，即係指當單獨或與其他資訊一併使用，可證明特定人之身分的證明方式均屬之。包括：姓名、社會安全號碼、生日、駕照號碼、外國人登記號碼、護照號碼、獨特電子身分證明號碼、地址、密碼等。所以在《身分竊用嚇阻法》定義之「身分證明方式」還包括了《美國聯邦法典》18 U.S.C. § 1029(e)(1)裡對「存取裝置」(access device)的定義，即：「任何卡(card)、版(plate)、碼(code)、帳號號碼(account number)、電子化序號(electronic serial number)、移動識別碼(mobile identification number)、個人識別

碼(personal identification number)或其它電信服務、設備或儀器識別器(identifier)、或其他方式單獨或與其他任何存取裝置配合使用而控制帳戶，以用來獲得金錢、貨品、服務或任何其他有價值之事物，或可以用來啟動資金轉移者。」這讓一些電腦犯罪(cyber crime)行為，也納入身分竊用罪的範圍內，對於打擊電腦犯罪多了一項可以訴追的工具。我國因為把輸入在電腦的個人資料一律視為文書，現行實務做法若是冒用，係以偽造文書罪處理。

我國在論罪上，因為身分竊用通常是為達犯罪目的的其中一種行為手段，在罪數論中常被視為「包括一罪」，故實務上處理常見運用到《刑法》第 55 條想像競合，即「一行為而觸犯數罪名者，從一重處斷。」所以常見到的是以較重之「行使偽造文書罪」處斷。至於在量刑部分，我國並無類似美國的《量刑基準手冊》臚列包含被告的犯罪前歷、犯罪涉及之被害人人數、犯罪所涉及偽造或非法取得之身分證明文件(方式)、犯罪導致受害者損失金額之多寡等各項考慮因子，並有《量刑基準表》可供法官於量刑時參考。我國的實務操作則是依《刑法》第八章「刑之酌科及加減」進行，輔以參考類似判決進行量刑。作者以為，我國審判實務在量刑時，在《刑法》第 57 條的基準上，似可同時參考「美國聯邦量刑委員會」所設計之《量刑基準》，依犯罪人本身的犯行、犯罪前歷和被害人數及所受危害之損失金額和

範圍，對於量刑做更有系統化之分類和考量，並時俱進，能供法官較易做判決科刑時的參考基準，也更能切合民眾對法律的期待和情感。本研究對於「美國聯邦量刑委員會」在其《量刑基準》上針對身分竊用罪的量刑考量及該委員會如此設計之源由稍有描述，或可為後續研究或實務參考之用。

美國在對抗身分竊用問題所採取的方式雖因為國情和歷史的不同，而和我國有相當程度的差異，但美國對身分竊用的法律策略重點，不再只針對個人隱私權和資料的保護，更進而加強對個人資料的不法利用的防制，其在身分竊用犯罪嚇阻控制上，特別注意建立執法機關的查緝能力、訴追工具和司法機關量刑裁判的嚇阻效益，實值得我國學習。特別是將身分竊用行為明確入罪化。

參考文獻

壹、中文部分

專書

1. Lawrence M. Fredman 著，楊佳陵譯，《美國法導論－美國法律與司法制度概述》(American Law: an introduction)，商周出版，2004年3月。
2. 林超駿等作，《英美法常用名詞解析》，新學林出版社，2008 年 8 月。
3. 林鈺雄，《新刑法總則》，二版，台北：元照出版社，2009 年 9 月。
4. 黃仲夫，《刑法精義》，修訂新版，台北：元照出版社，2009 年 9 月。
5. 《美國公平信用報告法》，財團法人金融聯合徵信中心譯，，2006年12月。
6. 《銀行法法令彙編(增修訂第七版)》，台灣金融研訓院，民國 2009年1月。

學位論文

1. 鍾葦怡，《論詐欺罪之「詐術」》，國立政治大學法律學研究所碩士學位論文，2011 年 1 月。
2. 郭詠華，《現代行國家下的個人身分及其識別—百年來的台灣個人資料法社會史》，國立台灣大學法律學院法律學系碩士學位論文，2010 年 7 月。
3. 陳妍沂，《美國財務資訊隱私權保護規定之研究》，國立政治大學法學院碩士在職專班碩士學位論文，2008 年 5 月。
4. 馬興平，《論資訊隱私權的保護-從釋字第 603 號解釋出發》，國立中正大學法律所碩士論文，2008 年。
5. 馮聖中，「論金融服務與消費者保護之法律問題」，南台科技大學，財經法律研究所碩士論文，2007 年。
6. 郭志剛，《詐欺罪之研究—以電腦詐欺及廢除牽連犯、連續犯之修法為題》國立政治大學法律學研究所碩士學位論文，2007 年 7 月。

期刊文章

1. 葉奇鑫、李相臣，「淺談個人資料保護法民事賠償責任及數位鑑識相關問題」，《司法新聲》，第 101 期，2012 年一月，頁 33-49。

2. 楊崇森,「美國刑法之原理與運用」,《軍法專刊》,第 57 卷第 3 期，2011 年 6 月，頁 39-89。
3. 吳兆琰,「美國 anti-phishing 法制策略簡介」,《台灣電腦網路危機處理暨協調中心(TWCERT/CC)電子報》,2011 年 1 月號。
4. 廖有祿、江芝迎,「冒用人頭資料犯罪及相關防制對策」,《刑事政策與犯罪研究論文集（12)》,法務部編印，2009 年 12 月。
5. 閩庆飞、季绍波、仲秋雁,「身分盗用的发展及其治理和研究趋势」,大连理工学院《公共管理学报》,第四卷,第一期， 2007 年一月。
6. 王志誠,「美國金融隱私權法制之發展」,《台灣金融財務季刊》,第 7 輯第 1 期，2006 年 3 月，頁 71-90。
7. 陈立峰,「浅议身分盗用犯罪问题」,《江西公安专科学校学报》,第 6 期总第 98 期， 2005 年 11 月。
8. 黃昭元,「無指紋則無身分證？換發國民身分證與強制全民捺指紋的憲法爭議分析」,《民主、人權、國家－蘇俊雄教授七秩華祝壽論文集」》,2005 年 9 月。
9. 劉佐國,「我國個人資料隱私權益之保護—論『電腦處理個人資料保護法』之立法與修法過程」,《律師雜誌》,第 307 期，2004 年一月，42-51 頁。
10. 孙晓云、骆宁,「FACT Act：美国消费信贷法的最新里程碑」,《数

字财富》，2004 第 5 期。

11.「個人資料保護在台灣：誰的事務」,《國家政策季刊》，第 2 卷第 1 期，行政院研究發展考核委員會出版發行， 2003 年 3 月，頁 53-70。

12.「個人資料保護之研究—以個人資訊自決權為中心」,《司法研究年報》，第二十一輯第十七篇，司法院印行， 2001 年。

13. 劉靜怡等,「戶籍資料運用、個人資料保護與身分辨識之研究：戶政資訊系統與相關制度建置之研究」,中央研究院資訊科學研究所，2001 年 2 月。

14. 陳起行,「隱私權法理之探討-以美國法為中心」,《政大法學評論》，2000 年 12 月，頁 297-341。

15. 吳景芳,「美國之聯邦量刑改革法」，刑事政策與犯罪研究論文集(三)，法務部犯罪研究中心編印，2000 年 11 月。

網站資料庫

1. 司法院法學資料檢索系統 (http://jirs.judicial.gov.tw/)

2. 法源法律網 (http://www.lawbank.com.tw/)

貳、英文部分

期刊文章

1. HOOFNAGLE, Chris J., "*IDENTITY THEFT: MAKING THE KNOWN UNKNOWNS KNOWN*", Harvard Journal of Law & Technology, Volume 21, Number 1, Fall 2007
2. MOYE, Stacey, "*Fair and Accurate Credit Transactions Act-More Protection for Consumers*", The Information Management Journal, May/June 2006
3. SLEWE, Ton; HOOGENBOOM, Mark, "*Who Will Rob You on the Digital Highway*", Communications of the ACM, May 2004
4. GORDON, Gary R.; WILLOX, Norman Jr., "*Identity Fraud: A Critical National and Global Threat* ", A Joint Project of the Economic Crime Institute of Utica College and LexisNexis, a Division of Reed Elsevier Inc., October 2003
5. WILLOX, Norman Jr.; REGAN, Thomas, "*Identity Fraud: Providing a Solution*", Journal of Economic Crime Management , March 2002
6. LOPUCKI L M. "*Human Identification Theory and Identity Theft Problem*". Texas Law Review, 2001
7. CLARKE R. "*Human Identification in Information Systems: Management Challenges and Public Policy Issues*", Information Technology & People, 1994

研究報告及專書

1. "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers", Federal Trade Commission, March 2012
2. FINKLEE, Kristin M., "*Identity Theft: Trends and Issue*", CRS Report for Congress (R40599), Congressional Research Service, Library of Congress, February 2012.
3. "*United States Attorneys' Manual*", Office of United States Attorneys, U.S. Department of Justice, 2012
4. "*2011 Federal Sentencing Guidelines Manual*", United States Sentencing Commission, November 2011
5. "*Report to Congress: Mandatory Minimum Penalties in the Federal Criminal Justice System*", United States Sentencing Commission, October 2011
6. "*2010 Consumer Sentinel Network Data Book*", Federal Trade Commission, March 2011
7. "*40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations*", Federal Trade Commission, July 2011
8. "*Report to Congress: Regarding Federal Mandatory Minimum Sentencing Penalties*", United States Sentencing Commission, July 2009
9. "*Online ID Theft: Changing the Game - Protecting Personal Information On The Internet*", Microsoft Corp., September 2008
10. TATELMAN, Todd B., "*The REAL ID Act of 2005: Legal, Regulatory, and*

Implementation Issues", CRS Report for Congress (RL 34430), Congressional Research Service, Library of Congress, April 2008.

11. SWENDIMAN, Kathleen S., "*The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality*", CRS Report for Congress (RL 30318), Congressional Research Service, Library of Congress, February 2008.
12. "*2006 Identity Theft Survey Report*", for Federal Trade Commission, Synovate, November 2007
13. "*Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*" (GAO-07-737), United States Government Accountability Office, June 2007
14. "*Social Security Numbers: Use is Widespread and Protection Could be Improved*", (GAO-07-1023T), Government Accountability Office, June 2007.
15. "*A Guide to Preventing Identity Theft*", Info-Tech Research Group, 2005
16. "*Putting an End to Account-Hijacking Identity Theft*", Federal Deposit Insurance Corporation, December 14, 2004
17. PURDY, Andy, *et al*, "*Identity Theft Final Report*", Economic Crimes Policy Team, United States Sentencing Commission, December 1999
18. "*Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited*", Briefing Report to Congressional Requesters, United States General Accounting Office, GAO/GGD-98-100BR, May 1998.

網站資料庫

1. Identity Theft: Outline of Federal Statutes and Bibliography of Select Resources, LLRX – Law and technology resources for legal professionals, (http://www.llrx.com/features/idtheftguide.htm)
2. US Federal Trade Commission: Fighting Back Against Identity Theft (http://www.ftc.gov/bcp/edu/microsites/idtheft/)
3. US Department of Justice: Identity Theft and Identity Fraud (http://www.justice.gov/criminal/fraud/websites/idtheft.html)
4. US Department of Homeland Security: Secure Driver's Licenses (http://www.dhs.gov/files/programs/secure-drivers-licenses.shtm)
5. Federal Bureau of Investigation (FBI) — Identity Theft (http://www.fbi.gov/about-us/investigate/cyber/identity_theft)
6. Federal Deposit Insurance Corporation (FDIC): Identity Theft (http://www.fdic.gov/consumers/consumer/alerts/theft.html)
7. US Government Printing Office: CODE OF FEDERAL REGULATIONS (http://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR)
8. United States Sentencing Commission (http://www.ussc.gov)
9. United States Attorneys' Manual, U.S. Department of Justice. (http://www.justice.gov/usao/eousa/foia_reading_room/usam/)
10. Federal Jury Instructions Resource Page, Federal Evidence Review (http://federalevidence.com/evidence-resources/federal-jury-instructions)
11. Identity theft is a crime: Resources from the Government (http://www.idtheft.gov/)

12. IT Law Wiki (http://itlaw.wikia.com/wiki/)
13. Cornell University Law School: Legal Information Institute: United States Codes (U.S.C.) (http://www.law.cornell.edu/uscode/text)
14. Westlaw (http://www.westlaw.com)
15. Electronic Privacy Information Center (EPIC) - National ID and the REAL ID Act (http://epic.org/privacy/id_cards/)
16. Identity Theft Resource Center (http://www.idtheftcenter.org/)
17. Roger Clarke's Identity Home-Page (http://www.rogerclarke.com/ID/)
18. Wikipedia: Identity Theft (http://en.wikipedia.org/wiki/Identity_theft)