

私立東海大學法律學研究所

碩士論文

指導教授：李成 博士

美國經濟間諜法之研析

兼 述 我業因應之對策



研究生：林慧玲

民 國 八 十 九 年 六 月

論文摘要

隨著高科技產業在全球市場持續增加價值性與流通下，竊取營業秘密行為的案件大幅增加，美國科技領先全球，相對的便提高受侵害之程度，為維護其企業之國際競爭力與經濟安全，國會遂於 1996 年立法通過經濟間諜法 (The Economic Espionage Act, EEA)。明文對於營業秘密、侵害行為加以定義，並對侵害者科以嚴刑峻罰，以向全球昭告其保護營業秘密之立場。該法立法通過後不久，我國永豐紙業公司與四維公司便相繼被控違反該法，引起國內業者對該法之重視。如何加強企業對該法規範之認識，以及避免或降低企業在從事技術移轉或延攬美籍人才之際可能存在之法律風險，遂成為本文探討之重點。

為此，本文以美國經濟間諜法為研究主題，並就針對企業與政府二方面提供因應該法之建議，共分為六章，茲簡述內容如下：

第一章 緒論：說明本文研究動機、目的與範圍。

第二章 傳統營業秘密之立法例：介紹美國傳統營業秘密之法規-侵權行為彙編與統一營業秘密，分析其營業秘密之定義、侵害行為態樣等規範，以利深入瞭解美國關於營業秘密保護之法律發展。

第三章 美國經濟間諜法之研析：介紹該法之立法背景，說明其規範內容，並就法律層面分析該法於規範與執行上之優劣點。該法對於商業活動與關係人可能產生之影響亦提及之。

第四章 各國立法與理論之比較：列舉介紹我國、日本、德國等關於保護營業營業秘密之規範，並與經濟間諜法法比較其相異處，分析未來營業秘密保護可能發展之趨勢。

第五章 案例分析：列舉若干以該法起訴之案件，並分析永豐案之判決，以更深入了解該法執行上之問題。

第六章 美國經濟間諜法之因應對策-暨結論：本章分別就政府與業者兩方面，援引外國企業經驗提供因應經濟間諜法之對策，期能避免誤觸該法，並培養我國業者主動保護自身營業秘密之意識。

目次

第一章 緒論	1
第一節 研究動機	1
第二節 研究目的	3
第三節 研究範圍	3
第二章 傳統營業秘密保護之立法例	5
第一節 侵權行為法彙編	5
第二節 統一營業秘密法	10
第三節 小結	14
第三章 美國經濟間諜法之研析	16
第一節 經濟間諜法之立法背景	16
第二節 經濟間諜法內容之分析	22
第一項 保護客體	23
第一款 營業秘密之定義	23
第二款 營業秘密之要件	26
第二項 犯罪類型	32
第一款 經濟間諜罪	33
(Economic Espionage)	33
第二款 竊取營業秘密罪	36
(Theft of Trade Secret)	36
第三項 侵害行為	39
第四項 法律責任	45
第一款 刑事責任	45

第二款 民事責任	47
第五項 域外管轄	48
第六項 維持資訊之秘密性	50
第三節 經濟間諜法之研析	52
第一項 與傳統營業秘密保護之比較	52
第二項 刑事追訴之優劣	55
第三項 對商業活動之影響	59
第四項 對關係人之影響	59
第四章 各國立法與理論之比較	63
第一節 各國立法與理論內容之分析	63
第一項 德國	63
第二項 日本	71
第三項 台灣	79
第二節 與經濟間諜法之比較	92
第五章 案例分析	96
第一節 起訴案例之介紹	96
一、United States of America V. Patrick and Daniel Worthing (Criminal No.97-9, W. D. Pa. December 7,1996)	96
二、United States of America V. Kai-Lo Hsu, et., (Criminal No.97-CR-323,E.D.Pa.)	96
三、United States of America V. Pin Yen Yang et., (Criminal No.97 CR288,N.D.Ohio September 4,1997)	97
四、United States of America V. Steven Louis Davis, (Criminal No.97-00124,D.C.M.D.Tenn,1997)	98
第二節 永豐案判決之評析	99
第三節 小結	103

第六章 美國經濟間諜法之因應對策-暨 結 論

.....	105
第一節 前言	105
第二節 業者因應之建議	106
第一項 營業秘密管理制度	108
一、內部資訊之管理	108
二、人事管理	110
三、成立智權單位	115
四、企業合作聯盟	115
第二項 引進國際技術之注意事項	116
一、確認移轉標的	116
二、主動質疑技術來源之合法性	117
三、確認合作主體	119
四、簽署保密協定	120
五、專家協助	121
六、技術引進書面化	121
七、損害賠償	121
第三節 政府之協助	123
一、建置智慧財產權諮詢服務	123
二、定期舉辦法規研討會	124
三、培養高科技素養的法律人才	124
四、結合政府及民間部門共同推動智慧財產權之管理及保 護	125
五、協助訴訟	125
六、修改法令	126
第四節 結論	127

參考資料131

附錄 140

第一章 緒論

第一節 研究動機

智慧財產權之保護原本屬於一國國內法之範疇，然由於世界經濟相互依賴、商品之跨國界流動之情況下，遂使智慧財產權不再僅被視為創作人之報酬與鼓勵研發之刺激，而轉變為「貿易資本」，及取得國際市場優勢地位之工具¹。因此各國政府為了提昇其業者之國際競爭力，除了鼓勵其從事技術之研發或提高研發之投資外，並且對於此等智慧財產提供法律保護，以健全其國內經濟之發展。然而隨著新興技術與產業的推陳出新，縱使專利權、著作權等傳統智慧財產權不斷被賦予時代意義，以擴充其權利內涵，但擴充畢竟仍有界限，在適用上不免會出現法律上盲點。因此各國逐漸承認其他類型的智慧財產權，在世界貿易組織架構下「與貿易有關之智慧財產權」協定(the Agreement on Trade-Related Apects of Intellectural Property Rights，以下簡稱 TRIPS)，遂將智慧財產權的範圍予以擴大，其中第39條第二項便對於「未經揭露之資訊」明文予以保護。

近年來因全球產業競爭白熱化，高科技產業不斷發展，在全球市場持續增加的價值與相對流通、擴散下，造成經濟間諜與竊取營業秘密行為的動機與機會均大幅提昇，因此外國政府、犯罪組織、竊賊等利用各種非法方式取得個人或企業價值昂貴之營業秘密之情事層出不窮。美國科技發展領先全球，相對的提高了受侵害

¹ 張心梯，「智慧財產權保護之法律經濟分析」，律師雜誌，第211期，第33頁，民國88年4月。

之程度。過去由於保護營業秘密的基礎係源於侵權行為或契約理論²，侵害行為人所需負擔之法律責任僅為民事賠償，然此對於惡意侵害他人營業秘密者仍無法達到嚇阻之效果，嚴重影響正常的商業行為，甚而間接波及國家經濟安全。有鑑於此，美國為維護其企業國際競爭力、保護經濟安全與建置商業倫理，遂於1996年立法通過經濟間諜法，明文將營業秘密的保護納入聯邦法。該法除了對於營業秘密、侵害行為加以定義外，更有別於過去州法或統一營業秘密法對於侵害營業秘密之行為人僅有民事責任，該法修正為科以嚴刑峻罰，以向全球昭告美國保護營業秘密之立場，作為美國企業保護營業秘密與嚇阻營業秘密侵害之利器。

由於我國業者對於該法並未特別注意，直到1997年6月永豐紙業公司顧問徐凱樂與國立交通大學教授何小台被美國聯邦調查局逮捕，並被控意圖竊取美國必治妥施貴寶公司(Bristol-Myers)抗癌藥物汰癌勝(Taxol)的配方而違反經濟間諜法；相繼不到四個月，四維膠帶公司負責人楊斌彥與其女楊惠珍亦被控涉嫌竊取美國艾佛瑞·丹尼森公司(Avery Dennison Corporation)有關製造膠帶的營業秘密，同樣違反經濟間諜法。兩起案件不但使得國內業者對於該法有所察覺，且從其起訴事實觀之，也不免發現國內業者在從事技術移轉工作之際，可能產生之疏忽與對他國智慧財產權法律知識的欠缺，因此深入瞭解經濟間諜法之規範內容，與分析我國廠商遭起訴之永豐案，即為本文研究動機。

² 湯明輝，「營業秘密保護理論之探討」，律師通訊，第163期，第62頁，民國82年4月。

第二節 研究目的

為了加速我國經濟快速發展，企業界莫不積極運用各種方法以強化競爭力，其中以與他公司從事技術合作或技術授權為最快速且最有效之方式，而美國便是我國企業主要技術來源之一。值得注意的是，經濟間諜法通過後，國內業者在與美國企業從事技術移轉時，將面臨潛在之法律風險，因此我國業者應該加強對於該法律規範之認識，免於因不熟悉該法而誤觸之。故本文將針對經濟間諜法之規範內容、特色、執行上措施並配合與我國業者有關之案例進行說明、分析，最後並嘗試提出業者與政府因應之策略，期能使業者對該法所可能產生之法律問題有所瞭解，並能有效地執行因應之對策，以避免日後重蹈永豐案與四維案之覆轍。

第三節 研究範圍

本文擬以經濟間諜法之規範內容為主要架構，並輔以美國傳統保護營業秘密之立法體例，分析經濟間諜法之特色與其立法發展之沿革。再者，介紹其他國家有關營業秘密之保護立法例，並與經濟間諜法相互比較其相異處，並分析營業秘密在國際間未來可能之立法趨勢。最後，分析若干以經濟間諜法起訴之案例，以作為殷鑑，並提供政府與業者因應對策之建議。為此，本文各章內容說明簡述如下：

第一章 緒論

說明本文研究動機、目的與範圍。

第二章 傳統營業秘密之立法例

介紹美國傳統營業秘密之法規-侵權行為彙編與統一營業秘密，分析兩者對於營業秘密之定義、侵害行為態樣之認定等規範，以利深入瞭解美國關於營業秘密保護之法律發展。

第三章 美國經濟間諜法之研析

說明美國經濟間諜法通過之立法背景，並論及其內容之規範，包括營業秘密之定義、犯罪類型、侵害行為之認定與法律責任與域外管轄等規定，並就法律層面分析經濟間諜法關於規範與執行上之優劣點，且說明本法對於商業活動與關係人，例如所有人、員工或顧問等方面可能產生之影響。

第四章 各國立法與理論之比較

列舉介紹我國、日本、德國等有關保護營業營業秘密之法規範，並與經濟間諜法相互比較其相異處，分析未來營業秘密保護可能發展之趨勢。

第五章 案例分析

列舉若干以經濟間諜法起訴之案件，並針對我國永豐案之判決分析其爭點、主張、判決、理由，以求能更深入瞭解經濟間諜法執行上之問題。

第六章 美國經濟間諜法之因應對策-暨結論

本章分別就政府與業者兩方面，援引外國企業經驗提供因應經濟間諜法之對策，期能避免誤觸該法，並培養我國業者主動保護自身營業秘密之意識。

第二章 傳統營業秘密保護之立法例

美國關於營業秘密保護制度原非建立在聯邦法的體系，而是各州依據普通法之精神制訂法規。法院判決之基礎主要來自於二大法源，一為侵權行為法彙編(Restatement of Torts)，一為統一營業秘密法(Uniform Trade Secrets Act)，二者對於營業秘密之定義、侵權行為之態樣均建立了原則性之判斷標準，對於日後經濟間諜法之制定有相當大的影響。本節將分別簡述侵權行為法彙編、統一營業秘密法之制定背景、營業秘密的定義與侵害行為的認定等相關規範，以深入瞭解美國在營業秘密保護立法上的沿革與發展。

第一節 侵權行為法彙編

侵權行為法彙編(以下簡稱為彙編)為美國法律學會侵權行為法委員會(The American Law Institute)於1939年彙編而成。其中，第三十六章第757-759條及註釋便規定營業秘密之定義及侵害行為之態樣。惟因侵權行為法彙編對於此等不公平競爭行為之規範力日益減弱，故美國法律協會遂於1978年刪除包括營業秘密在內之相關規定¹。因彙編對於營業秘密所為之定義與侵害行為之說明，仍為各州所採納，頗具參考價值，故本文仍引用之，藉以能更瞭解美國保護營業秘密之法律沿革。以下分別就彙編中關於營業秘密之規定說明之：

一、營業秘密之定義

¹ 「營業秘密法律保護之研究」，行政院科技顧問組委託辦理，第20-21頁，民國80年5月。

依據彙編第757條註釋B對於營業秘密之定義為：「營業秘密可涵括任何配方、模型、設計或資料之編纂，且給予擁有該資訊者較不知或不使用之競爭者獲得佔優勢之機會，它可以是一種化學混合物之配方；製造處理與保存物料之方法；機械之模型或其他顧客名單，與其他營業秘密資訊不同，營業秘密並非處理業務上單一或短暫之資訊，例如某一契約秘密投標之數額或其他條件、特定受僱人之薪資、已為或預定將為之證券投資、宣佈一項新政策或推出新樣品之日期。營業秘密，係事業經營上持續使用之程序或方法，其通常與商品之生產有關，例如生產物品之機器或配方，然其亦可能涉及商品之銷售或其他事業之經營諸如決定價格表或目錄上折扣或其他讓步之代碼、特殊化顧客名單、簿記或其他辦公室管理方法」²。依據該定義及註釋B分析營業秘密之要件如下：

1. 秘密性

秘密性為成立營業秘密最重要且為本質所需具備之要件。依據彙編註釋B之說明：「營業秘密之客體必須具秘密性。已為公眾所知或廣為業者所知之事務，不能做為個人之秘密」³。此所謂秘密性為相對秘密，非指絕對秘密，即該資訊在有限度之範圍內為特定關係人，例如為受僱人或合夥人所知悉者，仍不失其秘密性。此外，為符合該要件，營業秘密所有人主觀上除了將其視為秘密外，尚須採取合理之保護措施，以維護其秘密性。

2. 新穎性

² 林嘉彬，「營業秘密之概念及其侵害行為類型之研究」，輔仁大學法律研究所碩士論文，第53-54頁，民國83年7月。

³ 同前註2。

已為公共所有者，不能再為任何人所獨佔。故營業秘密所保護的對象僅限於某種未為一般大眾所共知的構想或資訊。且此處之新穎性並非如專利權等嚴格，而僅須達非一般人週知之程度即可，故營業秘密之新穎性係針對資訊而言，非對其物理之特性。

3.具體性

彙編雖未指出營業秘密須具體、明確，但基於普通法不保護單純構想與抽象事務之原則，因此尚在實驗中、發展階段的資訊或構想則無法受到保護。

4.商業上之價值

營業秘密之價值係源於所有人「因擁有該資訊者較不知或不使用之競爭者獲得佔優勢之機會」。此外，彙編同時要求該資訊須運用於商業上始足當之。

5.繼續性

營業秘密係事業經營上持續使用之程序或方法，故營業秘密應具備繼續使用之要件。若僅為短暫、單一價值之資訊，例如投標之數額、推出新樣品之日期等，遂被排除於彙編保護範圍之外。

二、侵害行為

彙編中規範營業秘密侵害行為之類型有二，一為洩漏或使用他人營業秘密(第757條)，一為以不正手段取得資訊(第759條)，以下分別說明之。

(一)洩漏或使用他人營業秘密：

依據第757條規定，「未經允許洩漏或使用他人之

營業秘密，有下列情形之一者，即應負責：

1. 以不正當手段取得營業秘密者；或
2. 其洩漏或使用他人之營業秘密，構成信賴義務之違反；或
3. 自第三人獲知該秘密時，知悉該資訊為秘密，且知悉第三人以不正當手段取得或違反義務取得；
4. 獲知該秘密時，明知該資訊為秘密，且知悉他人之洩漏係基於錯誤者。」

本條規制之行為態樣為「洩漏」和「使用」兩者，若僅單純不法取得他人營業秘密，而未予以洩漏或使用者，則不在本條禁止之列，而應適用第759條之規定。本條之要件除了必須無權使用或洩漏他人之營業秘密外，尚需具備該條各款情形始足當之，以下分述之：

1. 以不正當手段取得營業秘密者

所謂不正當手段，法無明文。依據該條註釋F之說明，係指低於一般商業道德或合理行為所能接受之標準而言，例如竊盜、不法侵入、以詐欺方式引誘洩漏、脅迫、暗中私下抄襲複製、產業間諜以竊聽或電子監控之方式取得等均屬之。此外，此處並不以帶走有形文件為限，倘若以記憶之方式取得者，因其與複製、拍照或攜出資料等在不當性之評價上並無實質差異，故同屬不正當手段。

2. 其洩漏或使用他人之營業秘密，構成信賴義務之違反

成立本款之先決條件需行為人與營業秘密所有人

間存在信賴關係，基於雙方之信賴，營業秘密所有人將秘密揭露予行為人，行為人即負有不擅自洩漏或使用之義務，一經違反該信賴義務，自有本款之適用。但值得注意的是，營業秘密所有人必須證明行為人認識其揭露係基於信賴關係所為，若行為人欠缺此認識，或表明不願承擔此信賴義務時，則信賴關係無由產生，自無本款之適用。至於信賴關係之產生，其方式有二，一為契約明示或默示之約定，另一為法律所擬制，例如代理關係、僱傭關係或其他商業關係之當事人間所產生之信賴關係。

3.自第三人獲知該秘密時，知悉該資訊為秘密，且知悉係第三人以不正當手段取得或違反義務而取得

成立本款者，行為人需同時認識：(1)明知該資訊為秘密，(2)明知第三人以不正當手段取得或第三人之洩漏係違反對他人之義務。例如甲不法取得乙之營業秘密後，出賣給知情之丙，若丙於事後將之洩漏或使用，即須依本款負責。

4.獲知該秘密時，明知該資訊為秘密，且知悉他人之洩漏係基於錯誤者

本款係導源於誠信原則。因錯誤而取得營業秘密之人，不論錯誤是因如何所致，只需行為人知悉該資訊為他人之營業秘密，且認識該錯誤之事實，則基於誠信原則，便不得利用此錯誤而圖利自己。

而同法第758條則係規範善意取得營業秘密之第三人之責任，亦即善意取得人應否負責，須視其事後是否知悉不法情事存在、有無支付對價及地位是否變動而定。

(二)以不正當手段取得資訊

依據第759條規定：「為提高商業競爭力，而以不正當手段取得他人營業之資訊者，應就其占有、洩漏或使用該資訊，對該他人負其責任。」

本條並非專以營業秘密保護為主，而係將「與營業有關之秘密性資訊」均列為保護之客體。本條在適用上應注意的是，本條規定僅為前述第757條之補充規定，即僅在無法依據第757條處理時始有本條之適用。因此，本條之適用應限縮為「以不正當手段取得營業秘密後之持有行為，而未予洩漏或使用者」。

第二節 統一營業秘密法

有鑑於侵害營業秘密之問題逐漸增加，各州立法規範不一，造成營業秘密保護適用上之困擾，故制定統一法將營業秘密法典化之議遂應運而生。此意見隨後為統一州法全國委員會議所採納，在統一營業秘密保護法特別委員會歷經10年的研究、審議後，終於在1979年批准統一營業秘密法，並建議各州採用⁴。根據統計，目前已有42州和哥倫比亞特區以之為基本架構，制定其營業秘密法⁵。統一營業秘密法雖僅有12條條文，但其對於營業秘密之定義、侵害行為之態樣與民事救濟均有所規定，也影響到日後經濟間諜法中若干規定，可見其重要性。

⁴ 馮震宇，「從美國經濟間諜法案論外國立法例對營業秘密之保護」，工業財產權與標準，第54期，第6-7頁，民國86年9月。

⁵ 馮震宇，「從永豐判決論美國經濟間諜法之適用」，萬國法律，第107期，第3頁，民國88年10月。

以下就其內容分述之。

一、營業秘密之定義

依據統一營業秘密法第一條第四款規定營業秘密之定義為：「營業秘密係指情報，包括處方、型式、編輯、程式、裝置、方法、技術或過程等，均得為營業秘密之標的，且：

- 1.其獨立之實質或潛在之經濟價值，來自於非他人所公知且他人無法以正當方法輕易確知，而其洩露或使用可使他人獲得經濟上之價值。
- 2.已盡合理之努力以維持其秘密性。」

由此定義可知，成立營業秘密之要件，有秘密性、獨立經濟價值與合理之保密措施三者。其中關於秘密性之意義與侵權行為彙編相同，於此不再贅述。就獨立經濟價值而言，侵權行為彙編以營業秘密須具有實質之經濟價值為限，蓋早期法院見解認為，若某一資訊並未在商業行為中加以利用，因於訴訟中無法計算被害人遭受不法行為所受之損害，自無法承認該資訊為營業秘密法規所保護之客體。惟該見解是經不起挑戰的，蓋系爭資訊是否為營業秘密與訴訟時能否計算損害賠償，應該分別視之⁶，故統一營業秘密法除了刪除了彙編之繼續性與在商業上使用兩要件外，對於尚在實驗室或發展中之資訊，即「具有潛在之獨立經濟價值」之營業秘密一併列入保護之範圍。是故，統一營業秘密法對於營業秘密之認定標準更具彈性。

二、侵害行為

⁶ 張靜，「我國營業秘密法介紹」，<http://www.moeaipo.gov.tw/nbs12/ipo3a.htm>

統一營業秘密法對於營業秘密侵害行為，分別於第一條第一項、第二項就「不正當手段」與「侵害行為」為定義性的規範，茲分述如下：

(一)不正當手段

係指竊盜、賄賂、不實表示、違反保密義務或引誘他人違反此種義務，或經由電子或其他方法之間諜行為。

本法以明文規範「不正當手段」之態樣。然此定義性規定僅為不正當手段之例示規定，非謂其僅以條文所列舉者為限。

(二)侵害行為，係指：

- (1)明知或可得而知以不正當手段取得他人之營業秘密；
- (2)下列之人，未經明示或默示同意而洩漏或使用他人之營業秘密；
 - (a) 使用不正當手段取得營業秘密；或
 - (b) 使用或洩漏營業秘密，明知或可得而知下列情況：
 - ①來自或經由利用不正手段取得營業秘密之人取得；
 - ②經由有義務保持秘密之人或有限制使用義務之人取得；
 - ③來自或經由受到禁止命令而富有保密義務及禁止不得使用營業秘密之義務之人取得；

(c) 在其地位實質變動前，明知或可得而知該資訊為營業秘密，且係基於意外或錯誤而取得。

由此規定可知，本法規範之行為係由「取得」、「使用」和「洩漏」三者所構成。與侵權行為彙編相較，不難看出，本法對於「洩漏」和「使用」行為之規範，係延續前者之架構，不同之處僅在於統一營業秘密法更周延地將「取得」行為一併納入，亦即結合前者第757條與第759條之規定。

除上述二項差異外，大抵上統一營業秘密法與侵權行為彙編對於營業秘密侵權行為之架構是相同的，因此可將美國傳統營業秘密之侵害行為歸納為四種侵害類型：

1. 不當取得營業秘密(彙編第 757 條第 1 款、第 759 條，UTSA 第 1 條第 2 款(1))
2. 違反當事人間信賴關係之洩漏或使用之行為(彙編第 757 條第 2 款)
3. 知悉營業秘密係他人不當取得或洩漏而仍予使用(彙編第 757 條第 3 款、UTSA 第 1 條第 2 款(2))
4. 知悉營業秘密係他人基於錯誤而仍取得者(彙編第 757 條第 4 款)

三、救濟

統一營業秘密法對於營業秘密之侵害係採取禁止命令(第二條)與金錢賠償(第三條)之救濟方式。

就禁止命令而言，依據該法第二條第一項之規定：「對於現實或將發生之盜用可加以禁止。基於對法院之

申請禁止命令應於營業秘密不再存在時解除，但禁止命令可於其他合理期間內存續，以防止因盜用獲致營業上利益。」法院核准原告之申請頒發禁止命令之目的，係在於消除因盜用營業秘密所取得之競爭利益，並避免營業秘密所有人之「領先時間」遭到縮減⁷。由於美國賦予法院以強制禁止命令作為救濟行為，通常限於「不適合以貨幣計算其損害」，而相對競爭利益往往不容易計算，故禁止命令便成為最常使用之救濟手段⁸。

至於在金錢賠償部份，依據統一營業秘密法第三條第一項之規定，被害人所得請求之損害賠償，可依原告因被告之竊盜所致之現實損失，與被告因竊盜而取得之不當得利來計算其賠償標準，此稱之為補償性損害賠償⁹。再者，若被告盜用係基於故意與惡意時，原告亦可向法院要求懲罰性損害賠償。但不得逾補償性損害賠償額之二倍。

第三節 小結

比較侵權行為法彙編與統一營業秘密法，可以發現兩者之差異在於，統一營業秘密法除了刪除了彙編之繼續性與在商業上使用兩要件外，對於尚在實驗室或發展中之資訊，即「具有潛在之獨立經濟價值」之營業秘密一併列入保護之範圍。因此縱使為使用一次之市場調查，或仍在開發中、試驗階段之新產品均得以營業秘密

⁷ 馮震宇，「了解營業秘密法-營業秘密法的理論與實務」，永然文化股份有限公司，第314頁，民國87年7月初版。

⁸ 經濟部商業司編著「營業秘密保護制度之研究」，第37頁，民國81年12月版，轉引自曹永遊撰「論專門技術在我國營業秘密法之保護」，中興大學法律研究所碩士論文，第152頁，民國86年7月。

⁹ 同前註，第156頁。

之形式獲得合法之保障，因此，統一營業秘密法對於營業秘密之認定標準較侵權行為法彙編更具彈性¹⁰，其規範內容遂成為日後經濟間諜法立法之參酌，益見其重要性。

由於不公平競爭與交易規範已不再倚賴侵權行為法，並轉而較廣泛之成文法發展，故侵權行為法彙編遂於第二次修正中刪除了上述營業秘密之相關規定；再者，統一營業秘密法雖然承襲侵權行為法彙編保護營業秘密之意涵與架構，截至目前為止，已有42個州和哥倫比亞特區以之為基本架構，制定其州營業秘密法。但統一營業秘密法和各州營業秘密法在處理侵害案件仍存在若干困境，例如無法有效遏止跨州竊取營業秘密行為、外國經濟間諜行為等。職是之故，以聯邦法保護營業秘密立法之呼聲甚高，經濟間諜法遂應運而生，將是下一節所欲討論之立法背景。

¹⁰ 參見徐遵慈，「論營業秘密保護之立法及其與不正競爭之關係」，東吳大學法律學研究所碩士論文，第 23-24 頁，民國 84 年 7 月 18 日。

第三章 美國經濟間諜法之研析

第一節 經濟間諜法之立法背景

美國每年花費近1500-2500億美元的經費在科技研發工作上，遠勝於世界其他國家，因此對美國而言，研發技術與資訊不但為其政府和私人企業創造競爭商機，更使得美國得以居於高科技資訊的領先地位¹。然而冷戰結束後，美國政府調查發現某些廠商不思正道，運用商業間諜，以直接侵入目標公司竊取情報、侵入企業電腦網路，或要求留學生刺探美國科技情報²，或透過收買企業內員工，或甚至由外國情報機構直接或間接，參與或主導經濟間諜活動³等方式不法獲取其技術或資訊的案件急遽增加。以美國全美工業安全協會(American Society for Industrial Security, ASIS)對於1992至1995年所為之調查報告為例，美國企業遭受智慧財產權侵害之案件，已經從1992年每月平均9.9件，增加到1995年平均每月32件，三年內增加323件，而所受的損害則每年達2400億美元。在這些侵害案件中，60%是策略性計畫(Strategic Plans)、研發(Research and Development Information, R&D)與製程(Manufacturing Processes)方面之資訊，也就是營業秘密法所保護之資訊⁴。由於這些

¹ <http://www.nsi.org/library/comm/commpricrey.txt>

² 伊拉·溫克勒在其著作中便明白指出，中國大陸政府不乏利用海外留學生作為蒐集情報之工具，藉機竊取外國新科技或商業機密。Ira.Winker, "Corporate Espionage-What It Is, Why It's Happening in Your Company, What You Must Do About It", Prima Publishing, 1997。張沛元譯，大盜入侵-你不能不知道的企業間諜商戰實錄，商業周刊出版，第74頁，1998年初版。

³ 同前註，第67頁。

⁴ 美國聯邦調查局局長 Freeh 在 1996 年 2 月 28 日經濟間諜之聽證會上便提出 ASIS 於 1992

攸關企業發展與競爭成敗的資訊並非全部均能受到如專利法、著作權法等智慧財產權之保護，因此如何另外尋求法律全面保護此等科技資訊，以維持其國際競爭力與經濟利益，便成為美國政府與企業關注的話題。

美國國會曾舉行兩次主要的聽證會來考慮制定聯邦法律，以規範營業秘密竊取行為。其一為1996年2月28日由參議院情治人員遴選委員會暨參議院恐怖主義、技術以及政府資訊司法小組聯合召開，其中賓州參議員Arlen Specter與威斯康辛州參議員Herb Kohl聯名提出「工業間諜法案」(Industrial Espionage Act of 1996, S. 1556)與「經濟安全法」(Economic Security Act of 1996, S. 1557)兩項法案。儘管兩項提案就營業秘密之定義與罰則等略有不同，但其立法意旨均為保護美國企業於事州際或國際貿易中所使用或擁有之營業秘密，以免遭受不法侵害⁵。同年5月9日再度由眾議院司法委員會犯罪小組舉行公聽會⁶探討該議題。兩次聽證會的首要證人均為聯邦調查局局長 Louis J. Freeh，其明確地指出美國政府在處理經濟間諜行為的瓶頸與企業迫切需要聯邦立法之急迫性。從國會在前後兩次聽證會中詳細地記載經濟間諜法立法的三個主要支持論點：

1. 後冷戰時期，美國國內經濟發展的重要性與國家安全的重要性，兩者無分軒輊。
2. 外國力量基於其國內本身產業界之經濟利益，透過

年針對246家公司就智慧財產權遭受侵害之調查報告，以作為立法依據。Louis J. Freeh, "Hearing on Economic Espionage", <http://www.fbi.gov/congress/econom/ecespion.htm>, 2. 28. 1996.

⁵ "Economic Espionage Legislation-Introduced in the Senate", adopt from <http://www.nacic.gov/cind/cind196.htm>

⁶ <http://www.securitymanagement.com/library/000/91.html>

各種方法，積極地介入向美國政府或公司竊取重要的技術、資料以及訊息。

3. 現行法律包括州際傳輸盜用財產法 (Interstate Transportation of Stolen Property Act, 18 U.S.C. Sec. 2314) 郵件詐欺(mail fraud)或是通訊詐欺(wire fraud)等，確實無法有效地起訴經濟間諜。

針對第一點，Freeh引用1993年11月4日國會外交關係委員會國務卿克里斯多福(Secretary of State Warren Christopher)的發言，說道：「冷戰時期結束後，我國國家安全與經濟安全息息相關」，並引用總統柯林頓在1994年7月所發表的「國家安全政策」會報，指出美國經濟之復興與強大為新政策之目標之一，蓋國家安全係建立在強大的經濟基礎，而非軍事能力，此項論點於前蘇維埃共產體制瓦解之結果中更是獲得驗證。是故，經濟安全之維護與有助於國家利益之追求，更是國家安全重要之一環，因此政府有責任為保護國家經濟安全而制訂防制與懲罰之法律，以打擊竊取高科技或商業資訊之不法行為。

針對第二點，Freeh報告指出，在冷戰結束後，雖然前共產經濟體制瓦解，許多東歐國家訓練精良的軍事間諜突然面臨英雄無用武之地的窘境，然而其並不代表間諜行動因此而停止，反而有將經濟政策或計畫做為間諜行動目標之情形產生，以發展其國內企業之國際競爭力，相對地，藉以提昇國家本身在國際上的影響力。

為有效解決此等經濟間諜行為，FBI在1994年便逐步展開名為「經濟反情報計畫」(Economic Counterintelligence Program) 主要從事調查和制止經濟情報收集之活動。根據FBI 目前所調查的經濟間諜案件

指出，從1994年的400件至今已經倍增至800件，且有近23個國家被指控對美國從事經濟間諜行為，其中不但包括美國的長期對手，如蘇聯和中共，還包括一些美國的盟國，如日本、法國、德國等在內，均涉嫌從事經濟間諜活動。是故，由外國力量所主導之經濟間諜活動確實值得美國當局的重視。

經濟間諜行動之目標含括美國成功之各類高科技工業，例如生物科技、航太、通訊、建構國家資訊基礎建設、電腦軟體與硬體、先進運輸與引擎技術、尖端材料與塗料、能源探測、國防與軍備技術、製程以及半導體等。美國白宮科技室(The White House Office of Science and Technology Policy, OSTP)針對美國企業因外國經濟間諜行為所造成之損害，估計每年損失幾達三千億美元，並指出在近十年內因間諜行為將導致工作就業方面損失超過6百萬個工作機會⁷。

綜上所述，以外國政府力量所主導之經濟間諜行為，將影響美國在全球市場上的競爭優勢，直接或間接使美國國內、外遭受龐大的經濟損失，因此立法需要迫在眉睫。

針對第三點而言，Freeh局長指出，過去聯邦法律僅以複製權和專利來保護私有經濟資訊，並無直接針對經濟間諜行為或保護營業秘密的法案。可資適用之聯邦法規，包括有1934年所制訂的州際傳輸盜用財產法(Interstate Transportation of Stolen Property Act, 18 U.S.C. Sec. 2314)和聯邦法律有關郵件詐欺(mail fraud)或是通訊詐欺(wire fraud)之相關條文。就前者而言，該

⁷ "Economic Espionage: The Looting of America's Economic Security in the Information Age", adopt from <http://www.cmahg.com/infosphere/news/issues/issues-articles/issues-espionage.htm>

法僅明文禁止將所盜取之貨物、物品或商品 (goods, wares, or merchandise) 等有形財產運送越過州界，以規避各州的管轄權之情形。然而營業秘密此種無形之資產，法院認定其係競爭的商業資訊，並非為法條所規定的貨品、物品或商品⁸，且侵害營業秘密之行為在本質上並不當然需要實際上的傳輸，故礙於營業秘密之無形性與法條相抵觸，故無法引用該法條來制止經濟間諜竊取或侵佔營業秘密之行為。至於後者，主要係規範使用郵件或通訊裝置所從事之侵害行為。倘若被告並未使用郵件或通訊裝置方式從事侵害行為，則同樣無法以該法規範之。此外，聯邦刑法典第1905條亦規定聯邦政府受雇人不得不當洩漏於任職期間所知悉之機密，因其適用對象僅限於聯邦受雇人，不及於一般民眾，且違反該法之處罰僅為一千美元罰金，或一年以下有期徒刑，及終止聘僱契約，對於懲戒竊密行為之效力仍然有限。至於其他間諜法案，由於當初立法意旨係用於對抗冷戰期間之軍事間諜戰，實無法將其適用在現今頻繁的經濟情報蒐集活動。因此，在經濟間諜法通過前，聯邦檢察官並無法援引現有的聯邦法律有效地起訴經濟間諜或竊取營業秘密之行為。

關於州法而言，其仍然無法填補聯邦法關於保護營業秘密或經濟間諜之漏洞。誠如上一節所言，多數州採取美國統一州法委員會所制訂之「統一營業秘密法」以作為其立法之範本。惟就統一營業秘密法本身之缺點而言，因該法僅供各州立法參酌之用，並無任何拘束力，不足以拘束各州立法機關，故各州可以根據自身之考慮，作出與統一營業秘密法不同之規範內容。另一方

⁸ Dowling v. United State , 473 US 207(1985), <http://laws.findlaw.com/US/473/207.html>

面，統一營業秘密法僅有民事責任而無刑事處罰之明文，對於惡意侵害他人營業秘密者並無嚇阻之效果。相同的，以州法來保護營業秘密的缺點，也因多數州以統一營業秘密法為範本所制訂之州法僅提供民事訴訟程序與救濟，根本無法有效遏止侵害營業秘密之不法行為。縱使對於營業秘密的保護提供刑事懲罰的少數州，例如阿肯色州、愛達華州、紐約州、德州等，但刑事法部份仍鮮為法院所使用，或若牽涉該州刑事法，竊取營業秘密的行為僅被認定為微罪⁹。因此，就法律責任而言，以州法來保護營業秘密可謂為是悲慘的。此外，各州僅對其州境內所發生之侵害行為方有管轄權，若涉及二州以上之侵害行為，依美國憲法之規定則屬於聯邦法院管轄權之範圍。是以，州法並無法有效規範具有州際或國際性質之經濟間諜行為。囿限於州法對於此種新興侵害行為在適用與規範上出現盲點，再加上各州法院見解不一之情況下，反而成為業者於尋求法律救濟時之障礙。

除了受限於聯邦法與州法立法不足外，許多公司在遭受營業秘密侵害後亦多選擇放棄民事訴訟。原因有一為犯罪行為人通常為年輕的工程師而無索賠實益，或是外國政府或公司而難以求償。再者，公司除了欠缺調查資源或時間對於侵權行為人興訟之外，同時公司也缺乏證明被告竊取係爭營業秘密的能力；原因之三為公司一

⁹ Barry R. Shapiro, "Economic Espionage", Marketing management, Spring, p.56, 1998. 美國目前對於侵害營業秘密設有刑事制裁之州，包括 Alabama, Arkansas, California, Colorado, Connecticut, Florida, Georgia, Idaho, Inois, Indiana, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, New Hampshire, New Jersey, New Mexico, Ohio, Oklahoma, Pennsylvania, Tennessee, Texas, Wisconsin, Wyoming 等共計有 27 個州, adopt from <http://www.usdoj.gov/criminal/cybercrime/intell-prop-rts/app-l-m.htm>.

旦發生侵害事件時，通常採取不公開的態度，蓋其害怕將嚴重影響公司股票價格、顧客信賴度或有暴露自身的營業秘密之慮¹⁰。故制定聯邦專法以保護業者之營業秘密自有其必要性與急迫性。

故為了健全美國經濟與其國際競爭力，進而維護國家安全利益，有必要保護營業秘密的產生和發展，以免於受到不法之侵害，並為了補充現行法規不足，表現美國嚴懲外國機構侵害營業秘密行為之態度，參議院與眾議院嗣於1996年9月28日修正S.1556 與S.1557兩法案，通過「一九九六經濟間諜法」(Economic Espionage Act of 1996, H.R.3723)法案，並送請柯林頓總統於同年10月11日簽署生效。

第二節 經濟間諜法內容之分析

從上述立法背景可知，美國政府體認到企業若欲保有競爭優勢便在於兼備各種智慧財產權。為了維護商業倫理、保護其企業永續發展與國際競爭力，防止外國政府或企業利用不法之方式獲取美國廠商之營業秘密，國會遂立法通過經濟間諜法，明文對於營業秘密提供聯邦法之保護，脫離以往營業秘密為州法保護之體系，並填補原有法律適用上之缺失，使得美國對於營業秘密之保護產生結構上之變化。

經濟間諜法中較引人注目之條文為第1831與1832條，蓋其不但依據侵害目的不同，而將侵害類型區分為外國政府或機構而竊取美國營業秘密之經濟間諜罪，與

¹⁰ "Economic Espionage Explosion", Security, p.18-19, May, 1998.

民間企業間經常發生之竊取營業秘密罪兩種，並且明確訂出五種侵害行為之態樣，讓營業秘密侵害之認定問題獲得有效解決。再者，本法與傳統民事救濟方式不同之處，即首次對於侵害營業秘密者課以刑事責任，使得欲侵害他人營業秘密者之法律風險從過去單純的民事責任，擴大為刑事責任。第三，本法更將適用範圍擴大至美國領域外，此種廣泛之管轄效力，將使得企業向美國挖角或與美國從事技術貿易時，增加涉案的法律風險。

隨著國內產業發展逐漸偏向高科技產業，美國也成為我國企業主要技術來源之一，因此如何在技術合作與技術移轉之際，加強對經濟間諜法內容之瞭解，以規避該法所可能產生之風險，將是國內業者與研究機構必須正視之挑戰。本節便從保護客體、犯罪類型、侵害行為之態樣與其他重要規定，依次加以分析說明之，以求深入瞭解經濟間諜法之規範內容。

第一項 保護客體

經濟間諜法所保護之客體為營業秘密，由於與其他同以營業秘密為保護客體之法規，例如美國侵權行為彙編 (Restatement of Tort) 與統一營業秘密法 (Uniform Trade Secret Act) 中關於營業秘密之定義、要件等方面，均有共通之處，因此本文將引用此等法律之相關規範，以作為解釋或互為對照本法之工具。再者，由於經濟間諜法對於侵害營業秘密行為人課以嚴苛之刑事責任，故有必要針對營業秘密之性質、定義和要件逐一分析，使保護之範圍明確化，進而確保犯罪者之合法權利。

第一款 營業秘密之定義

對於是否產生侵害營業秘密之情事，首先面臨的問

題，便是判斷系爭之資訊是否為營業秘密。營業秘密之定義，在經濟間諜法制訂之前，聯邦並未有營業秘密保護之專法問世，因此各州或有參酌統一營業秘密法之架構，來制訂營業秘密保護法。惟此畢竟是各州依其自身情況所為之規定，關於營業秘密之定義皆屬於廣泛性、原則性，且定義不一，至於何種秘密始屬於受法律保護之營業秘密，仍須由法院依實際案例判斷。在經濟間諜法制訂之前，法院本於侵權行為彙編與統一營業秘密法之規範意旨，大多會斟酌下列因素，作為判斷該資訊是否為營業秘密之標準¹¹：

1. 於研發該營業秘密時，所付出之時間、金錢及勞力之多寡。
2. 該項秘密之新穎性，即是否為大眾或其他商業競爭者所知。
3. 營業秘密所有人為維護秘密所為之努力。一般而言，企業為保護資訊之秘密性所採取的保護措施越嚴密，則該資訊就越可能成為得受法律保護之營業秘密。
4. 該資訊在營業秘密所有人營業內被員工及相關人員知悉之程度如何。若知悉該資訊之員工或其他人士越多，該資訊能受到營業秘密保護之可能性越低；相對的，若知悉的人越少，則該資訊受到保護的可能性也就越高。

¹¹ 張凱娜，「由近年國內發生之案例談企業保護營業秘密」，1997 全國智慧財產權研討會論文集，第 84 頁，民國 86 年。吳景源，「談營業秘密法關於營業秘密之保護」，萬國法律，第 107 期，第 19 頁，民國 88 年 10 月。

5. 第三者能透過正當管道取得該資訊的難易度如何。
6. 該營業秘密對營業秘密所有人及其競爭對手的價值如何。

經濟間諜法承襲了統一營業秘密法之規定，並配合上述營業秘密之判斷標準，首次以立法方式對營業秘密加以定義，消弭了過去因各州立法不一或個案所產生對於營業秘密名詞不一、涵義不一的問題。依據該法第1839條之規定，營業秘密係指「各種形式與類型之財務、商業、科學、技術、經濟或工程資訊，包括資料、計劃、工具、機制、組成、程式、程式碼或商業策略，不論其為有形或無形，亦不論其係以儲存、編輯、文字、或以物理性、電子、圖形或照相記憶，只要其符合：

- a. 此等資訊之所有人已針對情況採取合理措施以保護此等資訊之秘密性；
- b. 此等資訊由於未為一般大眾所知悉，或因公眾利用合法方式，無法即時確定、取得或發展出來，而具有現實或潛在之獨立經濟價值。」

本法關於營業秘密之定義與統一營業秘密法之規定相去不遠，且國會於立法報告中特別指出，上述定義之各種資訊類型，僅為例示規定，而非列舉規定¹²，更是使得保護之範圍幾乎涵蓋一切資訊。此外，立法者亦配合電腦資訊時代所衍生之資訊型態，例如該資訊係以電子、圖形或照相記錄等儲存者，一併納入保護之列，可見立法者有意將目前所存在或將來可能發生之所有

¹² Section670(c), <http://thomas.gov/cgi-bin/cpquery>

儲存營業秘密之方式及其他營業秘密存在之型態全部規劃進來¹³。因此本法意旨，對於高科技產品或資訊之保護實具有正面的貢獻，且較統一營業秘密法之規定更具完整性。

第二款 營業秘密之要件

營業秘密保護之取得並非如專利、商標法採取公示性的註冊主義或登記生效主義，而係該資訊具備營業秘密之各項要件後便自動地、持續地取得法律保護。是故，一定法律要件之具備係決定該資訊是否為本法保護之客體。本法第 1839 條將營業秘密定義予以明文化，使本法所保護客體之內涵與範圍不至於漫無標準，然在實際之案例中，是否可受到本法所保護，仍須符合下列要件：

一、秘密性

營業秘密，顧名思義，自然必須為一種秘密，故凡判斷某一資訊是否為本法所保護之對象，應以具有「秘密性」為第一要件。因此，倘若該資訊置於任何人均得接觸之狀態者，例如為學刊、期刊或網路上所公開之資訊¹⁴，則喪失其秘密性，非本法所保護之客體。此所謂

¹³ 鄭穎，「營業秘密侵害在刑事法上之研究」，中興大學法律學研究所碩士論文，第 31 頁，民國 87 年 8 月。

¹⁴ 以 RTC (Religious Technology Cor.) 公司之案例為例，由於 RTC 公司的營業秘密於遭受被告盜用之前，已經被他人張貼在網路上，為大眾所知悉，故 RTC 公司自不能再主張其對於營業秘密之權利，亦即已經由網際網路所揭露之資訊，將破壞其秘密性，無法成為營業秘密法保護之客體，(Religious Technology Cor. V. Netcom On-line Com., 923F. Supp.1231(N,D.Cal.1995)，轉引自林慧蓉，「論網際網路資訊安全與隱私權之保護以營業秘密保護為中心」，東海大學法律學研究所碩士論文，第 91-93 頁，民國 87 年 12 月。

「秘密性」，與統一營業秘密法同，係指相對性秘密，而非絕對或全然秘密性，亦即不以該資訊僅限於營業秘密所有人知悉為必要，倘為商業上之目的將該資訊告知於「業務上有知悉必要者」或「其他信賴關係者」，並與該特定關係人簽署或要求保密責任時，仍無損於該資訊之秘密性。

二、採取合理保密措施

承前段所述，秘密性為構成營業秘密要件之一，且營業秘密的經濟價值幾乎是全部建立在嚴密的持有關係上，一旦失去持有或為一定關係以外之人知悉時，秘密性亦隨之喪失，無法成為本法保護之客體。因此，秘密性的維持實為法院認定營業秘密之一項決定性因素。資訊秘密性之維持，除了資訊所有人在主觀上必須將該資訊視為秘密外，在客觀上尚有賴於所有人現實地採取積極、主動的保密措施，以維持其秘密性，避免外界知悉。

本法第 1839 條 (a) 中要求營業秘密所有人對機密之資訊應採取一定之「合理保密措施」，而「合理」乃為不確定之法律概念，如何方可謂為資訊所有人已為合理之保密措施，在適用上不無疑問。依據國會註釋 C 之說明，認為此所謂「合理」無須要求營業秘密所有人竭盡(absolute)所有可能之保密措施，蓋根本無法做到滴水不漏之程度。故應針對個案所爭執之資訊特質加以認定之，並無一定之限制或標準¹⁵，或有稱為在「特定情況下係屬合理」(reasonable under circumstances)¹⁶即足當之。對此法院在實際案例中大多會根據「資訊之價值

¹⁵ Section 670(c)

¹⁶ 林嘉彬，前揭文，第 70 頁。

或性質」、「現實所採取的措施」¹⁷並配合「企業規模」等相互衡量加以判斷。舉例來說，倘若某大企業之機密資訊，可以輕易地被公司較低階級之員工取得者，則該資訊將被視為未盡合理之保密措施，而無法受到本法之保護。

合理的保密措施，法既無明文，為具體說明其判斷依據，本文依據註釋 C 之意旨，並綜合過去學者及實務之見解，有下列措施可為判斷之依據¹⁸：

1. 雇用人是否設有物理之設備

例如文件之保存處所是否上鎖；保存之處所有無警衛、圍牆或其他保存設施；保存之處所與保存非秘密性資訊之處所是否分隔；在含有營業秘密之電腦終端機或硬碟容器等存取設備是否標示有「機密」字樣等警示用語。

2. 對於受雇人本身

例如受雇人進入公司時，所為之面試內容，秘密所有人是否與受雇人締結保密契約和禁止競業契約，並使其了解各項營業秘密保護之法規，且以安全手冊等書面資料宣導公司之保密政策；將某種資訊列為營業秘密之情況告知受雇人，並隨時提醒其保密之義務；將營業秘密區分為各等級，由不同階層之受雇人控制；對於接近營業秘密之人，須經過公司特別許可，且該人員必須作成書面記錄等。

¹⁷ "Federal Prosecution of Violations of Intellectual Property Rights", cited from <http://www.usdoj.gov/criminal/cybercrime/intell-prop-rts/SectV.htm>.

¹⁸ 參見徐玉玲著，徐火明主編，「營業秘密的保護公平法與智產法系列二」，三民書局，第 27 頁，民國 82 年 11 月初版。

3.對於公司以外之人是否設有保密之作業

例如是否對於訪客有所管制，以避免競爭者藉機滲透；工廠之參觀與否，以及參觀區域劃分之限制；與第三人進行營業秘密之交易時是否簽署保密契約或第三人接觸該營業秘密時是否告知其為專有營業秘密，以防止他人因不知情而洩漏其內容。

4.對於營業秘密本身是否盡力保護

如儲存營業秘密之軟體是否設定密碼，並隨時更新；含有營業秘密之文件或物品是否銷毀；傳送營業秘密之過程是否有加密措施等。

三、新穎性

所謂新穎性，有稱為「非周知性」，係指該資訊非已為公眾所周知或已為公共所有而言，故只要非一般且普通之知識經驗或技術即被認為具有新穎性。然營業秘密所具備新穎性之程度，依據1974年基華尼案(Keevane oil Company, V. Bicorn Corporation)最高法院之見

解¹⁹，認為「某種程度的新穎性係屬必要的，假如不具新穎性，即屬已為大眾知悉之事務；就營業秘密之範疇而言，秘密即隱含著最低程度的新穎性」²⁰，因此營業秘密所要求的新穎性程度，並不如專利權等嚴格²¹，僅以

¹⁹ Keevane oil Company, V. Bicorn Corporation, 416 U.S. 470, 40L Ed 2d 315,94s.t.1894(S Ct.1974)

²⁰ 湯明輝，「談美國營業秘密之構成要件」，公平交易季刊，第2卷第1期，第34頁，民國83年1月。

²¹ 專利法所要求係為「絕對新穎性」，即該發明或創作在未申請專利前，必須從未為公眾所知悉或使用而言。

具備最低程度的新穎性已足。又該要件係針對該資訊之秘密性，而非針對其物理性，故只須該資訊非公共所有，且其事實上被保持機密者，即可推斷其具有新穎性²²。

四、獨立之經濟價值

本要件係指欲成為可受保護之營業秘密，則該資訊必須給予擁有者較不知或不使用之競爭對手獲得優勢之機會而言。本法與統一營業秘密法相同，不以其具有實質價值為限，倘若該資訊對於營業秘密所有人具有商業經濟價值，縱然持有人並無行銷之計畫，或該資訊仍在研究發展，或是實驗室階段，尚未加以商業化推廣，亦即「潛在經濟價值」亦屬於營業秘密而受到法律之保護。換言之，其經濟價值不限於現在，縱使現在無經濟價值，但是未來有經濟價值者亦可受到保護²³。基於該法對具有潛在經濟價值之資訊加以保護之特性，將可使營業秘密與專利、著作權與商標等智慧財產權產生互補之效果，更能有效的保護研發成果²⁴。

再者，法律保障之範圍更擴大至「消極之資訊」，即「不成熟發展或努力」之經驗，本身雖未實際運用於企業中，但因可避免他人作無謂重複之努力，讓業者節省時間或經營之無效率，從而創造更高之經濟利益，故此項「不作為」之資訊，對於他競爭者而言，具有實質

²² 曹永遊，前揭文，第 74 頁。

²³ 馮震宇，「論美國經濟間諜法與營業秘密之保護趨勢」，1997 全國智慧財產權研討會論文集，第 70 頁，民國 86 年。

²⁴ 馮震宇，「資訊時代之新挑戰 論營業秘密之保護」，月旦法學雜誌，第 8 期，第 31 頁，民國 84 年 12 月。

之利益，故消極資訊亦為營業秘密保護之標的²⁵。職是，營業秘密存在與否，其判斷標準不在於是否實際使用，而是在於其有無價值。

本法關於營業秘密之經濟價值並未如州際傳輸盜用財產法(Interstate Transportation of Stolen Property Act, 18 U.S.C. Sec. 2314)之規定，對於所保護之客體必須有一定金額之限制²⁶。而其經濟性之具備與否，應由法院依據資訊之性質做決定。對此法院參考之基準有二：一為研發資訊所投注之努力與花費，另一為資訊在市場上之獲利能力。對此，法院可依據公開市場、黑市價格或其他合理方式決定該營業秘密之經濟價值²⁷。

此外，是否具備獨立之經濟利益，並非從犯罪者角度判斷，而係以營業秘密所有人觀點為依據，因此縱使所竊取之營業秘密對犯罪者無經濟價值可言，而所有人主觀上認為該資訊具有經濟價值者，則該資訊仍為本法保護之營業秘密。此推論係比較統一營業秘密法第一條第四項第一款而來，蓋前者規定營業秘密之洩露或使用可使他人獲得經濟上價值，而本法則規定此等資訊未為大眾知悉或取得即具有經濟價值，故經濟價值具備與

²⁵ 湯明輝，前揭註 20，第 37 頁。

²⁶ 依據該法之規定，其成立之要件有四，(1) 以竊盜、詐欺或傳輸等方式取得物品；(2) 被告不法傳送該竊取之貨物、商品或物品，且越過州際；(3) 竊取物之價值必須在美金 5000 元以上；(4) 被告明知其行為不法，其中第三要件中要求該行為客體必須有 5000 美元以上之價值，經濟間諜法則無此限制。18U.S.C.2314：「Whoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise securities or money, of the value of \$5000 or more, knowing the same to have been stolen, converted or taken by fraud」。

²⁷ United States V. Botton, 365 F.2d, 389 (2d Cir), 1996, 該判決中法院即主張被竊取之化學配方可依據歐洲藥品市場中業者欲購買之價格來決定其價值。

否，並不以犯罪行為人是否取得該資訊之經濟價值為斷²⁸。

綜上所述，某人所擁有之某項資訊（或稱為訊息、情報），必須同時具備秘密性、新穎性、獨立之經濟價值，及所有人採取合理之保密措施四大要件後始得成為經濟間諜法所保護之客體。

第二項 犯罪類型

誠如聯邦調查局局長 Louis J. Freeh 在 1996 年國會報告中所言，間諜活動自 1994 年的 400 件至今已倍增至 800 件。其中包括與美國對壘或盟國在內，有近 23 個國家正積極地竊取美國經濟或科技資訊。此種情形所造成之損失，根據美國白宮科技室之估計，每年可達 3000 億美元，於近 10 年內將導致超過 600 萬個工作機會喪失，進而危及美國在全球市場上的競爭力，直接或間接使美國內、外遭受龐大的經濟損失，影響國家經濟安全。此外，根據美國全美工業安全協會 (American Society for Industrial Security, ASIS) 所作的報告中指出，竊取營業秘密的犯罪類型，並非完全來自於外國個人或企業，反而在受侵害之受訪公司中有 3/4 為公司內部人員或與公司合作之團體竊取營業秘密所致，例如公司在職員工、離職員工、臨時雇員、共同投資者、關係企業等²⁹，順

²⁸ Linda K. Stevens, "The Economic Espionage Act, New Criminal Penalties for Trade Secret Misappropriation", <http://www.schiffhardin.com/econact.htm>。另參照馮博生，「營業秘密的定義及營業秘密法之保護客體」，<http://www.apipa.org.tw/apipa/b5/paper/tradesecret/ts3.htm>

²⁹ 根據 ASIS 報告指出外國涉案佔全指控案之 21%，74% 的指控案則為與公司有僱傭契約(在職員工或離職員工, 佔 59%) 或契約合作上關係(佔 15%) 的個人或團體所為，adopt from <http://www.fbi.gov/congress/econom/ecespionage.htm>.

手帶走公司機密資料，販售圖利，或是「帶槍投靠」為新公司效勞，或是自行創業。例如美國通用汽車集團控告其旗下德國歐寶汽車公司的離職主管荷西·洛培茲（Lose.Lopez）竊取營業秘密投靠對手福斯汽車公司³⁰，便屬於此類商業間諜侵害行為。

有鑑於犯罪態樣和侵害利益對象之不同，國會遂針對上述情形制訂兩種犯罪類型，一為外國政府、機構或單位刺探美國產業營業秘密的經濟間諜罪（第1831條），另一為一般企業界因競爭因素所出現的竊取營業秘密罪（第1832條），以下分別說明之。

第一款 經濟間諜罪

（Economic Espionage）

過去在冷戰時期，「間諜」原被定位為竊取軍事機密之情報人員，然而隨著冷戰的結束，間諜活動之目標逐漸擴大至工業或經濟機密，發生經濟間諜戰的情況。是以經濟間諜可定義為，由外國政府贊助，或由與外國政府對等的情報單位，針對美國政府、公司、協會或個人等，涉嫌以不法或秘密方式取得機密的商業、貿易、經濟政策、私有經濟資訊或技術者，或影響經濟政策決定或以之為目標者³¹。由於美國司法部一再強調「經濟安全」是國家安全重要之一環，且每年因外國政府和公司有計畫竊取營業秘密之行為已使得美國企業損失上千億之美金利潤，嚴重危及美國國家經濟安全。故特別

³⁰ General Motors Corpoyation V. Jose Ighacio Lopez de Arriortua, NO.96-71038(E.D.Mich), <http://www.nhold.com/hot/hh11.htm>

³¹ Edwin Fraumann, "Economic Espionage: Security Missions Refined", Public Administration Review, Vol.57, No.4, pp.304, July / August, 1997.

明文制訂經濟間諜之犯罪類型，用以打擊與嚇阻外國政府、機構及其代表對美從事經濟間諜法活動，並提供執行之正當性與法律責任之依據。

依據第1831條之規定，任何人(whoever)意圖或明知其行為將使外國政府、外國機構或是外國政府代理人受益(benefit)，而故意為該法所規範的五種侵害行為時，即為觸犯經濟間諜罪。準此規定，構成本條之要件如下：

一、該資訊符合營業秘密之要件；

該部份業於第一項說明分析，於此不再贅述。但值得注意的是，違反本條之罪，並未如第1832條規定營業秘密必須限於與產品有關或涵蓋於產品之內，因此縱使是獲取與產品無關之秘密，而只要為符合第1839條要件之營業秘密者，亦有本條之適用。

二、被告明知該資訊為他人所有之營業秘密；

一般刑事案件，檢察機關必須證明被告明知竊取者為他人所有之財產，意圖自己不法所有而竊取者。相同的，成立經濟間諜法之構成要件亦須被告明知該資訊為他人所有之營業秘密。惟系爭之資訊是否構成營業秘密之要件，不論是在民事或刑事案件均是辯論爭點所在，故限縮被告須明知該資訊為營業秘密，將可能成為被告脫罪之理由，無法有效以本法論罪，故有學者主張此處只須被告明知該資訊為他人所有而不法取得已足³²。又本法所處罰之意圖犯或共謀犯，因其本身具有可非難性，故法院主張僅須被告認為其所欲取得的資料為營業秘密已足，並不以該資訊實際為營業秘密為限，該見解

³² Linda. K. Stevens, Id..

也將放寬本罪之客觀構成要件，值得吾等重視之。

三、被告明知或意圖該資訊將使外國政府、機構或其代表受益；

行為人主觀要件只需具備使外國政府、機構或其代表受益之意圖已足，並不以該侵害行為「實際上」業已獲得利益為必要。此處並未如同法第1832條之規定，限制犯罪者必須具備意圖或明知其犯罪行為將使得營業秘密所有人受到損害為要件，此抽象危險性之認定也將擴大本法適用範圍。又本條「利益」範圍，依據美國國會註釋(Section 670(a))之說明，其與他間諜法條文相同，並未限於經濟利益，尚包括其他經濟以外之利益，例如有關預測(reputational)、策略(strategic)或戰術(tactical)之利益在內³³，因此本條圖利之範圍可說是相當廣泛。

本罪圖利之對象為外國政府、外國機構與外國政府代理人。其中，外國機構之範圍，根據第1839之定義，包括由外國所實質擁有、控制、資助、命令、經營或支配之任何單位、局處、部會、構成單位、機構、協會或任何法律及商業組織、公司、商號或其他實體。所謂「控制」，其並不以完全控制為限³⁴。根據此標準，由政府所贊助或控制之財團法人，或由政府與民間團體共同投資經營的企業，均有可能符合該項規定。以我國為例，工研院及生物科技中心等國家獎勵研發之財團法人，或中油、中鋼等公營機構，若將之認定為政府所資助或指

³³ Linda. K. Stevens, Id..

³³"Economic Espionage Act Criminalizes Trade Secret Theft" , <http://www.sf-law.com/espionage.htm>.

³⁴ 同前註。

揮之法人，則該機構之員工侵害美國企業之營業秘密時，便可能因其身份而成立第1831條之經濟間諜罪³⁵。這點與我國認知之協會、財團法人、基金會等隸屬於民間單位之概念不同，值得我國各單位或廠商注意。

至於外國代理人，根據第1839條之定義，係指一外國政府之任何官員、雇員、代理人、公僕、代表或議員。因此，具有公務員身份之人士均有觸犯經濟間諜法之風險。我國目前雖然與美國並無正式外交關係，然而我駐美代表仍可被定位為外國代理人³⁶，可知此處採取實質認定標準。

四、被告偷竊或未經授權等不法侵害該資訊；

本文將另於侵害行為中加以說明之。

第二款 竊取營業秘密罪

(Theft of Trade Secret)

本法雖然名為經濟間諜法，但並非僅侷限適用於對抗外國政府或公司。換言之，本法不但將焦點放在禁止竊取營業秘密而使外國政府受益之經濟間諜行為，同時也重視國內之商業競爭行為。本法於第1832條所規範之竊取營業秘密罪主要係規範企業間因競爭因素所產生的竊盜行為，其並不涉及外國政府、外國機構或外國政

³⁵ 在永豐案件之報導中即指出美國聯邦調查局最初便將生物科技中心與永豐公司一併列入調查之對象，並認為生技中心視為半官方之機構，「箭頭可能指向台灣官方」，聯合報民國86年6月21日第3版。

³⁶ 劉博文，「美國經濟間諜法簡介」，<http://www.moeaipo.gov.tw/nbs12/ipo3i.htm>

府代理人，故有稱之為企業間諜(Industrial Espionage)。條文中規定任何人意圖將為州際貿易或外貿而生產銷售之產品中的營業秘密，轉化為營業秘密所有人以外其他任何人之經濟利益，且明知此種行為對營業秘密所有人會造成傷害，而故意為侵害行為者即構成本條之竊取營業秘密罪，應按本條規定科以罰金(不超過25萬美元)³⁷，或科或併科10年以有期徒刑；若係法人團體違反此條竊取營業秘密罪，則可處以5百萬美元以下之罰金。準此規定，成立本罪之要件如下：

一、該資訊符合營業秘密之要件；

本條明文規定保護客體之營業秘密除具備本法第1839條之要件外，尚須限於「州際或國際貿易生產或銷售之產品之營業秘密」。此係源於本法為聯邦法，其侵害行為至少須屬於州際之行為或重大之犯罪方有聯邦之管轄權所致。再者，就該營業秘密須有關於生產或銷售之產品之要件，故本條可否適用於生產過程、服務或顧客名單等仍有待法院解釋。

一般而言，某資訊或技術是否為關於製造或生產產品之營業秘密，較容易被舉證，然倘若該營業秘密尚處於研究或發展之階段者，則較難以被舉證其係為州際或國際貿易而生產或銷售之產品中之營業秘密，蓋其未來是否成為州際之產品仍屬未定數。因此，研發中之製程或配方是否符合本條之規定應分別情形視之。即其倘與產品無關者，固不符合本條之保護要件，若與產品有關之秘密者，則應由檢察官舉證該秘密研發之最終目的係

³⁷ 18.U.S.C. § 3571(b) and (e), § 3559.

為州際間銷售之產品³⁸。

二、被告明知該資訊為他人所有之營業秘密；

本要件與第 1831 條之規定相同，於此不再贅述。

三、被告明知其行為將會損害所有人之權益，使自己或第三人取得更佳之經濟利益。

行為人主觀要件必須是明知(knowing)，亦即竊取營業秘密必須基於故意为之。是故，若僅因過失不知為營業秘密而使用者，則不構成本條之侵害行為。再者，成立本罪之犯罪意圖有二，一為行為人必須意圖使營業秘密之合法所有人遭受不利益，也就是行為人必須明知或可得而知其行為將會對營業秘密所有人造成某種之不利益，然此並不特別需要具有惡意的意圖(malice or evil intent)³⁹。二為意圖或明知其犯罪行為將使他人取得較營業秘密所有人更佳之經濟利益⁴⁰。該要件之目的在於保護無辜之第三者，若行為人非以使自己或第三人獲得經濟利益之目的而洩漏或使用者，或若僅係因錯誤或意外取得他人之營業秘密者，則不該當於第1832條之罪責。至於本條意圖圖利之範圍，相較於第1831條採取廣義解釋之圖利規定，本條所稱之圖利，則僅限於實質上之經濟利益(economic benefit)，並不包括抽象之利益。

四、被告偷竊或未經授權不法侵害該資訊；

此參見下節之說明。

³⁸ 同前註 17。

³⁹ Section 670(a)

⁴⁰ Ablondi, Foster Sobin & Davidow, p.c., "The Economic Espionage Act of 1996", p4-5, July 2, 1997.

第三項 侵害行為

為使侵害行為明確化，經濟間諜法特別明文訂出五種侵害行為的態樣。凡符合下列行為態樣者，便該當營業秘密之侵害，構成經濟間諜罪，以下分別說明之：

1. 竊取，或未取得適當授權而取得、攜去或隱匿，或以詐欺、詐術、欺騙等方法獲取此等資訊；
2. 未經授權而拷貝、複製、素描、繪畫、攝影、下載、上載、改變、毀損、影印、重製、傳送、交付、送交、寄送、通訊、或傳達此種資訊；
3. 明知該資訊係被竊取、盜用、或未經授權而取得或占有，而收受、購買、持有此等資訊；
4. 企圖實施任何(1)至(3)款所規定之任何行為；
5. 與一人或數人共謀實施(1)至(3)款所規定之任何行為，而其中一人或數人為達成其共犯之目標已著手實施。

從上述規定可知，經濟間諜法對侵害行為之方式不但包括傳統之竊盜類型，同時為配合營業秘密之無形性特質和電腦資訊化所衍生之新型態之犯罪方式，特別加入非傳統之竊盜方式，即在未剝奪營業秘密所有人對資訊之所有權情況下，以拷貝、複製、下載等無形侵害之方式取得或使用該資訊之內容者，一併列入本法禁止之範圍。此外，經濟間諜法將意圖犯與共謀犯規定為獨立之一罪，更是使得處罰行為廣泛。對於企業雇用留美人士之際，若未明確告知公司不希望亦不要求取得前雇主

機密資訊之立場時，稍有不慎，公司便有可能被控成立本法之共犯。因此，有必要針對經濟間諜法所規範之五種侵害行為加以分析，以免未來與美國進行技術移轉、合作或延攬美籍人士時誤觸法網。

以下針對各款之內容分析如下：

一、有形方式不當取得他人之營業秘密(第 1 款)

本款之犯罪行為涵蓋了英美法傳統竊盜罪的類型，但其範圍則廣泛至包括各種與盜用有關之行為，例如竊取、詐欺取得營業秘密等行為。此外，對於單純隱匿營業秘密者，其雖無實際使用營業秘密之行為，但因其足使所有人喪失對營業秘密之控制、管理或處分權，故本法亦將之列為侵害行為。

在美國法下，所謂「竊盜」係指以犯重罪之故意而偷竊、取走、移去他人之動產，且意圖移轉或剝奪所有人之權利。竊盜之構成要件必須有實際或建設性地將他人之物或財產取走，而未經同意或違反他人之意思，即未經所有權人之同意取走其所有物，或以詭計方法而騙取他人財產。質言之，竊盜係以下列故意行為，永久剝奪所有權人財產之佔有、使用及利益：

- (1) 未經權利人核准，獲得或摘取對該項財產的控制；
- (2) 藉詐欺手段取得該財產；
- (3) 藉威脅手段取得該財產；
- (4) 對一項明知係別人竊得的財產，再去獲取該

財產⁴¹。

條文中所謂「詐欺」係指為了引誘他人取得其信賴為目的，而故意編造事實，使他人將其有價財產予以交付，或讓與其法律權利。而該行為人必須就某事實作不實的陳述，不論是以文字或契約的方式，或是為虛設或誤導的主張，或故意隱匿事實等手段欺騙，或意圖欺騙他人，而使他人因此而受到損害。依美國普通法（common law）原則，詐欺之一般類型，包括經設計、錯誤建議或壓抑事實之手段，例如以詭計、奸詐、瞞混及任何不公平的方法，欺騙他人使自己取得利益⁴²。

本款所規範之侵害行為應係指以竊取或詐欺取得營業秘密所附著之有體物，而非營業秘密本身而言。蓋依前述所言，美國傳統刑法對於竊盜或詐欺罪之規定，需該侵害行為人在未經所有人之同意或授權情況下，實際將他人之物或財產取走，而永久地剝奪所有人之所有權而言。但由於營業秘密具有「非移轉性」之特質，亦即行為人能夠在資料並未發生所有權移轉現象，或不影響被害人利用可能性之情況下，運用下載、拷貝等方式知悉或取得該資料之內容。對此侵害行為，因所有人並未因此而當然喪失營業秘密之所有權，自與前述美國之刑法規定不符，故本款所規範之行為應限縮為直接對營業秘密所附著之媒體侵害之有形占有侵奪之類型⁴³。至於基於營業秘密「非移轉性」所發生之無形侵害行為則應適用第二款之規定。

⁴¹ 陳家駿，「公平交易法對營業秘密保護之評析」，公平交易季刊，第2卷第1期，第9-10頁，民國83年1月。

⁴² 同前註，第11頁。

⁴³ 鄭穎，前揭文，第118頁。

二、無形方式不當取得他人之營業秘密(第 2 款)

隨著資訊時代的到來，營業秘密等重要資料大多以電腦或其他磁性媒介儲存，是以，所侵害客體亦隨之而演變成此等媒介物，或甚至未竊取該媒介物，而以複製、下載等方式實質獲知該營業秘密之資訊內容，進而達到侵害營業秘密所有人之目的。就前者而言，仍屬於一般竊盜行為，可依據前款之規定規範之。至於後者，因此類侵害之行為並未實質取得營業秘密，與刑法竊盜罪之要件不符，但該行為之本質已足使營業秘密所有人喪失競爭優勢或降低該資訊之經濟價值，故有必要針對無形之侵害行為加以規範，以提供營業秘密所有人更完整的保障。

經濟間諜法為了有效解決上述所提之侵害態樣，特於第二款規範「無形之侵害類型」。即行為人於並未實質取得營業秘密之財產權或使所有人喪失其所有權之情況下，未經授權而複製或下載營業秘密，嚴重影響或破壞該營業秘密之價值而言。本款之規定係源於營業秘密之無形性特質而來。蓋以不正當手段取得營業秘密，非以取去有形之文件資料或電磁媒介物為限，若以拷貝、複製或素描等方式仍然可達到獲取該資訊之目的，因此本款與前款在不當性評價上，並無實質差異，應同時受到禁止。至於本款所列示之無形侵害行為，係因應電腦資訊時代之新型犯罪手法，包括有下載、上載、影印、重製、傳送等行為。透過網際網路方式傳輸竊取之營業秘密顯然即屬於該限制之範圍。

本款並未就「未經授權」特別加以定義，依據立法意旨其係指任何未經營業秘密所有人之允許之侵害行為均屬之，因此不論是在職員工或經合法授權者逾越權

限均有觸法之虞⁴⁴。然而，逾越營業秘密授權範圍之使用或洩漏行為，是否可同為規範之列，仍值得加以討論。逾越營業秘密授權範圍之侵害行為，本質上為契約義務之違反，宜透過民事法之損害賠償處理之。蓋經濟間諜法第1839條第四項規定該法所稱之所有人，係指對於營業秘密具有法律或衡平法上合法權利，或取得授權之個人或團體而言，因此已取得合法授權者逾越權限應屬於民事糾紛，且營業秘密所有人將營業秘密授權他人保管、使用時，應該與相對人簽署保密約定，加強相對人的保密義務，即進行「風險控管」，而此種控制應為營業秘密所有人所得為之，無庸國家以刑罰權強行介入，故本法所稱之未經授權在解釋上應不包括逾越營業秘密授權之侵害行為。然對此仍有待將來美國法院在適用上所做之解釋而定。但無庸置疑的是，無論此類行為究竟屬於民事或刑事事件，授權契約均必須明確約定授權範圍，以界定契約雙方之權利義務，而作為興訟時舉證之用。

三、由第三人處取得他人之營業秘密，而知悉該第三人係以不正當方法取得者

此即明知兜售或交付營業秘密之人，係以不正當之方法取得營業秘密，而仍然收受或購買者。成立本款之情況，該行為人於取得營業秘密之際，必須同時認識下列兩事實，一為知悉該資訊為他人所有之營業秘密，二為必須與竊取營業秘密之犯罪者，具備相同之主觀要件，即明知其收受行為將使得營業秘密所有人造成損害

⁴⁴ Gerald J. Mossinghoff, J. Derek Mason, Ph.D. and David A. Oblon, "The Economic Espionage Act: A New Federal Regime of Trade Secret Protection", adopt from <http://www.oblon.com/pub/mason-120.htm>

而言。本款並未限制行為人必須直接經由第三人取得營業秘密，因此行為人不論是直接或間接經由第三人取得營業秘密者，均包括在內。

四、意圖犯與共謀犯前二種類型者(第四、五款)

意圖係指超越單純準備、構思階段，但未達著手階段之犯罪行為。此需有犯罪之故意及準備犯罪之外部行為，相當於我國刑法之預備犯。而共謀犯罪者，須共謀犯中之一人已著手實施犯罪行為，其他共謀者雖未參與實施犯罪行為，亦以犯罪論。此相當於我國共謀共同正犯之概念，且本法並不處罰陰謀犯。一般刑事案件大多不處罰意圖犯，本法除了將其一併列入犯罪者外，更科以與正犯相同之刑責。而此等犯罪類型可能發生之案例即在於雇用競爭者之離職員工。即某公司倘若藉由雇用之名，意圖取得他競爭公司未經授權之營業秘密時，縱使該員工於取得營業秘密後，中止其犯罪行為者，其仍將與公司被控涉及經濟間諜法之共謀犯⁴⁵。有鑑於此，公司有意雇用競爭者之離職員工時，應秉持正當程序與心態，而不得藉此雇用手段而不法獲取未經他公司授權之營業秘密，並落實交叉確認手續，瞭解該名員工與前雇主間之權益關係，以避免任用後之訟累。

再者，由於意圖犯或共謀犯本身便具有可非難性，因此在永豐案判決中法院即明白表示，只要被告認為其所欲取得的資料為營業秘密已足，並不以該資訊事實上是否為營業秘密為必要。換言之，「法律上之不能」無法作為本法第1832條第(a)項第4款與第5款的抗辯理由或防禦方法，蓋若准許被告可以就意圖或共謀竊取他人營業秘密主張法律上之不能，則將迫使檢調單位使用

⁴⁵ Linda K. Steven, Id.

真正之營業秘密，揭露所有人之營業秘密，而有違經濟間諜法保護營業秘密之立法意旨⁴⁶。此項見解可謂放寬經濟間諜法之適用，值得國內業者特別注意。

上述五種不法之侵害行為，國會註釋中特別指出應採廣義解釋，只要行為人明知其重製或以其他方式控制營業秘密之行為，係不恰當(inappropriate)即可，因此檢察官不需指出其行為為違法，只需證明行為人並非因其與營業秘密所有人之關係所准許或授權，且行為人明知或可得而知其未經授權或准許即可⁴⁷。

第四項 法律責任

誠如本文在立法背景中所言，聯邦法原無保護營業秘密之專法，致使被害人僅得依據其州法來尋求救濟，然因大多州法對此僅提供民事訴訟程序與救濟，根本無法有效遏止營業秘密的侵害行為。故為有效解決營業秘密侵害行為，本法對於營業秘密之保護採取民、刑事兼具之救濟規定，以下分別說明之。

第一款 刑事責任

經濟間諜法首次對於侵害營業秘密者，課以刑事責任，而使得保護智慧財產權之法律於侵害救濟方面獲得一致。觸犯本法第1831條經濟間諜罪之個人將科以15年

⁴⁶ 馮震宇，「從永豐判決論美國經濟間諜法之適用」，萬國法律，第107期，第11頁。另參見 Efre M. Grail, W. Thomas McGough Jr., Jeffery M. Klink, "TradeSecret", The National Law Journal, p.B05, Aug.17, 1998. adopt from

<http://www.ljextra.com/practice/intellectualproperty/0817tsecrets.html>

⁴⁷ Section670(a)

以下之有期徒刑，或科或併科50萬美元以下之罰金；若為組織犯罪，則科以1000萬美元以下之罰金。觸犯第1832條竊取營業秘密罪之個人將科以10年以下有期徒刑，或科或併科25萬美元以下之罰金；若為組織犯罪，則科以500萬元以下之罰金。此規定遠比侵害其他智慧財產之刑罰為重，不難看出，美國對於侵害營業秘密之犯罪者已經下了猛藥，未來將可能重創涉案的企業與個人，使得與美國從事技術合作或技術移轉之個人或團體面臨極大的法律風險。

除了嚴苛的有期徒刑與鉅額的罰金之規定外，尚於第1834條規定所有用於侵害營業秘密的財產或是因犯罪衍生之所得均得由美國政府沒收之。故公司或組織若觸犯本法者，其所付出之成本將相當可觀。事實上，該條規定係參酌有關處罰毒販法規而制定，其目的在於能夠有較廣泛的財產可供美國政府沒收並加以拍賣，以救濟於被告經濟情況不佳時，得以拍賣所得賠償被害人之損害。然值得注意的是，被害人的營業秘密卻可能混在被沒收之客體，而面臨拍賣之命運⁴⁸，因此，在實際執行時應特別注意此一問題，以避免被害人之營業秘密同列為沒收客體而遭受更大之損失。至於沒收的界限，因經濟間諜法對此並未設有特別之規定，因此僅受到美國憲法第八條修正案的限制，即禁止與犯罪行為顯不合比例之沒收⁴⁹。

⁴⁸ James Pooley, "Criminal Consequences of Trade Secret Theft: The Economic Espionage Act of 1996". 馮震宇譯，「竊取營業秘密的刑事責任-美國 1996 經濟間諜法」，1998 技術貿易研討會產業升級之契機論文集，第 75 頁，民國 87 年。

⁴⁹ 馮震宇譯，前揭文，第 71 頁。

第二款 民事責任

經濟間諜法並未特別規定侵害行為人之民事責任，而係於第1836條中指出，經濟間諜法並不排除或取代美國聯邦或各州就竊取或盜用營業秘密所規定之其他任何民事救濟，因此被害人可依據聯邦法或各州之營業秘密法對侵害行為人提起民事訴訟，請求損害賠償，出現聯邦法與州法並行之雙軌制度。

就聯邦法而言，被害人似可依據聯邦法第1964條之規定⁵⁰，向侵害行為人請求三倍之損害賠償。蓋由於本條以規範侵害人以郵電詐欺或通訊詐欺、賄賂等不法方式，竊取並影響被害人商業之侵害行為，而此項規定與經濟間諜法對於不正行為之規範有共通之處，故有學者主張，未來可預期美國國會將修正第1964條之規定，使得應負賠償責任之不法行為包括違反經濟間諜法在內⁵¹，屆期對於營業秘密所有人之權利將更有保障。

此外，被害人亦可自行依據各州的州法提起民事訴訟，請求法院為適當之救濟。例如在四維公司的案件中，自稱為被害者的美商丹尼爾公司便另行在俄亥俄州的州法院提起民事損害賠償訴訟，請求賠償美金1億元。又值得一提的是，該條明文規定聯邦地方法院對侵害營業秘密之案件，有專屬的第一審管轄權，但因本法為公訴罪，私人並無訴權(no private cause of action)，故被害人不得直接向法院起訴，相對地，被害人亦無與侵

⁵⁰ The Packetter Influenced and Corrupt Organizations Act("RICO"), 18.U.S.C. § 1962(c) and 1964.

⁵¹ Irvin B.Nathan and Nancy L. Perkins, "Tough Enforcement of New U.S. Economic Espionage Act Reveal Need for Strict Compliance", 國際技術移轉管理面面觀-美國經濟間諜法及我國業者技轉因應之道補充資料, 第7頁, 民國86年7月。另參見"The Economic Espionage Act of 1996", <http://www.nhold.com/hot/wh11.htm>.

害行為人成立和解之餘地。以永豐案為例，必治妥公司即對外表示，該案由聯邦調查局進行調查、逮捕、指控，「這是美國政府的案子，不是必治妥施貴寶的案子」，因此，必治妥公司並沒有考慮庭外和解⁵²。蓋除了檢察官主導訴訟外，檢察官亦不願使其調查活動付之一炬，而遭受法院不受理之結果。由此可知，聯邦法院對於起訴案件不論在刑事或民事責任上均扮演主導之角色。

第五項 域外管轄

為擴大營業秘密之保護，經濟間諜法透過犯罪主體之規定，使其適用範圍涵蓋至美國領域之外。換言之，本法所規範對象，不但包括任何於美國境內所發生違反本法之行為，亦規範在美國境外所發生之侵害行為。對於行為地在美國境外之犯罪，尚須符合下列二種情形之一：

1. 侵害行為人係美國公民或擁有永久居留權之人士（亦即具有綠卡者），以及由美國公民或永久居留權人所實質擁有或控制的組織或根據美國法律所組織之公司；

例如持有綠卡或在美國依法成立之公司，該個人或組織於美國領域外竊取美國政府、企業或個人之營業秘密時，美國檢察官便可依據本法予以起訴。

2. 犯罪行為有一係在美國境內所為。

不論行為人之國籍，只要犯罪行為之一發生在美國境內，即有本法之適用。例如交付營業秘密之犯罪行為在美國領域外進行，故可免於被美國逕行逮捕的風險，

⁵² 「這是美國政府的案件-必治妥沒考慮庭外和解」，聯合報民國86年6月19日，第3版。

但若籌畫、接洽等係在美國領域內進行者，亦適用本法。此外，以網際網路使用電子郵件、檔案傳輸或瀏覽器等行為，若有侵害美國廠商情事者，縱在美國境外仍有可能受該法之管轄⁵³。但網路無國界之特性使得管轄權之權限為何，仍有爭議。蓋當某國開始規範網路行為時，結果往往超過其國家主權範圍，而侵害他國之主權⁵⁴。因此，美國可否能自主地依據經濟間諜法起訴網路行為人仍有存疑。

原則上該法之適用範圍係以行為在美國境內發生者為限，本條將其適用範圍擴大至美國境外係兼採屬人主義與保護主義所致。就第一款而言，行為人須為美國國籍之個人或組織為限，係因其所侵害之法益為國家與社會利益，故縱在美國領域外犯本罪者，無論係以屬人主義或保護主義之觀點，均有本法之適用；至於第二款即所謂隔地犯，係以犯罪行為有一在美國境內者，視為在美國境內所為。本法雖可規範一切侵害美國企業之犯罪行為，但在執行上值得懷疑的是，假設他國人在美國境內有一違反本法之行為後，隨即潛逃回母國，若該國並未與美國簽署引渡條約時，則將無法適用經濟間諜法制裁該犯罪者⁵⁵。以永豐案為例，涉案人周華萍即係因中美雙方未簽訂引渡條款，至今均未到案⁵⁶。因此，該規定實際上成效如何，仍有待觀察。但無庸置疑的是，此種廣泛之規範對象，不但對國內企業至國外挖角或雇用留美人士將產生某種程度之影響，同時亦對於自美國

⁵³ 馮震宇，前揭註 23，第 71 頁。

⁵⁴ 楊靜宜，「網路行為管轄權爭議問題之初探」，資訊法務透析，第 16 頁，民國 88 年 6 月。

⁵⁵ Sorojini J. Biswas, "The Economic Espionage Age of 1996", adopt from <http://www.carolinapatents.com-articles/trade-secret4.htm>.

⁵⁶ 參見「徐凱樂當庭認罪涉竊抗癌藥機密」，經濟日報民國 88 年 4 月 3 日，第 26 版。

引進技術的行動造成衝擊，蓋因技術引進不可避免的會涉及人才、技術資料與其受保護之營業秘密等問題。因此，在利用技術合作或技術移轉方式，從美國引進技術之際，如何防止違反該法之規定，乃成為廠商必須注意的問題。

第六項 維持資訊之秘密性

營業秘密之價值係源自於其所具備之秘密性，一旦營業秘密遭公佈而為公眾所知或所有時，其價值亦隨之喪失，因此如何在訴訟過程中維護其秘密性實屬重要。

經濟間諜法第 1835 條規定，於本章所進行的各種追訴或其他程序中為保護營業秘密之需要，法院應依據刑事訴訟規則、民事訴訟規則、聯邦證據規則與相關法律之規定為適當命令或採取適當的行為。法條所謂採取適當命令或適當之行為，包括在開示證據程序時核發保護命令、秘密審理、封鎖訴訟記錄、命令有涉案之訴訟關係人未經法院同意不得洩漏秘密等手段均屬之。然此規定卻與經濟間諜法刑法化所欲採行之刑事程序，產生「保護營業秘密之秘密性」與「訴訟審判公開」如何權衡之問題。

刑事案件依據美國憲法第四條和第六條修正案之規定，檢察官必須將所有起訴被告之證據公開給被告與大眾知悉，俾利於被告能夠針對起訴理由加以答辯，但此項被告基本權卻與經濟間諜法第 1835 條有相牴觸之處。蓋倘若法官准許營業秘密保護令核發，即禁止被告閱覽全部營業秘密資料時，顯然該保護令將侵害被告憲法上權利。反之，法官若不准許核發營業秘密保護令，

顯然又與經濟間諜法立法意旨相左。就此衝突，美國最高法院之見解認為，「若法律與憲法適用於同一案件發生相互抵觸，法院必須擇一適用時，依憲法定之」。是故，被告在憲法賦予之權利範圍內仍可主張檢視系爭之客體是否為營業秘密。一旦被告要求將「營業秘密」揭露予被告指定之特定專家，或可能之證人時，縱使法官以指定之方式揭露，但徵諸實際現況，營業秘密外露之風險卻大為增加。基於此種風險的不可避免性，營業秘密所有人是否仍願意配合檢方之追訴行動，顯然大有疑問，則經濟間諜法是否仍能達到其追訴竊取營業秘密者之立法意旨，則有待商榷⁵⁷。

從經濟間諜法之規範內容可知，美國政府為保護其國家經濟利益與企業競爭力，已經投下了猛藥，同時也透露出全球科技產業正新興起新的保護主義⁵⁸，智慧財產權也將成為市場爭奪戰之有利武器。因此我國企業必定要熟悉相關之國際規範，並尋求因應之對策，「知己知彼」才能防範於未然。對此，本文將於第五章作完整之闡述。

⁵⁷ 董浩雲，「美國經濟間諜法執行上的幾個問題-從永豐案的觀察」，資訊法務透析，第 63-65 頁，民國 88 年 5 月。

⁵⁸ 參見「新保護主義，台灣成為俎上肉」，自由時報民國 87 年 4 月 3 日，第 19 版。

第三節 經濟間諜法之研析

從上一節之分析可知，經濟間諜法較一般刑事法之管轄範圍為廣，同時，處罰亦較為嚴苛，其主要因素為美國國會希望藉由該法來打擊外國政府所支持之間諜活動，以保障其國家安全；另一方面則是希望以國家公權力來保護私人企業間之營業秘密，因此，造成經濟間諜法若干條款與一般刑事法大異其趣。該法開啟了以聯邦法保護營業秘密之大門，且首次對於侵害營業秘密科以刑事責任，相較於侵權行為彙編與統一營業秘密法，該法的特色可謂為「聯邦化」、「刑法化」。對此，本文將比較該法與前述之傳統營業秘密保護法說明其異同；並針對營業秘密之保護聯邦化和刑法化後所產生之優劣點為何，並嘗試探討其妥適性。

此外，美國在高舉自由貿易旗幟下，卻又以保護其廠商營業秘密為由制定本法，其所規範內容對於與美國從事技術合作、資訊流通等商業活動或雇用留美人士均將造成一定之法律風險，故本文並就本法對商業活動和營業秘密所有人、受雇人、顧問等關係人之影響加以闡述，以求深入瞭解本法所產生之效應。

第一項 與傳統營業秘密保護之比較

一、營業秘密之定義

根據立法意旨之說明經濟間諜法係以統一營業秘密法為依據，將民事法中營業秘密概念移植過來，因此關於營業秘密之定義大致上可說是大同小異。惟兩者差異在於經濟間諜法將其他類型之資訊型態，例如以電子、

圖形等方式儲存之資訊，均列為保護之範圍，換言之，目前存在或將來可能發生之儲存營業秘密的方式，均納入保護範圍，藉以因應發展迅速的科技工業。是故，經濟間諜法就保護營業秘密之定義與範圍較前兩者為廣。

二、營業秘密之要件

從經濟間諜法之規定可知，經濟間諜法關於營業秘密之要件與統一營業秘密法相同，必須具備秘密性、獨立之經濟價值和採取合理之保密措施三者。然經濟間諜法與統一營業秘密法不同之處，則在於是否具備獨立之經濟價值，並非從犯罪者角度判斷，而係以營業秘密所有人觀點為依據。亦即倘若所竊取之營業秘密對犯罪者無經濟價值可言，而所有人主觀認為其具有經濟價值者，則該資訊仍屬法保護之營業秘密，因此，有學者指出經濟間諜法顯然偏向營業秘密所有人⁵⁹，實不為過。

三、侵害行為

有別於彙編與統一營業秘密法為民事法規，經濟間諜法將侵害營業秘密之行為論以刑事責任，故基於法規性質之差異，則經濟間諜法關於犯罪意圖之認定、刑罰、沒收等皆為前兩者所無。且為遏止外國政府或機構不法獲取美國企業之營業秘密和維持其國內企業公平競爭，經濟間諜法基於侵害目的與圖利對象不同，將侵害行為區分為經濟間諜罪和竊取營業秘密罪，與前兩者係基於行為人與營業秘密所有人有無合法關係，區別其侵害態樣，截然不同。此外，經濟間諜法與前兩者就侵害行為之差異，說明如下：

⁵⁹ 馮震宇，前揭註 23，第 72 頁。

(一)不正當手段

彙編未以條文直接針對不正當手段加以定義，而係以註釋之方式說明其內涵。有別於此，統一營業秘密法則明文對於不正當手段為定義性之例示規定。儘管兩者在立法方式上不同，然細觀其內容仍屬一致，故可謂後者係承襲前者之立法而來。

而經濟間諜法，雖亦未以獨立條文對不正當手段為定義性之規定，然從第1831、1832條第1、2款之規定，可看出與前兩者之規範意旨實屬相同。此外，由於電腦資訊的繁榮與網際網路使用率的頻繁，不免增加不法人士竊取或傳輸營業秘密的機會。故為有效規範此類以電子設備所從事之侵害行為，經濟間諜法遂承襲彙編註釋與統一營業秘密法第1條第1項「以電子或其他方法所為之間諜行為」之立法意涵，特別明文規範例如「下載、上載、改變、毀損、傳送」等電腦犯罪行為，據此可謂經濟間諜法係傳承前兩者之規範，並配合電腦革命後侵害行為的多樣化，例示電腦犯罪態樣，其發展可謂具有長足之進步。

(二)侵害行為之態樣

統一營業秘密法所規制之不正行為，有「取得」、「使用」和「洩漏」三者，經濟間諜法所規範之侵害態樣則較為廣泛。蓋依據經濟間諜法第1831、1832條之規定，此不正當行為不限於不法取得或洩漏營業秘密，倘若行為人僅是單純地隱匿或毀損該營業秘密之行為，並未將其內容複製或傳輸給第三人時，因該不法行為已足以剝奪營業秘密所有人之所有權，降低該營業秘密之經濟價值，故仍可成立經濟間諜罪或竊取營業秘密罪。又各州對於以無形之方式侵害營業秘密，例如素描、繪

畫、攝影等方式是否構成侵害，係由法院針對個案或當地州法加以認定，不免會發生歧異。故經濟間諜法於第1831、1832第2款中明定此類以無形方式所為之侵害行為亦構成不正當行為，使得營業秘密侵害認定之問題，獲得有效的解決。

(三)侵害行為之範圍

由於經濟間諜法為刑事法，其所規範之侵害行為之範圍除了正犯外，尚包括預備犯與共謀犯，且該兩者均科以與正犯相同之刑責，範圍可謂相當廣泛，此為統一營業秘密法等民事法規所無者。

四、法律救濟

依據統一營業秘密法第三條之規定，對於因盜用營業秘密之行為，被害人可分別情形向行為人請求補償性與懲罰性之損害賠償。經濟間諜法首次對於侵害營業秘密者課以刑事責任，對於營業秘密之保護兼採民、刑事救濟規定。

從上述之比較可知，經濟間諜法與傳統營業秘密之保護，就基本架構之營業秘密定義、要件均屬相同，僅有之差異為增加營業秘密之資訊型態，以配合科技之發展。再者，侵害行為之認定因各州對於無形侵害行為之處罰各異，聯邦為制裁此等電腦犯罪，特於經濟間諜法中加以規範，並科以嚴刑峻罰，以因應該新興之侵害行為。故美國關於營業秘密之保護，實有其傳承性並配合科技發展之變革性。

第二項 刑事追訴之優劣

經濟間諜法將營業秘密之保護聯邦化與刑法化之

優劣點，分述如下：

一、刑事追訴之優點

經濟間諜法以聯邦法保護營業秘密，故營業秘密所有人將可求助聯邦調查局與檢察官運用其調查資源與網絡起訴竊密案，而不再受限於地方檢調單位調查資源日益縮減之影響。例如，本法授權聯邦檢察長得同意或命令聯邦調查局或其他聯邦單位，竊聽犯罪之通訊記錄或談話，這些調查資源都是地方機關無法比擬的。

再者，因刑事訴訟審理較為快速，被害人將可及時獲得救濟和避免遭受更大的商業損失。此外，因刑事定罪舉證責任之要求遠高於民事責任，故縱依據本法認為被告不足以定罪，其於刑事訴訟審理所獲得之證據，亦可作為被害人請求民事損害賠償之基礎，對於被害人而言，將可減輕其所負舉證責任所需耗費之時間、人力。是故，本法刑事追訴之優點即在於以國家公權力介入營業秘密侵害行為，藉此達到保護其國內企業競爭力之目的，對於其他有意效尤者產生強大的嚇阻作用，或可促使尚未被追訴之侵害者願與營業秘密所有人私下和解，以免遭受嚴刑峻罰。

二、刑事追訴之缺失

經濟間諜法屬於刑事法，故美國政府必須就被告之犯罪事實之構成要件負「超過合理懷疑」（Beyond a Reasonable Doubt）的舉證責任。就經濟間諜法之犯罪而言，被告是否具有主觀之（Intent），實為成罪與否之關鍵，例如證明被告「意圖」使營業秘密所有人受損或「明知」該機密係屬他人所有

等。惟從證據法之觀點，除非有明確的犯罪事證，否則要證明被告有犯罪之意圖，將十分困難。因此，有美國學者認為因刑事舉證責任所造成之障礙，將使得竊取營業秘密能以本法成功起訴並定罪的比例降低⁶⁰。

以經濟間諜法起訴犯罪行為者，營業秘密所有人將可利用聯邦廣泛的調查資源，加速保護其免於遭受更大的商業損失。然該竊密案件所有調查的策略、起訴時間、程序等事宜均將由檢察機關決定，亦即營業秘密所有人對該案將會喪失某種程度之處分權，例如禁止與被告成立和解⁶¹。

再者，因經濟間諜法並未提供民事救濟，故被害之營業秘密所有人可依據其他州法或聯邦法請求損害賠償，換言之，單一侵權案件將可能面臨在不同法院審判的危險。惟一旦依據本法起訴後，營業秘密所有人所進行之民事訴訟程序將可能被迫停止，蓋為民事訴訟程序之證人，將可能恐因其陳述而受刑事訴追或處罰，而主張美國憲法第五條修正案之權利拒絕作證，以避免自陷於罪(self incrimination)，導致民事程序無法有效進行⁶²。故以刑事法起訴侵害營業秘密行為，將可能間接地妨礙營業秘密所有人之民事救濟，導致使被害人無法獲得最佳之保障。

⁶⁰ Joseph N. Hosteny, "The Economic Espionage Act: A Very Mixed Blessing", <http://www.hosteny.com>

⁶¹ Arthur Wineburg and Timothy J. Klima, "Current Issues in Trade Secret Law: The New U.S. Economic Espionage Act", <http://www.pillsburylaw.com/publications/economic-espionage.html>.
"The Economic Espionage Act of 1996", <http://www.nhdd.com/hot/wh11.htm>.
Gerald .Mossinghoff, J. Derek Mason, Pg. D., and David A. Oblon,Id..

⁶² 黃家珍，「美國九六年經濟間諜法簡介」，通訊雜誌，第36頁，民國86年11月。

綜上所述，本法將侵害營業秘密之行為論以刑事責任，對於營業秘密所有人而言，可由聯邦調查單位進行案件之追訴，免於訴訟所需耗費之時間、金錢或人力。然而，面對刑事案件所要求之高度證據力，已經使得被害人卻步，再加上被害人對於營業秘密遭受侵害時所關注的畢竟還是民事賠償，而非犯罪者刑罰輕重，本法卻使得被害人喪失當事人處分權，延宕民事救濟求償。因此，有美國學者評論經濟間諜法僅為營業秘密所有人無法以民事救濟時之備用工具，換言之，僅於涉外案件、有實質的證據存在、很難獲得民事救濟或被害公司調查資源不足等情形，被害人願意選擇與檢調單位配合，以經濟間諜法起訴犯罪者，達到科以嚴刑峻罰或擊其商譽之目的⁶³，故本法可否能有效執行仍待觀察。再者，由於經濟間諜法之立法規範較為寬鬆，為避免產生執法的問題，美國司法部部長特致函國會指出，在2001年10月以前，所有以違反經濟間諜法起訴之案件，均需取得司法部長、司法部副部長等人之同意方可以進行⁶⁴。該司法部的自我設限，使得被認定違反經濟間諜法之案件寥寥可數，再加上永豐案判決被告有權檢視含有營業秘密之文件內容，許多美國業者反而開始積極利用各州營業秘密法，對於侵害營業秘密者進行追訴，使得各州法院受理該類型案件相對性增加⁶⁵。是故，美國企業利用經濟間諜法追訴營業秘密侵害行為之比例仍有待評估。

⁶³ Joseph N. Hosteny, Id.

⁶⁴ 馮震宇，前揭註46，第2頁。"Criminalization of trade secret theft as part of the economic espionage act", Current, Vol.4, Issue 3 Fall 1997, adopt from http://www.szd.com/articles/intellectual_Prop/Vol4iss2/TRDSCRTS.html.

⁶⁵ 馮震宇，前揭註46，第2、13頁。

第三項 對商業活動之影響

科技的發展須透過研究成果與資訊的交流、溝通、討論，才更能發生效果，並進一步促進科技的發展。然而美國在高舉自由貿易旗幟下，卻以保護其國內廠商營業秘密為由所制定之經濟間諜法。該法將過去商業爭議案件改由聯邦檢調單位介入，無異是美國政府提供司法與警察資源免費提供營業秘密所有人自由利用。若發生有濫用本法之情形，將因此而導致被告公司商譽受創、停滯系爭技術的研發工作或耗費訴訟時間、費用等，重創涉案公司。

又該法對於未經授權之使用或洩漏營業秘密等行為，均列入處罰之列，然該「未經授權」條文中並未詳細載明其定義，而依據立法意旨似包括所有未經授權之行為，亦即逾越原合法授權範圍者亦有本法之適用。是以，任何人一有怠忽未經許可而洩漏營業秘密者，均有觸法之可能。故與美從事商業活動將因經濟間諜法所產生之法律風險，而影響技術合作與資訊交流之進行。

第四項 對關係人之影響

綜觀經濟間諜法之規定，營業秘密所有人須採取合理的保密措施始獲得本法之保障，且公司可能因雇用新進人員，或受雇人轉業等情形而產生違反經濟間諜法之法律風險等。故本節將從營業秘密所有人、受雇人或顧問二方面說明本法對於關係人之影響，茲說明如下。

一、營業秘密所有人

經濟間諜法對於所有人之營業秘密提供了最有效的保護。蓋本法對於所定義之範圍相當廣泛，幾乎涵蓋一切資訊；尤其對於侵害營業秘密者科以嚴刑峻罰，更是提供了制裁犯罪者最強有力的武器。再者，本法之特色在於首次要求被害人須採取配合措施，始可主張權利之存在，故本法對於營業秘密所有人之正面影響即在於使其建立保密措施，作為權利主張與無涉入不法涉訟之證明。至於本法對其所產生之不利益，即在於以刑事追訴所產生之缺失，例如處分權之喪失、延宕民事賠償等，此可參見前節之說明。反之，若為涉案公司，則將面對 500 萬元以下之罰金與刑事沒收。

二、受雇人或顧問

由於經濟間諜法偏向於保護營業秘密所有人，相對的，對受雇人與顧問將產生較大的風險。蓋受雇人或顧問接觸公司若干技術、資料是不可避免的。然因經濟間諜法將所有未經授權之行為均視為不法行為之，此無非是使得在職員工肩負極大的法律風險。而對於利用不斷轉業以求升遷的受雇人，更應特別注意劃分其個人與原有雇主之智慧財產權，以避免因權責不分而違法。

經濟間諜法立法目的在於創設一個全國性法律架構，以保護美國產業之營業秘密。但經濟間諜法並不能因此而傷及或威脅企業競爭、個人轉業自由，故該法並無意用於起訴以受雇人一般知識、技術和專門知識所從事之競爭行為⁶⁶。然而，此舉卻可能使得受雇人陷入困

⁶⁶ 郭認美，「論台灣高科技工業如何因應美國經濟間諜法技術移轉 V.S.竊取營業秘密」，1997 全國智慧財產權研討會論文集，第 290 頁，民國 86 年。另參見 Mark D.Seltzer and Angela A.

境。蓋於前雇主工作期間所獲取之商業或技術知識中，何者為營業秘密，何者為一般技術或知識，在判別上不但對於受雇人造成困擾，對於新任公司亦造成難題，一旦該受雇人發生不慎侵害營業秘密之行為，新任職公司將可能被控共謀之罪，也將潛在地限制了該名員工在工作上的發展和工作的流動性。因此，受雇人之保身之道即在於與所任職之公司簽署智慧財產權劃分契約，將自己一般知識、技術與公司之營業秘密明確劃分清楚，而新任職公司則必須明白告知該名員工僅能使用一般知識之部分，並與前公司交叉確認該員工之保密契約等事宜，以徵明非為竊取前公司之營業秘密始雇用該名員工。

若謂經常轉業者所面臨的問題重大，則擔任企業顧問更是面臨無法超越該困境。蓋顧問可能同時擔任不同企業，或是先後擔任某企業短期的工作，知悉受雇公司之商業資訊係不可避免。面對經濟間諜法之刑事責任，如何與顧問簽訂契約以精確的劃分顧問本身與公司之關係，便具有特殊的重要性。

美國將營業秘密之保護從不公平競爭獨立出來，且對於營業秘密之侵害與救濟，已經從當事人處分之民事救濟變革為刑事案件，引發國家公權力介入之必然性，

Burns, "Criminal Consequence of Trade Secret Misappropriation: Does the Economic Espionage Insulate Trade Secrets from Theft and Render Civil Remedies Obsolete", May 25, 1999, <http://www.bc.edu/bc-org/avp/law/st-org/iptf/articles/content/1999052501/html>.

對於商業活動本身或關係人所產生之法律風險，均值得企業引以為鑑，並配合採取保護措施，才能避免發生類似永豐案或四維案之不幸事件。此即本文第五章所欲探討之因應對策。

第四章 各國立法與理論之比較

第一節 各國立法與理論內容之分析

第一項 德國

德國對於營業秘密之保護可分為二部份，一為不正競爭法，一為刑法第202a條資訊刺探罪。前者立法由來係源自於德國因營業秘密遭竊，而蒙受巨大損失，且產業間諜之行為嚴重損及德國工業力，和威脅到其工業上的優越地位，導致發生大量勞動者失業之社會問題等等，故將原本屬於私人利益保護之營業秘密變成保護整體國家、社會利益之觀點，此與美國經濟間諜法之立法理由可說是如出一轍；至於後者之立法則係基於第二次經濟犯罪對策法律而來，該條文雖其保護之客體不限於營業秘密，但因其可提供營業秘密之刑法上之保護，而與經濟間諜法之刑事制裁有共通之處，故將其納入本文中關於營業秘密侵害之法律效果，一併說明之。

一、營業秘密之意義與要件

德國不正競爭法關於營業秘密之定義與要件並未明文界定，而係委由學說、判例加以歸納¹。根據通說，營業秘密係指所有與營業有關且尚未公開之事實，秘密所有人對其有保密之意思，且該秘密之保持對於營業秘密而言有正當之經濟上利益。

根據上述之定義，可歸納出德國不正競爭法所保護

¹ 謝銘洋，「營業秘密侵害之類型觀察與責任分析」，資訊法務透析，第272頁，民國81年8月。

之營業秘密在主觀及客觀方面，應具備下述三特點：

1. 未經公開

以秘密之本質來說，當然僅為特定人或可得限定之人知悉，一經公開，即無秘密可言。

2. 保密之意願

依通說秘密之所有人應有排除經容許以外之人知悉秘密之意願。該意思雖不以明示為限，仍需有客觀守密意思之具體表現，以強化秘密為有意義，值得保護之法益，而不流於恣意²。

3. 正當之保密利益

所謂保密利益，係指秘密具有經濟上之價值，有助於企業所有人之競爭能力之提昇。且該利益須為正當、適法，即必須具有值得保護之利益。

二、 侵害行為之態樣

德國不正競爭法關於侵權行為之類型係規定於該法第 17 條、第 18 條。茲以行為主體之不同，將侵害行為之類型區分為四種，以下分別說明之。

（一） 僱員洩漏營業秘密：

依據第 17 條第一項之規定：「企業之職員、工人或學徒，為競爭之目的，供己之用或圖利他人，或意圖加損害於企業所有人，於僱傭關係存續中，將其因僱傭關係受託或獲悉之營業秘密或經營上秘密，無故洩漏於他

² 「營業秘密法律保護之研究」，行政院科技顧問組委託辦理，第 34 頁，民國 80 年 5 月。

人者，處 3 年以下有期徒刑或併科罰金」。構成本項之主、客觀要件可細分如下：

1.客觀構成要件

(1) 行為主體

行為人須限於與營業秘密保有人間具有人之從屬關係者，即行為主體以職員、僱員、學徒等有特定身份之人為限。此處「職員」應採廣義解釋，即只須對於營業秘密所有人提供勞務，不論職位高低、是否受有報酬、工作種類、工作期間長短等均屬之。甚有認為董、監事會成員、經理人等亦應包含在內，以求保護能更週延。

(2) 行為客體

此處限於僱員因僱傭關係受託或知悉之營業上或經營上祕密。「因僱傭關係受託或知悉者」，係指該營業秘密為行為人於僱傭關係期間，基於企業主之信賴所擁有或接觸者。倘若行為人與公司間並無存在僱傭關係，或雖有僱傭關係但所知悉者與行為人職務無關之營業祕密者，則無本項之適用。

(3) 行為

「洩漏」為本項規範之行為。所謂「洩漏」，係指營業秘密以作為或不作為之方式，以書面或言詞將營業秘密通知或傳達於他人而言。且僅須受領人居於對營業秘密能使用或繼續傳播與他人之地位已足，並不以其確實知悉該營業秘密之內容或實際利用為要件。再者，行為人須「無故洩漏於他人」，是故，倘若行為人自己不法利用此營業祕密者，因其並無洩密行為，自非本款規範

之對象，而應以背信罪論處³。

該侵害行為發生時間為「僱傭關係存續中」始屬之，故僱傭關係存續與否之認定實屬重要。對此應依法認定之，亦即僱傭關係終止須依法律或約定方式為之，若未依法律或約定終止者，則因契約關係仍然存在。

2.主觀構成要件

行為人除須認識客觀構成要件外，須具備一定意圖，即行為人必須基於特定目的而實施洩漏行為，始該當本項之要件。本項規定之意圖有四，只要具備其一已足：

- (1) 為競爭之目的：係指增進自己或他人營業發展目的之主觀意圖而言。
- (2) 供己之用：意圖為自己取得利益而洩密。所謂利益並不以財產或物質上之利益為限，無形財產或精神上之利益亦包括在內。
- (3) 圖利他人：意圖使他人取得利益而洩密；
- (4) 加損害於企業所有人：行為人有加損害於企業所有人之意思而言，此謂之損害不僅指財產上損害，亦包括對企業信用、名譽等非財產上之損害。

(三) 第三人不法刺探取得營業祕密

此為 1986 年德國修正不正競爭防止法時新增列之侵害類型。依據第 17 條第二項第一款之規定：「為競爭之目的，或供己之用，或圖利他人，或意圖加損害於企

³ 徐遵慈，前揭文，第 42 頁。

業所有人，而為下列行為之人，處以相同之刑：取得或佔有營業秘密或經營之秘密係經由

- a. 利用技術上之方法
- b. 具體複製秘密
- c. 取走秘密所附著之物」

茲將本款之要件分析如下：

（1） 行為主體

本款並未限制行為主體之身分、資格或應具備特定關係，故任何人均得為本款之主體。

（2） 行為客體

本款之行為客體為經營上或營業上之秘密，其定義與要件前節第一款已做說明，於此不贅述之。

（3） 行為

本款規範之行為係以特定方式「取得」或「保存」他人之營業秘密，尚未加以利用之情況。所謂「取得」，係指將營業秘密置於自己實力支配範圍內，而處於隨時知悉之情況；至於「保存」，係指行為人將其以瞭解內容之秘密，透過複製等方式，使之確實成為自己之物之行為。然並非所有不法「取得」或「保存」營業秘密之行為均受本法之制裁，而係僅限於特定行為。根據本款之規定，此等特定行為方式有三：

a. 利用技術上之方法：

利用技術上之方法係指利用任何技術上之裝置將

營業秘密精確地傳達於他人，而非實體取得營業秘密而言。例如利用影印機、照相機、監聽裝置、錄影機、竊聽器、小型傳送或接收器等，故凡照相、利用電話探悉、電腦取閱秘密等行為均屬之，至於如果僅係憑記憶力將營業秘密內容記下，則尚非所禁止對象。

b. 具體複製秘密

係指以有體物複製秘密，嗣將其全部或一部轉知於他人之行為，例如以電話監聽後將所知內容作成筆記、素描或錄音等均屬之。

c. 取走秘密所附著之物

係指違反營業秘密所有人明示或可得而推知之意思，取走有形之營業秘密，例如竊取營業秘密所附著之磁片。此相當於取走他人之有體物，故亦可能觸犯竊盜罪。

(4) 主觀構成要件

行為人所應具備之主觀意圖與上述第 17 條第 1 項相同，請參閱該條項之說明，不再贅述。

(四) 利用或洩漏不法取得之營業秘密

依據第 17 條第二項第二款之規定，「不法利用第一項所指之洩漏或自己或他人因第一款之行為而取得，或其他不法取得或佔有之營業秘密或經營秘密，或洩漏於任何人。」

本款所規範者為「利用」與「洩漏」他人營業秘密之行為，然非所有無故利用或洩漏行為均受本款之制裁，僅行為人以本款所規定之不法方式取得營業秘密後

無故利用或洩漏之，始有本款之適用。

依本款之規定，不法取得營業秘密之方法可能經由員工洩密所取得，或可能由自己或他人之行為，或其他不法取得或保有之營業秘密。此所謂不法不但違法，亦包括任何違反營業秘密所有人守密利益之行為，此外不法利用之範圍則指不法之利用和不法轉知於第三人而言。

至於本款其他主、客觀構成要件，與第 17 條第二項第 1 款同，故予從略。

（五）盜用樣品罪

依據第 18 條規定：「因業務往來而受託持有他人之樣品或技術文件，特別是圖樣、模型、模版、式樣、處方等，因意圖為競爭或自行使用之目的，而不法使用或交付他人，處 2 年以下有期徒刑或併科罰金。」

本條規範之行為主體係企業與企業間之關係，亦即企業之對外關係，非企業與員工間之內部關係。惟個人若受託持有樣品等資料，亦不排除本條之適用。本條保護之客體為行為人於營業秘密交易上受託之技術性文件，至於其委託之方式為書面、言詞或明示、默示或基於契約關係均可。

三、法律責任

不正競爭防止法保護營業秘密係以刑事罰為主，另有民事救濟之方法，包括被害人享有損害賠償請求權及不作為請求權；此外德國刑法第 202a 條對於侵害營業秘密之行為亦規定刑事責任，茲介紹如下：

（一）刑事責任

就不正競爭防止法而言，該法第 17 條規定對於前述侵害營業秘密之類型：(1) 僱員洩漏營業秘密，(2) 第三人不法刺探取得秘密者，(3) 利用不法取得之秘密，處以三年以下有期徒刑或併科罰金，及第 18 條盜用模具罪則處以二年以下有期徒刑或併科罰金。此外，依據第十七條第三、四項、第二十條第二項、第二十條之一之規定，對於未遂犯、預備犯及在國外犯罪加重處罰之類型，均有刑事罰之規定，明顯的看出該法擴張其可罰行為之範圍，而第十七條第四項之規定，更是基於國家利益考量所為之立法，此與美國經濟間諜法第 1838 條之立法意旨係屬相同。

至於刑法第 202a 條資訊刺探罪，其規定為⁴：

「未經許可，而使自己或第三人取得其無權使用而設有避免不當接近之特別保護措施之資料者，處三年以下之自由刑或併科罰金刑。（第一項）」

前項意義之資料，以電子、磁性或其他使人無法直接認知之方式而儲存或傳送者為限。（第二項）」

本條之客體並不以營業秘密為限，尚可以包括關係個人之資料、著作權法上所保護之程式，以及國家機密，且本條與不正競爭防止法第 17 條成立想像競合犯之關係，故本條之規定亦可提供營業秘密在刑事法上之保護。

（二）民事責任

侵害營業秘密之行為，行為人須就其所生之損害負

⁴ 鄭穎，前揭文，第 26 頁。

擔損害賠償責任（第 17、18、20 條），亦得根據同法第一條之概括規定，「於營業交易中，以競爭為目的而違反善良風俗之行為，得請求不作為」。

第二項 日本

日本對於營業秘密之保護原未設有專法，而係藉由民法、刑法加以規範之。惟因營業秘密與民、刑法所規定之構成要件，多數不易完全符合，再加上經濟、產業發展日新月異，有必要提供營業秘密完善之保護，遂於 1990 年透過修正不正競爭防止法，明訂營業秘密之定義、要件與救濟方式，並具體列舉六種侵害行為之態樣。其後，1993 年雖再次修正競爭法，但就營業秘密部份未有修改⁵，故本文仍以 1990 年新增訂之第一條第三項、第二條就營業秘密之規定加以論述。

一、營業秘密之定義與要件

依據日本不正競爭防止法第 2 條第 4 項規定，營業秘密係指被「視為祕密而予以管理之生產方法、販賣方法及其他不被公眾所知悉，且對事業活動有用之技術上或營業上之情報」。由此可知，營業祕密在法律上必須具備三項要件：

1. 秘密性：即該營業秘密尚未公諸於世。此要件與經濟間諜法同，係指相對性之秘密性而言。
2. 經濟性：或稱為有用性，該秘密須係對於生產方法、

⁵ 幸志中，「日本不正競爭防止法簡介」，公平交易季刊，第 5 卷第 1 期，第 121-125 頁，民國 86 年 1 月。

銷售方法及其他事業活動有用之技術上或營業上之情報。蓋法律所欲保護者應為企業活動中具有經濟價值之祕密，而非企業之一切祕密，是故，對於企業之財務、服務、生產、販賣、研究開發及改進經營效率等具有利益之情報，方有可能構成營業祕密，例如設計圖樣、研究資料、顧客名冊、販賣目錄等。至於經濟價值之有無則須依客觀標準決定，以符合其立法出自經濟考量之原意。另外，對於大量投資經費及人力於研發工作的日本企業而言，消極資訊因可避免其他企業發生重複錯誤，浪費研發成本，故亦符合此處具有經濟價值之要件，而成為受保護之營業祕密。

3. 祕密管理：即經濟間諜法所要求之保密措施而言。

二、 侵害行為之類型

依日本「不正競爭防止法」第 1 條第 3 項之規定，營業祕密之侵害行為態樣有下列六種⁶：

「...保有營業祕密之事業（以下稱為保有人），因下列各款行為之一（以下稱為不正行為），致其營業上利益有受損害之虞者，得請求停止該不正行為或防止之：

1. 以竊盜、詐欺、強迫或其他不正手段取得營業祕密之行為（以下稱為不正取得行為），或取得後之使用或洩漏行為（包括在保密狀態下洩漏給特定人之情形，以下同）。
2. 明知或因重大過失而不知有不正取得行為介入而取得營業祕密之行為，或取得後之使用或洩漏

⁶ 曹永遊，前揭文，第 125 頁。

行為。

3. 取得營業秘密後，明知或因重大過失而不知有不正取得行為介入，而使用或洩漏營業秘密者。
4. 意圖不正競爭或其他不正利益，或以加損害於保有人為目的，將保有人所揭示之營業秘密予以使用或洩漏之行為。
5. 明知或因重大過失而不知有營業秘密之不正洩漏行為或不正洩漏行為介入而取得營業秘密之行為（此係前款所規定之洩漏行為及違反法律上保密義務之洩漏行為，以下同），或取得後之使用或洩漏行為。
6. 取得營業秘密後，明知或因重大過失而不知有不正洩漏行為，或有不正洩漏行為介入而使用或洩漏營業秘密之行為。

分析上述之條文可知，日本不正競爭防止法將侵害行為之態樣統稱為「不正行為」，其係由「取得」、「使用」及「洩漏」三行為所構成，且該法對於此三種侵害行為之違法性評價並未做層次性之差別待遇，而一律同等禁止之。換言之，並未賦予「取得」行為較低之不法內涵，而賦予使用或洩漏行為較高之不法內涵，因此只要犯罪者有「取得」之不法行為即須受到制裁，不以其達到使用或洩漏階段為必要。茲分析如下：

（一）竊取等不正取得類型（第一款）

本款係規範產業間諜等不正行為而設之規定，凡行為人以不正手段「取得」營業秘密之行為，及取得後自行「使用」或「洩漏」該營業秘密之行為，均在

規制之範圍內。

就「取得」行為而言，條文所提及之「以竊盜、詐欺強迫或其他不正手段取得營業秘密」，僅為不正手段之例示規定。而所謂「其他不正手段」，除該當於刑法之竊盜、詐欺外，尚包括依社會通念被認定具有同等違法性或違反公序良俗之行為。至於行為是否違反公序良俗，則應以商業倫理為基準，視行為手段與目的、保有人管理狀況、營業秘密之型態、保護利益重要性等因素具體判斷之。又因營業秘密具有非移轉性質，故以違反保有人之意思複製、開拆書信、閱覽記憶、竊聽、以網路入侵之方式下載或以暴力、脅迫等方式取得營業秘密之內容者，均屬於此處之不正手段。

就取得後之「使用」或「洩漏」營業秘密之行為而言，成立本款者以取得手段具有不正性為前提。此處「洩漏」行為包括將營業秘密向不特定人公開，或在不自喪失其秘密性之狀況下告知、洩漏給特定人。

（二）自不正取得者轉得--自始惡意類型（第二款）

本款係為制裁自始惡意取得者所設之規定。即行為人於取得營業秘密之際，明知或因重大過失而不知有第一款所規定之不正取得行為介入而仍予「取得」，或取得後之「使用」或「洩漏」行為而言。若以刑法觀之，第一款係相當於刑法之正犯，本款則相當於贓物犯。本款之行為包含第三人(丙)之轉得人(丁)之使用或洩漏行為，例如甲乃營業秘密之所有人，而乙為以不正手段取得之人，丙係自乙惡意轉得知第三人，丁則係從丙受讓營業秘密再轉得人。

構成本款之要件有三：

1. 須先有不正取得營業秘密行為之介入

所謂「不正取得行為之介入」，係指營業秘密從所有人輾轉流通至本款行為人的過程中，有某階段涉及不正取得行為而言。是故，不論係直接自不正取得人取得營業秘密，或間接自其他第三人取得者均屬本款規制之範圍。然倘若途中介入善意、無重大過失之第三人時，其後手之惡意取得人是否仍應負本款之責？對此應從營業秘密之特性加以分析，非可逕行適用民法善意取得原則。蓋因營業秘密為無形之資訊，非有體物，並非民法上所有權之客體，不適用一物一權主義，而可同時為複數主體共同享有利用，即使遭他人不法取得，所有人對營業秘密管理利用之權並不因此而喪失。準此以觀，營業秘密遭不正取得之過程中倘發生有善意取得之情況，仍不生營業秘密「權利」終局歸屬之問題，故營業秘密所有人仍保有營業秘密之所有權或利用權，自有受保護之必要，故營業秘密流通過程中之事後惡意取得人仍應負本款之責，而不能以其前手為善意取得而主張免責⁷。

2. 明知或因重大過失而不知有此不正行為

因營業秘密未具有公示性質，過度保護恐有危及資訊交易安全。故本款行為人主觀上須出於惡意或重大過失，始該當本款之要件，倘為輕過失之行為則不在此限。所謂「惡意」，係指明知不正行為之存在；所謂「重大過失」，係指顯然欠缺交易上必要之注意義務，致未認識不正取得介入之事實，例如未經調查即向來歷不明之人以低價取得重要之營業秘密。

⁷ 曹永遊，前揭文，第129頁

3.轉得行為或取得後之使用或洩漏行為

此與前述（一）內容同。

（三）自不正取得者轉得類型一事後惡意(第三款)

本款係用以制裁事後惡意轉得者，即行為人於取得營業秘密之際，善意或無重大過失不知有第一款之不正取得行為介入，而於取得後始明知或因重大過失而不知此等不正行為，但仍「使用」或「洩漏」該營業秘密而言。本款與前款之差異在於故意或重大過失之時點不同，一在取得營業秘密之際，一在取得營業秘密行為之後。是故，因善意或無重大過失取得營業秘密之人，事後因情事變更為惡意者，須對其轉換為惡意後之使用或洩漏行為依本款負責。

（四）誠信原則違反類型(第四款)

本款係規範基於營業秘密所有人之信賴而正當取得營業秘密之人，違反誠信原則之義務而予以「使用」或「洩漏」之行為，茲分析如下：

1.營業秘密須歸屬於所有人

根據本款規定，行為人係因所有人之揭示或授權而取得營業秘密，是故，以該營業秘密歸屬於保有人為前提。

2.行為人須負誠信原則之義務

此處營業秘密保有人與受領人間誠信原則之義務，係基於法律行為或法律規定所產生，前者如雇傭、轉包或授權契約等債權關係所生之義務，後者如我國刑法第316、317條之依法令負有守密義務者。前者之適用

範圍，經當事人合意，通常不僅及於契約關係存續中，亦存在於締約準備階段或契約終了後。為此，該義務之發生和內容應非漫無限制，而係斟酌當事人間信賴關係程度、營業秘密所有人或受領人之利益、營業秘密態樣等因素，在合理範圍內拘束當事人之誠信義務，以避免一味保護營業秘密所有人之經濟利益，而造成商業活動或轉業自由之不當限制。

3.行為人主觀上須有意圖不正競業或其他不正利益之行為或加損害於保有人之目的

即行為人主觀上須出於特定意圖、目的，違反誠信原則使用或洩漏營業秘密，始構成不正行為。此所謂「意圖不正競業」，係指顯然違反誠信原則上義務而言，而「意圖不正利益」，不論為自己或他人之利益均屬之，「以加損害於保有人為目的」則以行為人有加損害於營業秘密所有人為目的之意思已足，並不以確實造成營業秘密保有人受損害結果發生為必要。

(五) 自不正洩漏者取得類型一自始惡意(第五款)

本款所規範者為行為人於取得營業秘密之際，明知或因重大過失而不知有不正洩漏行為之介入而仍予「取得」，或取得後自行「使用」或「洩漏」之行為。本款基本上與第二款同是制裁相當於刑法贓物犯之行為，差異點僅在於第二款係處罰「不正取得行為之介入」，而本款則係以「不正洩漏行為之介入」為處罰之要件。本款之「不正洩漏行為」包括有：1.該當於第四款所規定之「有意圖不正競業或其他不正利益之行為或加損害於保有人之目的」之洩漏行為；2.違反法律上保密義務之洩漏行為。

(六) 自不正洩漏者轉得類型--事後惡意(第六款)

本款係規範行為人於取得營業秘密，善意或重大過失不知有第五款規定之不正洩漏行為介入，取得後始明知或因重大過失而不知此等事實者，而仍惡意「使用」或「洩漏」行為。

從上述法條之分析可將歸納出日本不正競爭防止法之不正行為可分為下列四大類型，更有助於瞭解該法主要規範之侵害態樣：

- (一)不正取得者之行為(第一款)
- (二)不正洩漏者之行為(第四款)
- (三)事前惡意轉得者之行為(第二、五款)
- (四)事後惡意者之行為(第三、六款)

三、法律效果

(一)刑事責任

不正競爭防止法對於侵害營業秘密之行為人，僅設有民事責任，而無刑事責任。但非謂其毫無刑事責任，而應視行為態樣分別論罪。以竊盜為例，若侵害行為人直接竊取營業秘密所附著之文件、磁片等，該行為應成立竊盜罪無疑；至於行為人以複製方式竊取營業秘密本身者，可否以刑法保護與保護之界線如何，在日本學界則引起相當大的爭議。反對說見解認為：(1)營業秘密之概念不明確，有違刑法「罪刑法定主義」；(2)以刑法保護之將使企業可享有不公開而獨佔利益，則專利制度將流於形骸化，故日本現行刑法尚無以營業秘密為客

體之刑法出現⁸。

（二）民事救濟

日本不正競爭防止法中有關營業秘密之民事救濟，包括有不作為請求權、損害賠償請求權和回復信用請求權三種權利可得行使。

就不作為請求權而言，只須該侵害營業秘密之不正當行為，有危害營業上利益之虞時即得請求，並不以損害確實發生為要件。又請求權人行使不作為請求權時，亦得請求「廢止構成營業秘密不正當之物、因營業秘密不正當行為所產生之物或公營業秘密不正當行為所使用之設備，以及其他為禁止或預防營業秘密不正當行為所必要之措施。」（第一條第三、四項）

此外，行為人因故意或過失以不正當行為侵害他人營業上之利益者，被害人對之有損害賠償請求權（第一條之二第三項）。但不作為請求權罹於時效後之損害，則不得請求賠償，以使法律關係早日確定，並促使被害人儘速行使其權利。而侵害他人營業秘密造成營業秘密持有人營業上信用受損者，亦得依據第一條之二第四款請求回復信用之相當措施。例如由加害人負擔費用在新聞紙上登載道歉廣告等行為。

第三項 台灣

我國在智慧財產權之領域，原先尚欠缺完整之營業秘密保護，而係以民法、刑法與公平交易法之相關規

⁸ 鄭穎，前揭文，第 38-40 頁。

定作為保護的依據，惟或因規範侵害之行為態樣不周延，或因適用對象有限，或因法律效果不直接，且為因應烏拉圭回合談判 TRIPS 協定對營業秘密之保護，故為建立當前產業競爭與經濟環境，故制訂了「營業秘密法」，於八十四年十二月十六日公佈施行⁹。該法對於營業秘密之定義、侵害之態樣、救濟等均有詳盡的規定。然我國營業秘密法就營業秘密之侵害行為並未如經濟間諜法，對於侵害行為直接科以刑事責任，而僅提供民事上之救濟，是為柔性立法¹⁰，至於刑事責任之部分，則須就侵害之態樣，依據刑法和公平交易法相關規定之適用，認定其刑事責任。因此本節將以營業秘密法為主軸，分析營業秘密之定義、要件與侵害行為之態樣，並輔以公平交易法、刑法之相關規定說明侵害營業秘密之刑事責任，以瞭解我國營業秘密法與經濟間諜法之相同或相異之處。

一、營業秘密之定義與要件

根據營業秘密第 2 條規定，營業秘密係指「方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊」。因此，各類資訊本身，不論是否經過處理皆有可能構成營業秘密，且不論係儲存於何種媒介，如以錄影帶、磁碟片或磁帶等媒介，或以何種形式表示，如以文字、圖案、數字或表格等方式，亦包括無形或有形資訊均屬之。而得以成為本法所保護之營業秘密仍須符合一定之要件：

⁹ 法律案專輯第一百九十一輯-經濟(四十)-營業秘密法案，立法院秘書處編印，第 3 頁，民國 85 年 2 月初版。

¹⁰ 郭懿美，「兩岸智財權保護環境之發展淺析」，1999 全國智慧財產權研討會論文集，國立交通大學法律中心主編，第 271 頁，民國 88 年 11 月 25 日。

1. 非周知性

此所謂非周知性係指「非一般涉及該資訊之人所知者」，此與美國統一營業秘密法規定「非他人所公知」或日本不正競爭防止法規定「不被公眾所知悉」僅指一般人不同，而係採關稅貿易總協定烏拉圭回合談判「與貿易有關之智慧財產權」協定較為嚴格的「業界中人標準」¹¹。惟此非周知性，有稱之為「新穎性」，且認為其與專利法所要求之新穎性不同，僅須為「相對性新穎性」已足¹²，然未避免與專利法上的新穎性混淆，本文認為稱「非周知性」為宜。

2. 經濟價值性

即企業對該等秘密之利用，可使其在營業上與對手競爭時，因競爭對手不知悉該資訊或未加以利用之情況下，取得優勢之地位，即可解釋為具有經濟價值¹³，且本法規定此經濟價值，不論實際或潛在者，均可成為營業秘密而獲得法律之保護。

3. 秘密性與適當保密措施

所謂秘密性係表示該資訊只能為特定之少數人知悉，且未洩漏而言，即具有相對秘密性。由於秘密性之取得與維持，不但為與非周知性相涉，且因其秘密性而使得該資訊具有實質或潛在之經濟價值，故秘密性可說是營業秘密最重要之要件之一。根據營業秘密法之規

¹¹ 駱志豪，「TRIP 對營業秘密之保護」，公平交易季刊，第4卷第3期，第70頁，民國85年7月。

¹² 馮震宇，前揭書，第102頁。

¹³ 駱志豪，前揭註11，第71頁。

定，所有人必須「以採取適當的保密措施」，以防止秘密洩漏，若未採取適當之保密措施，而使得秘密資訊為外人或員工不當取得，自無主張營業秘密法之保護。

二、 侵害類型

關於營業秘密之侵害類型，以下就營業秘密法第 10 條及公平交易法第 19 條第 1 項第 5 款之規定，說明如下：

我國仿照德國不正競爭法第 17 條、第 18 條及日本不正競爭防止法第一條之立法體例，於營業秘密法第十條中列示下列五種侵害類型：

（一） 以不正當方法取得營業秘密者

所謂「不正當方法」(本條及包括下述各款)，依第十條第二項規定，係指竊盜、詐欺、脅迫、賄賂、擅自重製、違反保密義務、或引誘他人違反保密義務或其他類似方法等不正當或不公平方法取得他人之營業秘密者，均構成營業秘密之侵害。至於以不正當方法取得該營業秘密之人與營業秘密所有人間，是否有僱傭關係或其他法律關係，則非所問。因此，例如員工未經許可拷貝公司的研發製程、設計或銷售計畫等指定為營業秘密之資料，提供他人或自己利用，而與公司競爭；或是產業間諜竊取公司之機密資料等行為均屬於本款規範之不正當方法。

（二） 知悉或因重大過失不知其為前款之營業秘密，而取得使用或洩漏者

本款與前款之規定不同之處，在於前款係以自己本身有不正當方法取得他人營業秘密者為規範對象，而

本款則以轉得人為規範之對象，即本身並無不正當方法直接取得他人營業秘密之行為。轉得人本身雖無不正當之行為，但為確保營業秘密所有人之正當利益，避免營業秘密繼續被流傳出去，故有本款之必要。因本款所規定之對象畢竟只是轉得人，其本身並無不正當之行為，是以其責任不應過重，本項僅限於知悉或因重大過失不知之情形始須負責，若轉得人為善意且無過失或僅有輕過失，則除有同條項第三款情形外，並不構成營業秘密之侵害。

(三) 取得營業秘密後，知悉或因重大過失而不知其為第一款之營業秘密，而使用或洩漏者

本款與第二款相同處在於避免營業秘密遭他人以不正當方法取得營業秘密後，繼續被傳送出去。至於兩者不同處則在於，第二款係規範轉得人事前明知或因重大過失可得而知之情況，而本款則為規範轉得人取得該營業秘密之初，並不知情，亦無重大過失，而於嗣後才知情之情形。

(四) 因法律行為取得營業秘密，而以不正當方法使用或洩漏

本款係規範如僱傭、委任等雙方法律行為或單方法律行為如代理權等法律行為發生侵害營業秘密之態樣。本款之特徵在於行為人非不法取得營業秘密，而係基於因該等法律關係而「正當取得」營業秘密，顯與前三款之規定不同。然正當取得之營業秘密，若以不正當方式使用或洩漏者，對於營業秘密所有人所造成之損害，或甚較前三款情形為重，是以有規範之必要。

須注意的是，本款並非用於規範受雇人離職後競業禁止之問題，僅係禁止受雇人於離職後將其原僱傭關係

中所取得或知悉之雇用人所屬之營業秘密再予使用或洩漏之情況。惟若受雇人所使用或洩漏者為其於任職前本身已具有之專業或一般知識，因該技能或知識非屬於企業營業秘密之範圍，自不構成營業秘密之侵害。

(五) 依法令有守營業秘密之義務而使用或無故洩漏者

依法令有守密義務之人，雖同以正當方法得知他人之營業秘密，但如使用或無故洩漏所知悉者，亦構成營業秘密之侵害。此所謂依法令有守營業秘密之義務之人應包括營業秘密法第九條與刑法相關之規定。綜合兩者之規定，此處規範之行為主體，包括下列四種特定關係人¹⁴：

1. 公務員或曾任公務員之人，因公務（職務）知悉或持有營業秘密（營業秘密法第 9 條、刑法第 318 條）；
2. 當事人、代理人、辯護人、鑑定人、證人極其他相關之人因司法機關偵查或審理，仲裁人極其他相關之人處理仲裁事件而知悉或持有他人營業秘密者，依法應負守密義務等人（營業秘密法第 9 條）；
3. 醫師、藥師、藥商、助產士、宗教師、律師、辯護人、公證人、會計師或其業務之佐理人，或曾任此等職務之人因業務知悉或持有他人之秘密（刑法第 316 條）；
4. 依法令或依契約有守因業務知悉或持有工商

¹⁴ 林慧蓉，前揭文，第 102-103 頁。

秘密之義務之人（刑法第 317 條）。

準此，舉凡上述之人違反其守密之義務者，均有營業秘密法第 10 條第 5 款之適用。

其次，依據公平交易法第 19 條第 5 款之規定，其係規範事業之不公平競爭行為。按事業不得以脅迫、利誘或其他不正當方法，獲取他事業之產銷秘密、交易相對人資料或其他有關技術秘密之行為，而有妨礙公平競爭之虞。至於事業如有藉由國外參展或與國內外事業合作機會，在國外竊取他事業之營業秘密，而在本國或外國製造相關產品，嗣後在國內市場銷售者，該利(使)用行為是否屬於本款規範之對象？公平交易委員會於 1995 年 5 月第 188 次委員會決議，透過法律之論理解釋原則認為，「事業在國外以不正當方法獲取他事業營業秘密，而在國內利(使)用該營業秘密者，有下列三種情形：(1)利(使)用行為之行為人與獲取行為之行為人為同一人者，該利(使)用行為違反公平法第 19 條第 5 款規定；(2)利(使)用行為之行為人與獲取行為之行為人不同，而有犯意聯絡形成共犯者，該利(使)用行為亦違反公平法第 19 條第 5 款規定；(3)利(使)用行為之行為人與獲取行為之行為人，雖無犯意聯絡但對該不正當獲取行為明知或因重大過失而不支者，則該利(使)用行為違反公平法第 24 條規定。」¹⁵故此類在國外竊取他事業營業秘密，而在本國或國外製造、生產相關產品之不法行為，應分別其侵害態樣，列入本款或公平法第 24 條規範之對象。

¹⁵ 蘇宏文，從永豐公司商業間諜案看我國營業秘密之保護（下），網路資訊，第 70 期，第 107 頁，民國 86 年 9 月。

三、法律救濟

(一) 民事責任

營業秘密侵害之救濟，依據營業秘密法之規定，包括有：1.排除侵害請求權(第 11 條第 1 項前段)；2.侵害防止權(第 11 條第 1 項前段)；3.損害賠償請求權(第 12 條第 1 項)。該規定賦予營業秘密所有人與不動產、動產受侵害時相同之請求權，可知其提供給營業秘密所有人相當大之權利，因此在營業密之認定上，應該保持審慎之態度，以避免造成商業自由之過度干涉。此外，依據營業秘密法第 13 條之規定向侵害人請求損害賠償，且侵害行為如屬故意，法院得因被害人之請求，依據侵害情節，酌定損害額以上之賠償。但不得超過已證明損害額之三倍。此種酌定損害額以上之賠償，乃屬懲罰性損害賠償，藉以遏阻惡意侵害營業秘密之不法行為。此外依據，民法新增訂第 245 條之 1 第 1 項第 2 款之規定，「契約未成立時，當事人為準備或商議訂立契約而有左列情形之一者，對於非因過失而信契約能成立致受損害之他方當事人，負賠償責任：知悉或持有他方之秘密，經他方明示應予保密，而因故意或重大過失洩漏之者」。此規定將提供企業於技術授權契約簽訂前，被授權人接觸授權人之技術進行價值評估時，對於授權人技術或機密資料之保障，仍得作為侵害營業秘密民事救濟之依據。。

此外，依據公平交易法第 19 條第 5 款規定：「以脅迫、利誘或其他不正當之方法，獲取他事業之產銷機密、交易相對人資料或其他有關技術秘密之行為，而有妨礙公平競爭之虞者，事業不得為之。」如事業違反該規定，致侵害他人權益者，被害人得請求除去之；有侵害之虞者，並得請求防止之；事業違反本法之規定，至

侵害他人之權益者，應負損害賠償責任。此係公平交易法對於侵害營業秘密所規定之民事責任。至於公平交易法與營業秘密法兩者適用之關係為何？因兩者均以保護營業秘密為目的，若限制其適用，則另一法律將形同具文，故當事人應同時可主張營業秘密法及公平交易法所規定之請求權。惟公平交易法於「有妨礙公平競爭之虞者」始得適用，該要件較為抽象而不易證明，因此，營業秘密所有人當以選擇營業秘密法所規定之請求權較為容易。

（二）刑事責任

由於我國營業秘密法對於不當侵害他人營業秘密之行為僅設有民事救濟規定，而未設有刑事責任，但此非謂侵害他人營業秘密之行為即無任何刑事責任，行為人就營業秘密法第十條規定之五種侵害行為，是否應負刑事責任，應視其犯罪事實，分別適用刑法、公平交易法之規定。以下分述之：

1. 洩漏工商秘密罪（刑法第 316、317、318 條）

刑法所稱之「工商秘密」，其範圍相當廣泛，包括個人之活動或其社會經濟活動之秘密¹⁶，因此解釋上應包括營業秘密法所稱之營業秘密。依據營業秘密法第 10 條之規定，依法令有守營業秘密之義務，而使用或無故洩漏者，成立侵害營業秘密之行為。又依同法第九條規定，依法應負守密之義務者，包括公務員因公務；當事人、代理人、辯護人、鑑定人、證人及其他相關之人因司法機關偵察或審理；仲裁人極其他相關之人處理仲裁事件而知悉或持有他人營業秘密者，依法應負守密之義務。此範圍與刑法之規定不盡相同，其中公務員洩

¹⁶ 林山田，刑法特論（上），自版，第 190 頁，民國 78 年 9 月。

漏公務所知悉之工商秘密者，應適用刑法第 318 條並無疑問。至於前開所提及之其他依法令負有守密義務之人，若有無故洩漏之情事，是否應受到刑法之規範，則須依個案認定其是否因業務而知悉或持有該工商秘密，如該等秘密非行為人於業務上知悉或持有之物，則行為人其後雖有交付或洩漏於他人之行為，但仍與刑法第 317 條之要件不符¹⁷。又營業秘密法第 10 條第 2 項所規定侵害行為中所稱之「違反保密義務」，除了上述依法令有守密義務者外，若營業秘密所有人與行為人於訂立僱傭或委任契約時增列保密條款，要求相對人就其因業務所知悉或持有之營業秘密須負保密之義務時，則亦有刑法第 317 條之適用。唯本罪處罰之對象本質上為身份犯，且侵害態樣限於「無故洩漏因業務知悉或持有工商秘密」，行為人若欠缺法規所規範之義務，或所洩漏者非業務所知悉之工商秘密，則與本罪構成要件不符，在面對局外人之「產業間諜」恐力有未逮¹⁸。

2. 洩漏電腦秘密罪（刑法第 318 條之 1）

按無故洩漏因利用電腦或其他相關設備知悉或持有他人之秘密者，為洩漏電腦秘密罪。由於現今電腦資訊之發達，大多數的人往往會利用利用電腦或相關設備處理自己或公司之資料，因而利用電腦或其他相關設備之人，有更多機會知悉或持有他人之秘密，其無故洩漏此等他人之秘密，自應加以處罰，而此類以電子方式所從事之犯罪行為，亦可謂為侵害營業秘密之不當行為之一。以網路駭客為例，利用連結網路之電腦或其他相關設備，竊取某公司之營業秘密後，將其洩漏給競爭對手

¹⁷ 蘇宏文，同前註 15，第 107 頁。

¹⁸ 鄭穎，前揭文，第 43 頁。

或任意散佈，造成公司損害者，自有本條之適用。

3. 竊盜罪（刑法第 320 條）

按意圖為自己或第三人不法之所有，而竊取他人之動產者，為竊盜罪，是構成竊盜罪之二大構成要件為「意圖不法所有」及「竊取他人之動產」。行為人若竊取營業秘密所附著之文件、圖表、磁片等有體物者，則著重於該營業秘密有體物化之移轉行為，對於違犯者應論以竊盜罪無疑¹⁹。惟行為人若以無形侵害方式，例如影印、下載等方式知悉該資訊之內容而洩露或傳達，並未取得前開營業秘密所附著之有體物時，因營業秘密本身具有非移轉性與非排他性兩項特質，故侵害行為人雖然取得該營業秘密之內容的持有支配關係，但另一方面，營業秘密所有人並未因此而喪失對其利用可能性及持有支配關係。此種特性與傳統財產所稱之「物」有所出入，且與竊盜罪保護因占有侵奪，而破壞原所有人的持有支配關係建立新的持有支配關係概念不合，故難以解釋營業秘密本身得成為傳統竊盜罪之客體，故不可能成立「竊取營業秘密」之犯罪²⁰。故營業秘密法第十條第二項規定之「不正當方法」中所包括竊盜，於此應解釋為就營業秘密所附著之文件、圖表、電磁記錄等物品之竊盜，而非指對營業秘密之竊盜。

再者，竊取營業秘密之行為若發生在我國領域外，是否與美國經濟間諜法同，可依據竊盜罪處罰行為人？答案是否定的。蓋因竊盜罪之最輕本刑非為 3 年以上有期徒刑，依刑法第 7 條規定之反面解釋，中華民國人民縱使在中華民國領域外有竊取營業秘密之犯行，亦無從

¹⁹ 黃朝義，論經濟犯罪及其對策，法學叢刊，第 169 期，第 45 頁，民國 87 年 1 月。

²⁰ 黃榮堅，刑法問題與利益思考，月旦出版公司，第 310 頁，民國 84 年初版。

適用刑法加以論罪科刑。類此涉外侵害營業秘密之案件，適用上不免有所不足，無法與美國經濟間諜法廣泛之管轄相提並論²¹。

我國刑法於民國 86 年 10 月 8 日通過電腦犯罪之關聯法案，其中將電磁記錄列入刑法第 323 條規定之擬制動產，可見刑法有關「物」之概念正逐步擴張。該修正似乎認為竊取無形營業秘密可以竊盜罪論處，一反傳統見解。惟所謂電磁紀錄以動產論之概念為何，修正說明並未說明，導致在解釋上不無疑義。有認為所謂依據立法定義電磁紀錄並非僅指被記載之資料，而係指與被載資料相結合之實體物而言。惟若此處電磁記錄係指電磁記錄的實體物，則無庸另以法律擬制²²。若將其解釋為電磁記錄所內涵之抽象意識內容，誠如上述所言，該資訊所具有非移轉性與非排他性之特徵與傳統竊盜罪之「物」有異，若對之以無形方式侵害者，至多以重製方式為之，又與竊盜罪之竊取定義有違。故有學者主張不妨將竊取重新定義為，未經持有人同意而建立新的持有支配關係²³，始得以竊盜罪規範此等侵害營業秘密之行為。

立法者將已存在之基本刑法原則來解釋電腦犯罪，無法一體適用，所產生之問題，均有待司法機關做最後決定。但無庸置疑的是，此種侵害行為對於營業秘密所有人所造成之損失程度，並不亞於竊取有體物，因此智慧財產權犯罪應就其特徵於營業秘密法中增訂刑責，以解決無形財產在現行法上所產之疑慮。

²¹ 蘇宏文，同前註 15，第 106 頁。

²² 鄭穎，前揭文，第 46-47 頁。

²³ 黃榮堅，前揭註 20，第 312 頁。

4.背信罪（刑法第 342 條）

按為處理他人事務，意圖為自己或第三人不法之利益或損害本人之利益，而為違背其任務之行為，致生損害於本人之財產或其他利益者，為背信罪。營業秘密所有人之受雇人、受任人，係為營業秘密所有人處理事務之人，其若有意圖為自己或第三人不法之利益或損害本人之利益，而違背其任務將其職務或基於委託所知悉之營業秘密，自行利用或販賣給他人時，則將成立本罪。

論者尚有引用侵佔罪為處罰之依據，為與竊盜罪同，係以營業秘密所附著之媒介為犯罪之客體，茲不再贅述。

綜上所述，營業秘密之侵害故可依據犯罪事實，依據刑法相關規定加以規範，然繫於營業秘密本身之特質與侵害行為態樣，在適用上爭議頗多，故日後在修法或立法上若有意單獨明文規範時應一併考量之。

5.公平交易法

公平交易法對於營業秘密同時提供了民事與刑事上之保護。就刑事責任而言，事業違反公平交易法第十九條第五款者，依據同法第三十六條之規定，違反者經中央主管機關命其停止其行為而不停止，處行為人二年以下有期徒刑、拘役或科或併科新台幣五十萬元以上罰金。但公平交易法以「產銷機密、交易相對人資料」為保護客體，與營業秘密法所稱之營業秘密並不盡相同；該法以「事業」為規範對象，不及於一般之個人，且其行為須有妨礙公平競爭之虞者始為規範之對象。由於此等附加限制使得公平交易法對於營業秘密所有人之保

護並不充足，對此，日後在行政或立法修正上有必要詳加斟酌²⁴。

第二節 與經濟間諜法之比較

比較美國與日、德就營業秘密保護體系可知，日、德兩國將侵害營業秘密之行為視為不正競爭行為類型之一，故以不正競爭防止法規範營業秘密侵害行為，而對其侵害行為之評價，則以維護公平競爭之秩序為主，立法者對之採取合併立法方式，無庸另行制定一部保護營業秘密之專法。相較於美國，因其對於營業秘密之保護緣起於信賴關係或契約責任之違反，逐漸發展出商業侵權之概念，同時因營業秘密本質上有別於一般有體財產權，故對於此種特殊侵權行為遂有必要透過單獨立法之方式，將法院所為之判例見解予以統一、整理，使能達到周延保護營業秘密之最終目的。至於我國而言，我國本屬大陸法系之立法結構，立法者於制定公平交易法之際，將營業秘密侵害類型一併列入法條之中，但卻因以公平交易法保護營業秘密之效果不彰，再加上國際規範 TRIPS 之影響，遂將營業秘密之保護予以單獨立法，對此使得我國與美國在立法體系上相同。惟不論採取單獨立法或合併立法，各有其不同功能與定位，並無孰優

²⁴ 若一行為違反營業秘密法，同時構成公平交易法所禁止之行為，應可認為以公平交易法為特別規定，優先被適用。謝銘洋、蘇宏文、許智誠、張凱娜合著，「營業秘密法-經濟部重要施政計畫執行暨輔導成果叢書」，經濟部中央標準局出版，民國 85 年 5 月，第 7 頁，轉引自林慧蓉，「論網際網路資訊安全與隱私之保護-以營業秘密之保護為中心」，註釋 31，第 126 頁。

孰劣之說²⁵。

至於規範內容而言，由於美國為了維護商業倫理，保護其企業永續發展與國際競爭力，防止外國政府或企業利用不法之方式獲取美國廠商之營業秘密，並填補原有法律適用上之缺失，國會遂立法通過經濟間諜法，明文規範經濟間諜罪與竊取營業秘密罪，並對於侵害行為人改課以刑事責任，使得行為人之法律風險從過去單純的民事責任，擴大為刑事責任。再者，經濟間諜法對侵害行為之方式不但包括傳統之竊盜類型，同時為配合營業秘密之無形性特質和電腦資訊化所衍生之新型態之犯罪方式，特別加入非傳統之竊盜方式，即在未剝奪營業秘密所有人對資訊之所有權情況下，以拷貝、複製、下載等無形侵害之方式取得或使用該資訊之內容者，一併列入本法禁止之範圍。對此，相較於日本而言，其不正競爭防止法對於營業秘密之保護僅有民事救濟，並無刑事處罰。雖其後刑法修正草案第三百一十八條擬制定，「企業之職員或從業員，無正當理由，將有關其企業之生產方法或其他技術之秘密洩漏於第三人者，處三年以下有期徒刑或 50 萬元以下之罰金。曾居此等地位之人，因違反保守企業生產方法或技術之法律上義務，而洩漏第三人者亦同。」。對該修正草案，業界為維護其經濟利益多採肯定態度，學界則認為草案中「秘密」定義並不明確，有違罪刑法定主義；以刑法保護保護企業之營業秘密而使其享有獨佔權，將架空專利權等。故目前日本並未有處罰侵害營業秘密本身之刑法規定。再者，德國不正競爭法立法背景與美國經濟間諜法相同，對於營業秘密之保護兼採民事與刑事救濟；在侵害行為之規範內容上，也同樣規範資訊犯罪之類型，可謂兩者

²⁵ 徐遵慈，前揭文，第 99 頁。

關於營業秘密之保護，除上述立法體系不同外，就規範內容大致相同。至於我國而言，由於我國營業秘密法係仿照德國不正競爭法與日本不正競爭防止法所制定，因此侵害類型大致與兩者相同。我國營業秘密法並未直接對於侵害行為設有刑事責任，而是視其行為分別依據刑法、公平交易法相關規定規範之。惟與經濟間諜法相異之處，即在於經濟間諜法將無形侵害營業秘密之行為，例如下載、拷貝、傳送等均列入處罰範圍；而我國刑法相關規定，例如竊盜罪，則因此等無形侵害與傳統構成要件不符，自現行法無法有效規範此等犯罪行為，因此若欲將此等侵害營業秘密行為科以刑事責任，則應直接於營業秘密法中增列，以有別於一般傳統財產犯罪。

綜上所述，日、德、我國與美國經濟間諜法關於營業秘密之保護，本於其發展沿革與政策不同，除了就營業秘密之定義、要件相同外，在立法體系、規範內容、法律責任均有所不同。

美國政府與企業在全球市場中一直維繫著緊密的夥伴關係，美國政府的政策即是協助企業維護其營業秘密，給予其從事研發創新的誘因，扮演經濟利益保護角色，也因此經濟間諜法將侵害營業秘密從原本當事人處分之民事救濟變革為刑事案件，引發國家公權力介入私人民事糾紛。智慧財產權已經取代以往的關稅壁壘，成為商戰的新焦點，激烈的產權爭奪戰有蓄勢待發之。因此未來各國政府如何修改不合時宜的法令，關於營業秘密保護會朝向經濟間諜法模式發展以增加刑罰，或加重民事賠償責任等，以確實保障企業的研發成果，仍有待觀察。但無庸置疑的是，企業與國外公司或團體從事任何商業活動或技術引進，均應將所可能涉及的法律層面一併評估，以降低或避免誤觸法網，而喪失市場先機、

損及商譽，或甚而影響我國在國際上的形象。

第五章 案例分析

第一節 起訴案例之介紹

經濟間諜法正式實施以來，由於本法首次對於侵害營業秘密者科以刑事責任，增加與美從事商業活動時之法律風險，故備受各方重視。茲介紹美國最近發生之案件，並分析永豐案之判決，俾完整了解經濟間諜法之執行。

一、United States of America V. Patrick and Daniel Worthing (Criminal No.97-9, W. D. Pa. December 7,1996)

該案之事實略為，被告Patrick為PPG公司雇用人員。其利用工作機會竊取PPG公司光纖研發機密之研發資料，並意圖將該資料販售給康寧公司(Owens-Corning)。隨後為康寧公司與聯邦調查局合作逮捕之。檢察官依據經濟間諜法第1832條第a項第1、3與5款之規定起訴，法院遂於1997年6月5日以被告認罪分方式，判處15個月的有期徒刑¹。

二、United States of America V. Kai-Lo Hsu, et.,(Criminal No.97-CR-323,E.D.Pa.)²

國內永豐紙業公司人員被控意圖以不法方式，向佯裝必治妥公司員工之聯邦調查局探員，購買有關Taxol

¹ R.Mark Halligan,Esq., "Reported Criminal Arrest under the Economic Espionage Act of 1996", <http://www.execpc.com/~mhalign/indict.html>

² <http://www.paed.uscourts.gov/>

之營業秘密。聯邦大陪審團遂以「意圖竊取營業秘密」(U.S.C.1832(a)(4))、「共謀竊取營業秘密」(U.S.C.1832(a)(5))、「共謀從事商業賄賂」等11項罪名，正式起訴涉案三人，法院並同時對於目前人在台灣的周華萍發出拘捕令。本案美國檢方於去年（1999年）1月28日主動向法官申請撤銷對何小台有罪之指控，同年四月正式判決何小台無罪；至於徐凱樂則因其於今年3月31日以當庭認罪來換取減刑，法院於7月13日輕判徐二年管束釋放、罰款三萬美元。關於本案之事實、爭點、評析等將於下節完整說明之。

三、United States of America V. Pin Yen Yang et. al.,(Criminal No.97 CR288,N.D.Ohio September 4,1997)

繼永豐案後，四維公司負責人楊斌彥及其女楊慧貞（任研發部專案經理）遂於同年9月4日遭到FBI以涉嫌竊取美商艾佛瑞·丹尼森公司(Avery Dennison Corporation)商業機密為由逮捕，並以50萬美元交保候傳。嗣後美國司法部檢察官以經濟間諜法第1832條及州際傳輸盜用財產法第2315條等21項罪名起訴楊氏父女。

丹尼森公司係美國國內最大的黏性接著產品製造商之一，生產郵票及標籤等產品，與我國四維公司生產同類產品，兩者似乎處於競爭之地位。本案據調查顯示，丹尼森公司一位華裔化工研究人員李天宏(Ten Hong "Victor" Lee)，自1989年起便陸續提供其公司「高度敏感極高價值的製造資訊與研究計畫」給四維公司，並因此而收受四維公司所支付之15萬美元做為顧問費用。

本案聯邦調查局同樣以誘捕行動，先讓李天宏現

身，再牽引出楊氏父女。在1997年1月由聯邦調查局佈局一場丹尼森公司內部會議，李天宏與在場之他人故意被告知現場有一關於該公司遠東計畫之機密文件夾。其後隱藏之閉路電視系統將李天宏接近該文件之舉動一一記錄，其於同年3月認罪，並與聯邦調查局合作於同年9月完成拘捕楊氏父女之計畫。聯邦檢察官遂以郵店詐欺、洗錢、經濟間諜法之共謀竊取營業秘密等21項罪名起訴被告。而丹尼森公司亦自行提起民事損害賠償訴訟³。本案於今(2000)年1月5日宣判，四維公司竊取丹尼森公司營業秘密之罪名成立，依據經濟間諜法判處四維公司500萬美元之罰金（最高額）；楊斌彥被判處六個月的家中監禁與罰款25萬美元，緩刑18個月；楊慧真則被判處5000美元與緩刑1年⁴。另外丹尼森公司另行提起之民事賠償，於今年2月5日判定四維公司應支付丹尼森公司1000萬美元損害賠償，和3000萬美元懲罰性賠償⁵。

四、United States of America V. Steven Louis Davis, Criminal No.97-00124(D.C.M.D.Tenn,1997)

本案被告Davis係田納西一家Wright公司的製程控制工程師。在1996年間知名刮鬍刀廠牌吉利(Gillette)公司因業務需求聘僱Wright公司協助新一代剃刀-Mark系統，Davis正是該計畫領導人。同年9月底Wright公司應吉利公司之要求撤換了Davis的職務。然而Davis卻罔

³ 同前註1。

⁴ "First corporate sentencing under the economic espionage act Four pillars to pay \$5 million fine", <http://www.usdoj.gov/opa/pr/2000/January/00003.htm>. 「四維企業間諜案 罪名成立」，自由時報民國89年1月7日，第19版。

⁵ 「四維被判賠償4000萬美元」，經濟日報民國89年2月6日，第1版。

顧曾簽署保密契約之事實，將該新設計之營業秘密，下載傳送給 Gillette 公司競爭對手，包括 Bic 公司、美國安全剃刀公司 (American Safety Razor) 等。檢察機關遂以經濟間諜法第 1832 條第 a 項第 2 款未經授權傳輸營業秘密、第 3 款不當持有營業秘密等罪名起訴被告。據報導被告已被判處 27 個月有期徒刑，並對於吉利公司、Wright 公司和吉利公司關係企業附損害賠償責任 1,271,171 美元⁶。

從上述案例可知，美國政府以經濟間諜法起訴之案件，仍僅有商業競爭所發生之竊取營業秘密罪，如同美國 ASIS 所作的調查報告所言，反而以公司內部員工竊取營業秘密之情事所占比例最高，因此業者應加強內部營業秘密之監控與人事管理，避免遭受損害而影響公司發展，對此本文將於第五章詳細說明。

第二節 永豐案判決之評析

一、事實

永豐公司技術指導徐凱樂 (James Hsu)、周華萍 (Jessica Chou) 及交通大學教授何小台 (Chester S. Ho)，涉嫌竊取施貴寶 - 必治妥公司 (Bristol-Myers Squibb Company) 的抗癌藥物 - 汰癌勝 (Taxol) 的營業秘密乙案，根據美國賓州東區地方法院大陪審團起訴書之記載，本

⁶ 勤玉華，美國經濟間諜法案例與順從程序之運用，<http://www.moeaipo.gov.tw/nbs12.ip03j.htm>。 "Gillette Conviction", <http://www.newdimensions.net/headlines/j18.htm>

案緣起於1995年6月7日，被告周華萍開始與喬裝技術資訊仲介之美國聯邦調查局探員書信接觸，其後於1995年8月28日至1996年1月12日間被告周華萍便數度主動向該名密探表示並要求能取得汰癌勝的技術製程與經銷權，在1996年2月27日之面談中周再度表達有意引進生物科技之相關資訊，以發展永豐公司多角化經營之目標，然而該探員卻告訴周，施貴寶公司並無意將汰癌勝之技術與永豐公司分享，周當時便表示或可用金錢向施貴寶公司員工收買該技術。其後的14個月內周又多次與該探員聯繫商討汰癌勝技術移轉事宜，而且在探員之引薦下與自稱願意提供汰癌勝技術的員工簽訂了技術移轉契約，移轉該項技術之對價為40萬美元、股票和權利金。嗣後雙方約定於1997年6月14日在賓州費城四季旅店會面交付汰癌勝之技術。會談過程中為了確認該名施貴寶公司之身份及汰癌勝技術的真正性，被告還曾檢視該員工之公司識別證，廣泛地尋問該項技術之相關問題，該員工遂提出標註施貴寶及機密字樣之文件以資證明。

基於以上之事實，美國司法部檢察官嗣於同年7月10日宣佈起訴。美國聯邦大陪審團裁決以「意圖竊取材營業秘密」(U.S.C.1832(a)(4))、「共謀竊取營業秘密」(U.S.C.1832(a)(5))、「共謀從事商業賄賂」等11項罪名，正式起訴涉案之三人，法院並同時對於目前人在台灣的周華萍發出拘捕令。

二、爭點

本案主要之爭點在於系爭之汰癌勝製程資訊是否為營業秘密。

三、主張

原告主張系爭之資訊為營業秘密，蓋施貴寶必治妥製藥公司因研發制癌藥品--汰癌勝，而取得藥品市場上之優勢，其對於施貴寶公司具有重要之價值性。施貴寶公司為了維護該技術之秘密性已經採取下列措施來維護其機密性：

- (一)所有機密文件均加註「機密」符號；
- (二)所有技術職位之應徵者均被要求審視和簽署保密契約；
- (三)所有機密性資訊僅限於在公司執行職務時使用；
- (四)管制執行Taxol之人員；
- (五)Taxol技術文件與產品所使用之植物細胞均被存放於加鎖之保險櫃；
- (六)所有員工均發給關於安全及保護機密資訊之書面指示；
- (七)對於該公司所贊助培育植物細胞之Phyton公司，並要求其維護該研究之機密性；

綜上所述，該資訊係屬法律所保護之營業秘密無誤。且本案所依據之條文(第1832條第4款)係僅處罰行為人「企圖」(attempt)之犯罪意圖，則檢方只須證明被告有「超過合理懷疑」意圖竊取被告自認存在之營業秘密以足，縱使系爭之客體屬於法律上不能，仍不影響罪名之成立，故被告以此為抗辯之理由實誤解法律之規定，不足採之。

被告則抗辯謂：

(一)營業秘密存在與否係屬本案犯罪成立構成要件之一，而其判斷標準係依據本法第1839條A項之規定，保護之客體必須具備「秘密性」、「新穎性」、「價值性」之要件始可謂為營業秘密。因此，成立營業秘密之先決條件須具有秘密性，尚非屬公眾所知悉之資訊。本案所系爭之汰癌勝，因該產品之相關資訊絕大多數早已於專利、科技資訊報導中問世，應認為其已喪失秘密性，故本案並無營業秘密之存在；

(二)喬裝之聯邦探員於1997年6月14日會議中並未攜帶真正之汰癌勝技術文件，故本案之犯罪事實顯屬於「法律上不能」，縱使被告已經完全依其犯意實行犯罪行為，但其行為仍不構成犯罪，自無違反經濟間諜法可言。

四、判決

美國檢方於去年（1999年）1月28日主動向法官申請撤銷對何小台有罪之指控，同年四月正式判決何小台無罪；至於徐凱樂則因其於今年3月31日以當庭認罪來換取減刑，法院於7月13日輕判徐二年管束釋放、罰款三萬美元。

五、理由

依據本法第1839條之規定，判斷營業秘密是否存在之先決要件為秘密性，而汰癌勝之製程已於70年代問世，至今早已不是機密，故無法依據本法之規定處罰其行為。

六、評析

從本案爭點可知，某一資訊或技術是否為經濟間諜

法所保護之客體，首先必須判斷該資訊是否為營業秘密，亦即分析其是否具備「秘密性」、「新穎性」、「價值性」與「採取合理保護措施」等要件。本案由於系爭之汰癌勝已經以專利方式公開，喪失其秘密性，自非該法所得保護之範圍；相對而言，業者如何就公司本身所擁有智慧財產，依其性質尋求法律保障，在訴訟與求償上，實屬重要。

本案雖以被告徐凱樂庭認罪換取減刑收場，然而第三巡迴上訴法院在審裡中駁回被告以誘補中所使用之文件資料不屬於營業秘密，主張「法律上不能」為抗辯之見解，造成經濟間諜法之意圖犯與共謀犯認定上寬鬆，影響廠商甚巨，於此一併敘明。第三巡迴上訴法院仔細審視經濟間諜法立法意旨與發展沿革後，判決表示國會並不認為准許被告得以法律上不能作為意圖竊取營業秘密的抗辯。蓋若准許被告可引用法律上不能作為防禦方法，則將迫使執法機關使用真正的營業秘密，揭露營業秘密所有人所欲保護之營業秘密，將有違經濟間諜法立法保護營業秘密之目的。故法院明白表示法律上不能不得作為第1832條第(a)項第(4)款與第(5)款之抗辯理由。據此，法院只要有合理的懷疑可資證明被告意欲取得其所相信為營業秘密之資訊者，便足以構成第1832條第(a)項第(4)款意圖犯之罪名，與該資訊實際上是否為營業秘密並無直接關係。此項見解可謂擴大經濟間諜法之適用範圍，值得國內業者特別重視。

第三節 小結

隨著我國高科技產業急速發展，廠商除了投入大量資金研發技術之外，也積極向海外尋求技術移轉，並延

攬海外學人歸國服務。根據報導，我國廠商技術移轉有72%來自美國，有15%來自日本⁷，因此我國與美國在技術移轉方面關係可說是非常密切。經濟間諜法實施後，對我國技術移轉之衝擊便是令業者面臨更大的法律風險，而且可預見的是，在市場開放的自由化遊戲規則下，智慧財產權將成為唯一合法的「市場獨佔權」，因此未來經濟間諜的指控將會越來越多，所以熟悉該法與如何因應不容忽視之。自永豐案之起訴事實觀察，國內業者為了商業利益，在尋求新科技之際，應了解他國法律，並尊重他人研發成果，切勿因一時「貪小」而限自身於犯法泥沼。故業者應該開始正視「技術移轉」的妥善程序，例如與有權移轉技術者洽談技術移轉時，宜向技術所有人洽商最為妥當，若洽商之對象僅為被授權人時，則宜請其出示授權文件，或主動向所有人徵信，以確保技術仲介人之可靠性；或慎選洽談場所；或尋求律師協助等都是技術引進過程中可避免廠商誤觸法律之因應措施。其次，政府為提升競爭力，推動臺灣成為亞太營運中心，建立「科技島」，則政府應加強鼓勵、重視企業研發工作，在相關法令配合與執行上當效法先進國家，並協助業者處理智財權訴訟，期能使我國企業有信心與能力迎接國際競爭之挑戰。關於經濟間諜法之因應對策，第五章將有較為詳盡之說明。

⁷ 「美經濟間諜法僅處罰故意犯」，經濟日報民國87年5月22日，第26版。

第六章 美國經濟間諜法之因應 對策-暨 結 論

第一節 前言

我國近年來積極地發展高科技產業，包括積體電路工業、通訊工業、資訊工業、生物技術產業等領域，業者或尋技術授權、企業購併、現金購買或以外人投資技術移轉等方式引進尖端技術，期能強化現有技術研發水平，提昇企業獲利能力與經營格局。惟這些努力不僅在國際市場對於競爭國造成威脅，亦使歐、美、日等先進科技大本營陷入緊張狀態，深恐其辛勤研發所得不法地輕易移轉至我國業者手中，因此不乏有藉由立法來保障其國內產業，並作為貿易保護之工具，經濟間諜法可謂此趨勢下的產物。而國內廠商近日便相繼面臨有關智慧財產權國際保護之挑戰。從永豐、四維涉嫌觸犯美國經濟間諜法、韓國檢調單位指控南亞侵權案、美商普司通控告翰時等公司侵犯專利權，到華邦遭美商EMI指控專利侵權等，顯示自一九八〇年代全球智財權體系強化以來之趨勢，即擁有大量智財權之國家將廣泛運用之「策略性智財權訴訟」方式，藉由控告競爭對手侵犯智財權、商業間諜等伎倆，來達到打擊干擾對方商譽、商機，或阻止、延緩其進入市場等目的，以搶得先機或壟斷市場。換言之，法律已經成為高科技產業主要競爭手段之一。我國正逐步邁入全球高科技商戰風暴，故預料未來智財權之訴訟與糾紛將會更加層出不窮。

由於經濟間諜法規範內容廣泛與嚴刑峻罰，不論是
目前或將來與美國企業從事技術合作、技術授權或延攬

美籍人士，均有發生觸法之風險。而一旦被控以違反經濟間諜法，就算最後判決結果為無罪開釋，惟訴訟期間對於個人、公司或政府所造成之名譽損失、商機之喪失等卻是無法彌補的。故國內業者應積極共謀因應之道，正視智財權之重要性，並記取國內、外相關業者前車之鑑的教訓，審慎規範並嚴格執行智財權管理制度，除了可規避或降低訴訟風險外，同時也保障了自己的智慧財產權。其次與美國企業進行技術合作、技術移轉時亦應同時注意有無觸犯該法之嫌，以免於重蹈永豐、四維案之覆轍。目前在政府強調提升我國競爭力，並致力建設台灣成為「亞太營運中心」與「科技島」的努力下，企業的競爭力便為政府施政成敗的關鍵之一，故政府應輔導企業從事國際技術貿易行為，避免成為美國經濟間諜法施行下的俎上肉。本章將分別企業與政府兩方面對於經濟間諜法因應之建議加以整理闡述。

第二節 業者因應之建議

由於經濟間諜法係處罰竊盜、收受等不法侵害營業秘密之故意行為，故企業正視經濟間諜法之積極作法即在於建立並徹底實行一套完整的資訊管理與人員之控管辦法，除有助於保護自身之營業秘密外，同時表明公司及其員工係遵守法律規定而無侵害他人智慧財產權之故意，該控管制度即所謂「營業秘密管理」。公司建立營業秘密管理制度之實益在於：(1)符合法律規定之保護要件，俾利主張、利用營業秘密，(2)避免或降低流失本身之營業秘密，影響公司商業競爭力或股票價格，(3)防止未經他人授權之營業秘密，進入公司知識庫，造成感染，(4)建立公司與其員工尊重智慧財產權之態度，並增進兩者間倫理關係，(5)有助於降低營業秘密之爭訟風

險或利於舉證等¹。依據美國聯邦量刑準則(Federal Sentencing Guidelines)之規定，法院對於涉案公司起訴與否或衡量刑罰輕重時，需參酌其營業秘密管理制度之存在與使用程度²，故營業秘密管理制度係設定客觀準則與步驟，將主觀態度予以客觀化，俾防止自身營業秘密之喪失、降低涉訟的可能性與成罪與否之斟酌，為經濟間諜法所創造之新環境中，公司因應該法之基石。

企業所恃之競爭力不外乎資金與技術，而技術往往會帶動資金的投入與累積，因此在瞬息萬變的競爭環境，新技術的取得便成為勝負成敗的重要關鍵。技術的取得大抵有自行研發、技術移轉或授權、成立合資公司、買斷技術或併購等方式，其中技術移轉或授權因可縮短自行研發的時程，節省研發經費或買斷技術之龐大金錢負擔，有助於爭取商機，故較為企業所青睞。技術移轉過程中不免會有因資訊交流而知悉他人之營業秘密之情形，特別是引進美國技術時，稍不留意而取得未經授權之機密資料或落入陷誘，將有觸犯經濟間諜法之風險。是故，公司除了應於內部建立營業秘密管理制度外，更應將所有可能涉及國內、外之法令或政策，落實在技術授權或移轉模式中，作好風險管理。故本節將分別從營業秘密管理制度(對內)和引進國際技術(對外)二方面闡述企業因應經濟間諜法之策略。

¹ 馮震宇，論營業秘密之保護、查核與管理，工業財產權與標準，第57期，第10頁，民國86年12月。

² 美國聯邦量刑準則將判斷公司可責性之基準稱之為遵從計劃(或譯為順從程序)(Compliance Plan)，係指公司制度應與法律精神相符合而言，本文將其意義延申稱為營業秘密管理制度，於此敘明之。另參見勤玉華，美國經濟間諜法案例與順從程序之運用，<http://www.moeaipo.gov.tw/nbs12/ipo3j.htm>

第一項 營業秘密管理制度

一、內部資訊之管理

營業秘密之特色即在於企業必須透過若干保護措施，以維護資訊之機密性，而繼續享有競爭廠商所不知或沒有的優勢。例如可口可樂公司的飲料配方即因備有一套完整的保密措施，才使其市場競爭力歷久不衰。誠如經濟間諜法第 1839 條所述，構成營業秘密的客體極廣，於資訊快速發展之現代社會，營業秘密與非營業秘密若單就外觀並不易區分，故企業於保護營業秘密之首要即確認營業秘密之範圍，並針對其採取相關保密措施，以達到法律所要求之「採取適當保密措施」，以降低流失自身之營業秘密，並可避免將「妾身未明」之技術引進公司，故有效管理公司內部資訊對於企業相當重要。本文將援引國外企業之管理經驗，以作為我國企業建立營業秘密保密制度之參酌。

(一) 確認營業秘密之範圍

承上所述，營業秘密之範圍與存在之態樣相當廣泛，其藉由不同形式或媒介呈現，除研發的新技術、產品或記錄外，行銷計畫、財務報表、會計資料、人事檔案、薪資及聘僱記錄或顧客名單等均屬之，故首先應歸納出公司內部資訊中何者符合營業秘密之要件，並衡諸經濟效益，以確立是否對其採取營業秘密保護之策略。

不論是依據 TRIPS、經濟間諜法或我國營業秘密法之規定，資訊須具備秘密性、經濟價值性與採取適當保密措施方可成為法律所保護之營業秘密，該部份已於本文第二章、第三章敘明，不再贅述。再者，公司對於新

技術是否採取以營業秘密方式保護，因其可避免申請專利過程所需之成本或答辯費用，且只須維持資訊之秘密性便可永久享有獨佔，故公司在確立營業秘密範圍之同時，應評估採取或搭配何種智慧財產權之保護方式，俾利公司享有極大化利潤。公司對於機密資訊或技術採用營業秘密策略保護之考量因素如下³：

1. 該技術他人不易取得或產生；
2. 公司技術領先同業之時間較長，且公司營業秘密制度完善無洩密之慮；
3. 產品生命週期短，經專利審核後對該技術保護之時間已不具功效；
4. 該技術不具專利法定要件，然具有經濟價值亦可列為保密資訊；
5. 技術範圍不易確定，難以申請專利權者；

(二) 內部監控

釐清公司營業秘密之範圍後，便需對之採取適當措施以維護其秘密性。就資訊管理而言，應區分秘密等級，例如標示「極機密」、「機密」、「限閱」、「僅供內部使用」等警告字樣，並針對機密程度或性質制定保密方法；對於內部電腦系統之使用建立偵測監視管理，以限制或追蹤員工或業務上無關人員接觸與取得營業秘密；公司或員工個人對外發表演講或發行刊物應先行審閱其內容，避免發生營業秘密洩漏之可能性；此

³ 吳念祖，樊台齊，「新產品開發之專利權管理策略與作法」，1999 全國智慧財產權研討會，國立交通大學法律中心主編，第 677 頁，民國 88 年 11 月。張凱娜，前揭文，第 88-89 頁。

外，並應就日常工作中員工所棄置之文書、磁片等物品加以留意。

就設備監控而言，公司必須設有全套防盜系統，以電腦設備派專人全天候監視看管整個公司；此外，公司重要管制區域或機房應以磁卡及密碼等操縱方式，限制進出人員，以達充分控制之效果。

(三) 預防外界刺探

為防止公司員工以外之第三人，例如競爭對手的刺探或竊密行為，公司應致力於加強內部監護系統。對外接觸方面應執行門禁管理。訪客參觀廠區時，除登記及配戴識別證外，須由員工親自接待訪客循一定路線參觀公司，而非任其自由活動，並嚴格管制訪客照相或錄影。

二、 人事管理

企業營業秘密之產生、維持與保護，與員工息息相關，且人才為高科技的根本，人才的流動即代表技術之流動，也易促成營業秘密流傳、公開，間接造成產業間諜之事實。依據美國ASIS調查報告指出，侵害營業秘密案件中有 74% 指控案與公司有僱傭契約(在職員工或離職員工，佔59%)或契約合作上關係(佔15%)的個人或團體所為。而以我國為例，世界先進、聯電等公司即於去(1999)年4月間陸續發生離職工程師帶走秘密資料之事件⁴，故公司尤應重視員工「近水樓台」之竊密行為，以避免因此而喪失市場上優勢的競爭地位，且對簿公堂的結果往往是兩敗俱傷。因此，如何教育公司員工瞭解公

⁴ 「離職員工帶走秘密-半導體智財權堪慮」，自由時報民國 88 年 4 月 18 日，第 26 版。

司營業秘密之價值與防止流失自身營業秘密，並在人才進出之際，避免因取得未經授權之營業秘密，發生違反經濟間諜法第1832條第3、4或5款，對此企業於管理營業秘密時應一併規劃。以下分別針對現職員工教育、延攬新進人員與離職員工管理制度三方面說明業者在人事控管所應注意事項⁵。

(一)現職員工

1.簽訂保密契約

對公司內部員工或出資聘任之受雇人，公司須訂定僱傭契約規範相關權利義務。其中除明訂智慧財產之歸屬與加列可能涉及經濟間諜法之條款外，應訂明保密條款，以規範其嚴密的保密義務，避免其將知悉或接觸的營業秘密洩漏予第三人或供自己使用，而產生不公平競爭。簽訂保密契約之實益即在於：(1)透過簽約，可明白宣示公司對機密資訊的保密政策；(2)提醒並加強員工的忠誠觀念；(3)日後若發生違約情事，公

司得據此追究其民、刑事責任⁶。

保密條款之主要內容包括告知義務與保密義務。前者係受僱人告知公司其所擁有，或與他人共有之發明、創作、著作或專門技術，若與前僱主曾簽訂保密契約或競業禁止約定者，亦應一併告知。後者則係指不得於在

⁵ 參見黃俊英、凌儀玲撰，「企業內部營業秘密之保護措施-兼論智慧財產權下的員工管理」，1998 全國智慧財產權研討會論文集，第 222 至 223 頁，民國 87 年 11 月 19 日。

⁶ 蘇宏文，從永豐公司商業間諜案看我國營業秘密之保護（上），網路資訊，第 69 期，第 108 頁，民國 86 年 9 月。

職期間或離職後，將受僱期間知悉之營業秘密，為自己或他人之利益，直接或間接洩漏、告知、交付或其他不法方式移轉他人或供自己使用而言⁷。藉由該契約之簽訂，企業將可瞭解該員工對於前僱主之義務，從而避免任用後所衍生之訟累，亦可產生並加強對企業之忠誠義務，實為公司對於營業秘密保護之重要程序。

2. 製作研究日誌

研究日誌之目的在於使創新技術、設計、概念、方法或歷程得以文字或圖示等方式記錄在可追溯之證據記錄簿⁸。高科技公司之研發單位要求工程師製作研發過程日誌，一方面可控制研發進度、改進作業程序，另一方面亦有助於創作人之權利主張，若發生爭議時，於訴訟中可作為排除故意侵害之舉證，不失為因應經濟經濟間諜法之良策。

3. 教育訓練

公司應將其對於營業秘密的保密政策以書面傳達給員工。此外，應以國際性宏觀之態度來管理自身的智慧財產權，定期透過教育訓練，教授各國智財權法規，宣導員工尊重智財權之觀念。以工研院為例，其內部便制定智慧財產管理及運用綱要，就教育政策分別為定期教育與臨時教育二類。定期教育包括新進人員講習及智權週等；臨時教育則於智財權法令有重大修正或發生侵害智財權事件時舉行⁹。該教育訓練制度可作為他業者建

⁷ 邵瓊慧，「營業秘密之保護兼談企業如何擬定相關條款」，月旦法學雜誌，第 46 期，第 76-76 頁，民國 88 年 3 月。

⁸ 吳念組、樊治齊，前揭註 3，第 675-676 頁。

⁹ 工研院智慧財產管理及運用綱要，參見 <http://www.itri.org.tw/feature/fe-0880420.html>

立保密政策之參考。此外，公司應指示員工以正當方法從事商業活動，並指導其如何發現麻煩，即公司必須告知受雇人於決定某資訊可否加以利用時，除了要求授權人提供來源證明書外，同時務必先行與法律部門研討，以避免收受不法或妾身未明之技術，而發生遭陷誘之情事。

(二)延攬新進人員

公司招募員工，除了應重視其學識、經驗或能力外，應同時查核其工作背景，即瞭解其履歷表所陳述之事項是否可靠及對前雇主之義務。例如保密義務、智慧財產權歸屬問題、競業禁止條款等，避免任用後所衍生之訟累。再者，延攬歸國學人或海外專家學者為我國高科技企業促進技術流通與升級方式之一。為防範企業因雇用華裔人才而被控竊取營業秘密情事再度發生，公司須建立保身之道。對於新進人員所為之面談內容，舉凡：

- 1.該員前雇主為孰？是否曾任職於美國公司，是否具有美國國籍或永久居留權？
- 2.應告知其不得使用原任職公司之營業秘密，否則將有涉入經濟間諜法之嚴重性，並簽署契約以證明其知曉。
- 3.妥處新進員工工作業務與性質，避免其使用前雇主之營業秘密¹⁰。
- 4.交叉確認：公司應主動與其原任職公司作交叉確認，要求前公司提供該員工所簽署之法律文件，例如僱傭契約、保密契約或競業禁止約定等，俾利瞭解該員工

¹⁰ "Raid the Competition for Workers, Not Their Secret", by Gillian Flynn, workforce, pp.123, December 1998.

與前公司間之義務關係，知悉其不得在本公司從事何種業務或技術研發，以徵明公司並非為取得前公司之營業秘密始雇用該員工，或避免日後若發生該員工洩漏前僱主之營業秘密時，公司被法院認定為共犯之麻煩¹¹。

5. 聘請國外顧問或邀請技術專家進行專案研究或演講時，務必留意其研究計畫或演講之內容是否有洩密之疑。
6. 聘僱合約之內容應特別設計，加列可能涉及經濟間諜法之條款。

(三)離職員工

公司對於即將離職之員工，除了辦理交接手續，徹底點收該員工所領借之各種文件或物品外，應實施離職面談，再度提出該員工於當初進入公司所簽訂之契約，告知其離職後應善盡之義務，如保密責任、智慧財產權的保護義務、競業禁止等負有持續性之義務，並設法瞭解其離職之原因與去向。如此一來，不但可徹底防堵企業營業秘密外洩的可能性，他方面亦可掌握該員工之動態，便於隨時注意其有無洩密違約之情形，或可主動聯繫其新僱主，告知該員工與原公司之權利義務關係，亦可收防止營業秘密外洩之效。以 Autodesk 公司竊取 Vermont Microsystems 公司有關係統軟體 Display List Driver 架構之營業秘密案為例，由於 VMI 公司對於重要離職員工仍不斷追蹤其動向，以防止公司營業秘密外洩，並於有侵害之虞者，適時提醒該員所任職之新公司切勿使其涉及侵害營業秘密之工作或職務，凡此均證明

¹¹ 「技術移轉引進人才，當心觸法」，工商時報民國 87 年 2 月 12 日日，第 4 版。

VMI 公司對其營業秘密的長期保護與管理，此也正是 VMI 公司勝訴之最大原因，值得國內業者加

以效法¹²。但同時應避免因此而影響該離職員工之工作權¹³。

三、成立智權單位

有鑑於智慧財產管理事務繁多，所涉及之內容除了技術與商業層面外，尚包括法律層面。蓋營業秘密本身屬於無體財產，如同一般商品具有交易價值，悉賴法律創設與保護。因此，公司建立專職之智權單位已屬勢之所趨。企業所成立之智權單位（或稱為法制室），其法制人員須具備智財權管理能力、技術移轉授權中之交涉能力、智財權評估能力、智財權糾紛之詮釋能力與國際智財權實務處理能力等，且審閱公司所制定智財權相關條款，例如保密契約或雇傭契約等¹⁴。公司將藉由法制室的成立以提昇並強化企業本身體質，未來不論是面臨國內、外企業有關智財權或營業秘密事項質疑或指控時，才能具備事先防範、事後因應之能力。

四、企業合作聯盟

面對外國高科技業者動輒組成上百人的律師團利用訴訟或散發律師警告函之方式藉以打擊或延緩競爭

¹² Autodesk, Inc 竊用 Vermont Microsystems Inc.營業秘密之判決剖析，電通所法務智權園地，民國 86 年 1 月 16 日，<http://www.csl.itri.org.tw/Text/law/86008.htm>

¹³ Marco E. Brown, Electronic Business, "When employees leave", p.43, June 1998.

¹⁴ 「智財權管理 ISO 化-雙效合一」，智慧財產權管理季刊，第 21 期，第 34-35 頁。民國 88 年 6 月。

產品進入市場，我國業者實難招架。業界不妨考慮成立「合作聯盟」，以合力作戰之方式，與外國廠商搏鬥¹⁵，以保障我國業者權益，而非任由外商頻頻對國內廠商指控侵權行為。

第二項 引進國際技術之注意事項

在高科技產業競爭白熱化之情勢下，智慧財產權儼然已經成為商場競爭之利器，因此如何取得智慧財產權當為高科技產業最重要課題之一。我國廠商在面對產業競爭激烈的情勢下，為了突破自身技術瓶頸，取得經濟競爭之優勢，亦莫不採取多元化的技術引進方式或直接延攬海外科技長才，藉以獲取所需的技術。以技術授權方式取得營業秘密之目的，在於經由授權人與被授權人的合作使被授權人節省技術研發時間，而可快速達到技術升級之目標，授權人亦可藉由收取權利金等方式擴大其技術之實質利益，雙方可謂互蒙其利¹⁶。美國為世界高科技領導國，我國業者與其廠商合作從事技術研發、移轉或購買的比例最高，關連性也相對地提高，因此對於技術貿易過程中可能涉及經濟間諜法之範疇之部分均應於授權契約一併設計、考量。

一、確認移轉標的

由於技術移轉之標的，除了營業秘密外，尚包括

¹⁵ 「防杜風暴，企業應主動出擊，維護自身權利」，工商時報民國87年2月9日，第25版。

¹⁶ 馮博生，「技術移轉之型態與契約解析」，1999全國智慧財產權研討會論文集補充資料，第1頁，民國88年11月。

商標專用權、專利權或著作權等，因此，對於所移轉之技術係屬何種智慧財產權？是否已依法定程序取得權利？權利是否在有效期間等均應先行確認與評估，並於契約中界定授權範圍，一方面可確定被授權人之權能，一方面避免侵害他人之技術，作為日後發生爭議時之依據。此外，授權契約簽訂前，對於授權人所提供之技術或資料，應與他方以書面確認該資料之性質，究屬機密或非機密，以避免發生不當洩漏或使用機密技術，有觸法之虞。

二、主動質疑技術來源之合法性

業者於引進技術或營業秘密時，除了企業內部必須先行對該技術作開發或獲利之評估外，應對其來源、可靠性、權利有無瑕疵等事項透過不同管道加以調查。即與海外廠商進行技術移轉之際，任何過程均須嚴謹，且務必找對「本尊」，以避免發生如永豐案遭誘陷之情事。是以，為確認技術來源合法性，可分別就不同授權人型態加以說明之¹⁷。

（一）與個人進行技術移轉

技術擁有者為個人時，被授權人應要求其提出獨立研發之證明。倘若該人剛從某公司離職，則應詢問該技術與原公司之關係，以避免其不法竊取並販賣該公司之營業秘密，使得被授權人觸犯經濟間諜法第 1832 條第 3 款之規定。所有授權過程均應以書面紀錄留存，並簽署技術移轉合約，載明權利聲明書、「智慧財產權保證條款」，即一旦發生智慧財產權侵害之爭議時，由授權人

¹⁷ 同前註 16，第 5-6 頁。

自負其責，以作為日後涉訟舉證之用。

（二）與公司進行授權移轉

技術授權是非常「中央集權」的事情，外國公司都相當重視，故被授權人應要求洽談者以「公司」名義來洽談技術移轉事宜。若接洽者層級過低或該授權行為與其業務顯不相當時，為避免取得未經授權之技術，被授權人除了應主動要求其出具合法授權書，並判斷其真偽，以確定對方係經公司合法授權外，更可主動向公司徵信有無授權之事實存在，以表達合法取得技術之心態。

（三）透過掮客進行技術移轉

被授權人首先應對該技術掮客之背景、資歷及信譽有所瞭解。除了透過周邊人士進行調查外，應要求其提供書面證明其係經過所代表之企業授權，並說明過去成功案例，藉以判斷該掮客之可靠度。而在協商過程中，應儘量避免單獨與對方接觸，於主要議題達成之際，則需技術移轉者、技術接受者與掮客三方到場簽署授權契約，以確保授權行為合法、可靠性。

被授權人除針對洽談者身份徵信以確認技術合法性外，亦可經由移轉價格是否相當加以判斷，將技術移轉建立在「使用者付費」之觀念上，切忌貪小便宜而因小失大。

業者從事技術過程中若發現對方提供之技術或資料為不法取得或未經授權者，應立即停止使用，且不得再持有或洩漏之。蓋經濟間諜法對於明知他人係以不法方式取得之資訊，仍收受、購買或持有者，依據該法第1832條第3款之規定同為處罰之列，故一旦知悉技術移

轉之他方發生違法行為，便應該停止使用或洩漏該資訊，以防止該未經授權之營業秘密進入公司，產生感染作用。對此，公司除了向授權人追究民事責任外，應主動積極、主動地通知營業秘密所有人，並向司法單位告發，用以作為自身無與之共謀竊取或收受他人營業秘密之佐證¹⁸。以美國 Worthing 案為例，被告不法竊取受雇公司 PPG 之營業秘密，且意圖販賣給其競爭對手 Owen Corning 公司。Corning 公司面對被告知兜售行為，不為所動，且警告 PPG 公司其營業秘密遭受侵害之危機，並向聯邦調查局檢舉，促成逮捕

行動之成功¹⁹。本案 Corning 公司可謂採取了正確的措施，若當時知情不報且購買之，則將論以經濟間諜法第 1832 條第 3 款之罪。因此，從事技術移轉時，確認洽談者之身分及技術的合法性，業者應具備「主動」與「多疑」之觀察能力，一旦發現不法情事，則應採取民、刑事法律途徑以保障自身權益。

三、確認合作主體

對授權人而言，授權對象之特定應避免無限制之擴

¹⁸ 林行、樊治齊、張勤敏，「從永豐及四維公司等相關人員涉嫌竊取營業秘密案談從事引進技術工作人員的自保之道」，1997 全國智慧財產權研討會論文集，第 300 頁，民國 86 年。

¹⁹ United States of America V. Patrick and Worthing, Criminal No.97-9(W. D. December 7,1996), cited from "Reported Criminal Arrest under the Economic Espionage Act of 1996", R. Mark Halligan, Esq, <http://www.execpc.com/~mhallign/indict.html>. 另參見馮震宇，「從永豐紙業案論如何因應美國經濟間諜法案」，智慧財產權管理季刊，第 15 期，第 10 頁，民國 86 年 10 月。

大，而及於非預期之被授權人；因此授權契約中，被授權人之關係企業是否為授權主體與可否再授權等事項應詳實列明。過去我國企業並不太注意該問題所涉及之法律風險，與其關係企業或子公司幾乎是資源共享，美國經濟間諜法之通過對此將有相當之規範性，業者必須扭轉原有心態，應盡可能於授權契約中載明母公司與子公司或關係公司間之法律關係，以避免關係企業或子公司被控不法或未經授權竊取營業秘密之情事發生。

四、簽署保密協定

技術貿易之合作夥伴往往也同時為市場競爭對手，因此，如何在從事技術授權時確保自己之機密資訊，與避免侵害他人之營業秘密，授權契約雙方應簽署保密協定，明訂雙方保密之義務、事項與範圍，並詳實記錄可對外公開或交換的資訊²⁰。此協定應妥善保存，以供日後如發生爭執時，對於有關營業秘密事項予以認定的有利依據。通常保密條款之內容有²¹：

- (一) 授權人及被授權人雙方應訂定對於授權或簽約過程所知悉之他人營業秘密，均有保守秘密之義務。
- (二) 授權人及被授權人內部應建立妥善之保密制度，包括和其使用人及受雇人簽訂保密契約，以維持授權標的之機密性。

²⁰ 黃嘉珍，前揭文，第 36 頁。

²¹ 劉承愚，賴文智合著，「技術授權契約入門」，智勝文化事業有限公司，第 95-96 頁，民國 88 年 7 月初版。

- (三) 授權人或被授權人違反上述義務，致他造受有損害，應負債務不履行之責任。

五、專家協助

技術移轉工作，尤其是跨國性的，所涉及者不僅為技術層面外，尚有國、內外法令、稅務、習慣等法律層面。故業者應建立專業領域事務委由專家負責之觀念，就降低法律風險之工作，以預防法學之態度，借重法務人員判斷法律行為合法與否之專業知識與能力，與外國廠商爭取技術授權時，從事前規劃授權契約、談判到正式簽約都應諮詢熟悉對方國內法律之律師，並與之陪同洽談，藉由其豐富之實務經驗與管道，幫雇主過濾可疑資訊。尤其經濟間諜法適用範圍很廣，若干條文解釋彈性很大，一有疏忽，很容易被認定為有罪，故更應該借重律師之專業。此外，任何與美商洽談之公司代表也應對於經濟間諜法有所認識，以降低被誣陷或涉入不法交易之法律風險。

六、技術引進書面化

任何法律上爭執，一旦訴諸司法程序，舉證便成為相當重要之課題。由於經濟間諜法僅處罰故意不法行為，因此在訴訟過程中如能舉證並無不法意圖者，將可判無罪。從而，於技術引進之研商過程中應留有書面紀錄，以降低涉案之法律風險。

七、損害賠償

企業一旦發現其營業秘密遭受他人侵害，除應先於

公司之內部及外部進行蒐證之外，亦應對於侵害營業秘密之個人或公司之人力及財力狀況加以分析，以判斷對方是否可能獨立研發；是否應以訴訟方式或以其他方法進行求償；求償過程中對公司營運狀況及員工士氣是否造成負面影響等事項進行評估。此等程序進行過後，如確定其營業秘密係遭他人侵害，則公司所可採取之方法有以下數種：

- (一)請求侵害公司給付一定額度之權利金；
- (二)請求法院為假處分禁止侵害人使用，販賣與原告營業秘密有關之產品，並請求被告返還原告之營業秘密；
- (三)依不當得利或侵權行為之規定要求被告賠償原告一定之損失。

此外，於美國法院之判例中，法院如認為原告公司之動機並非出於惡意，而此一通知之寄發亦確能保護原告公司之營業秘密不因此而外洩者，尚承認受害公司可將侵害之事實通知與侵害公司從事交易之第三人，防止侵害公司與第三人進行或繼續維持之交易關係²²。此種效果，我國民事訴訟法中之保全程序亦可達成，業者於日後如遇他人侵害營業秘密時，不妨善加利用之，以於訴訟之判決確定前，事先維護自身權益。

此外，於移轉技術之洽談過程中，雙方協商之時間、場所亦應注意。換言之，應儘量選擇在工作日之工作場所進行之，避免瓜田李下之嫌。

²² 資策會 MIC 智慧財產權研究小組，「智慧財產權管理手冊」，第 12 頁，民國 81 年。

第三節 政府之協助

一、建置智慧財產權諮詢服務

政府相關部門應就技術移轉相關資訊包括國內外專利、商標著作權等資訊建立一完整資料庫，供業者隨時取用資料並定時更新。在去年(88年)1月26日將中央標準局改制為智慧財產局，原標準、度量業務移撥標準檢驗局，另納入原內政部掌理的著作權法相關業務、商業司掌理的營業秘密法與國貿局的查禁仿冒小組等業務，成為掌理全國專利、商標、著作權、積體電路佈局、營業秘密及查禁仿冒有關智財權業務的專責機構。我國智慧財產局此種「六合一」的單位在全球可謂先進與創舉²³，而其改制也將使得智財權業務在行政組織上「事權統一」，藉此促進我國智財權發展體系之國際化。

此外，政府應建立科技法律諮詢中心與危機處理中心，解答業者的相關疑問，必要時並協助業者處理智慧財產權之爭議與糾紛。根據報導，目前經濟部已聘請財團法人資策會科技法律中心提供高科技業者關於法律層面的協助。資策會科法中心目前正陸續蒐集研發單位及業者技術移轉之法律問題，未來計畫就我國業者與主要合作國家引進技術時所面臨的法律問題建立資料庫，並提供技術移轉線上諮詢服務，且編纂「技術移轉相關法規及注意事項」手冊，讓業者對於技術移轉法制面有充分的認識，並配合產業升級政策，推廣技術移轉相關法制，協助業者合法、順利引進技術²⁴，以避免業

²³ 「營業秘密法將朝重罰重賠方向修正」，經濟日報民國88年8月9日，第4版。

²⁴ 「技術移轉須先自保」，經濟日報民國87年5月7日，第27版。

者因不諳國外法令而誤觸法網。

二、定期舉辦法規研討會

政府應有規劃地舉辦說明會或研討會，就有關營業秘密之相關法規動態與涉及技術移轉等應注意之資訊向業者說明，使業者了解其內容與重要性，並建立或修正其從事技術貿易的策略或方式，以避免因不諳國外法令而觸法，並可逐步提昇我國智財權保護之國際形象。以永豐、四維公司竊密疑案為例，經濟部技術處為使國內業者瞭解經濟間諜法內容與其對於技術貿易之影響，便於 1997 年 10 月 8、9 日邀集美國律師與國內學者舉行「美國經濟間諜法說明會」，探討有關技術移轉、科技研發管理、國際合作與技術移轉契約實務與被訴案件之始末等議題²⁵，不但讓業者瞭解該法之內容，更能提高其因應此等智財權糾紛的能力。未來政府相關單位也應持續結合學術與業界舉行智慧財產權說明會或開辦科技法律課程，對於產業發展過程中可能發生之侵權問題，進行專案研究，以解決廠商困擾與加強訴訟因應之能力。

三、培養高科技素養的法律人才

智慧財產權管理人才的培育，須有賴於健全的法學教育或完備的公司訓練制度，即如何掌握智慧財產權，最大的關鍵在於科技與法律的整合，捨此別無他途²⁶。

²⁵ 「經濟部下月舉辦美國經濟間諜法說明會」，工商時報民國 86 年 9 月 18 日，第 3 版。

²⁶ 黃俊英、劉江彬著，「智慧財產的法律與管理」，華泰文化事業出版，第 288 頁，民國 87 年 5 月 2 版。

然國內目前的法學教育，仍多侷限於法律的範疇，此固無可厚非。惟面對日趨複雜的商業活動及科技發展，政府亦應在加強法學基礎教育之際，利用國家考試的機會導引法律與技術交流，加強習法者跨領域的思維模式，以提供高科技業者所需要的法律人才，方可因應日益專業，日益複雜的高科技法律與紛爭，實為日後提升國家競爭力所不可忽視的課題。

四、結合政府及民間部門共同推動智慧財產權之 管理及保護

智慧財產權的問題隨著國際化、自由化的發展，逐漸地多樣而複雜，為求適切地諮詢、管理與保護智慧財產，使產業界儘早知悉最新技術發展之狀況，除依靠政府相關部門的機能外，仍需民間的產業工會、協會與企業之間相互配合，方更足有效地防止國際交流所可能產生的風險²⁷。

五、協助訴訟

對於智慧財產權已經成為國際產業間的新戰場，今後侵權訴訟，例如專利侵權、竊取營業秘密罪等將會與日俱增，且更趨複雜，政府機關除了應輔導廠商合法引進國外技術外，若不幸涉訟時，更應協助業者應訴，而不是任由外商對國內廠商指控侵權行為。而在協助延攬外國律師處理糾紛案件時，應同時邀請國內律師參與，

²⁷ 林能中，「商業間諜對國際高科技交流影響」，1998 技術貿易研討會升級之契機論文集，第 57 頁，民國 87 年 3 月。

將處理國際智財權訴訟之能力帶入國內²⁸，提升國內應訴之能力。

此外，政府對於所補助研發經費之專案，為免於被懷疑涉入（或鼓勵）經濟間諜，政府相關應先行擬定說明書，闡述政府對智慧財產之重視與尊重，並告誡承接經費補助單位不得非法取得他人之智慧財產。

六、修改法令

我國對於侵害營業秘密之行為，並無直接單獨明文之刑責規定，有無必要追隨美國作法增訂刑責？如自我國此刻正積極尋求加入世界貿易組織(WTO)目標觀之，針對竊取營業秘密之犯行增訂刑責將使我國營業秘密自低度立法(民事責任)提升至高度立法(民刑事責任均有之)，符合 TRIPs 之要求實有正面意義。此外，窺知美國經濟間諜法之立法方式，係將民事法營業秘密概念移植過來，而恪遵罪刑法定主義之大陸法系國家(我國)，對於侵害營業秘密之惡行，仍應配合罪刑法定主義，並針對無形財產之特徵增訂對應條文，以徹底解決營業秘密與傳統刑法財產犯罪在適用上之爭議。

²⁸ 「應培養法律科技整合人才」，經濟日報民國 87 年 2 月 11 日，第 11 版。

第四節 結論

資訊革命使得產品與技術更替的速度急速增加，企業在面對全球競爭之白熱化之情況下，如欲於國際市場中取得優勢，除了應配合科技潮流汲取新知，投入大量心血在研發、經營與管理等方面從事最有效率的整合之外，無形的智慧財產儼然已經成為競爭決勝的關鍵。自1980年代以來，產業經濟依賴科技程度日益加重，科技研發成本日益增高，科技市場價值亦隨之增大，帶動了對智財權強勢之需求，希冀藉由智財權法的庇護，得以無後顧之憂，積極的進行研發工作。傳統保護智慧財產權的手段，殆多仰賴於著作權法、商標法或專利法，惟隨著科技的快速發展及日趨複雜，前述的法律已不足以應付新的需求，生物技術、營業秘密等新客體逐漸納入智慧財產權之體系中，例如世界貿易組織「與貿易有關的智慧財產權」協定、美國的經濟間諜法便應運而生，也同時藉此維護商業道德及其國家科技領先地位。

美國政府有感於冷戰結束後，遭受商業間諜侵害智慧財產之案件逐漸增加，嚴重影響美國企業國際競爭力與國家經濟安全，而且此類攸關企業發展與競爭成敗的資訊多屬於營業秘密之範疇，為尋求聯邦法能全面保護此等科技資訊，遂立法通過「經濟間諜法」。就經濟間諜法基本架構而言，係根源於侵權行為法彙編及統一營業秘密法，因此就營業秘密之定義與要件均與該二者意旨相同，僅有之差異係在於經濟間諜法將目前存在或將來可能發生之儲存營業秘密的方式，均納入保護範圍，擴大了營業秘密之範圍，藉以因應高科技存在之型態。再者，經濟間諜法不但規範了經濟間諜罪與竊取營業秘密罪兩種犯罪類型，且明文規範有形與無形侵害營業秘密行為之態樣，使得法院原依據侵權行為法彙編和

統一營業秘密法所遭遇認定不一的問題能得以解決。該法最大的特色即在於「聯邦化」、「刑法化」，此不但令美國就營業秘密法之保護產生結構上的變化，更使得國家公權力介入原本民事糾紛，對此，是否真正符合當事人的利益仍有爭議，但可知的是，已經造成商業活動、營業秘密所有人、受雇人或顧問等一定的影響。凡此，均係於第二章加以討論。

我國已逐漸步入技術出口國家之林，日後國人或業界亦可能面臨商業間諜之困擾，我國現行法在面對此等侵害行為上，因其與傳統刑法之竊盜罪、詐欺等構成要件不符，而無法適用之，但此等侵害行為惡性重大，造成商業損害亦甚大，因此建議參酌外國立法例，就營業秘密法增列刑事責任以臻完備，並針對無形財產之特徵增訂對應條文，以徹底解決營業秘密與傳統刑法財產犯罪在適用上之爭議。

美國制定「經濟間諜法」之際，對於違反該法之被告科以極高之刑責，其是否再次藉由該法做為對付競爭國家之手段，姑且不問。惟「經濟間諜法」公布實行之後，隨即發生永豐案與四維案，美方是否「柿子挑軟的吃」而藉此等作為以收殺雞儆猴之效，姑且不論。但徵諸永豐案與四維案事實觀之，不免發現國內業者在從事技術移轉工作之際，可能產生之疏忽與對他國智慧財產權法律知識的欠缺，故我國業者除了應深入認識該部法律，瞭解其執行面外，且更應慎防競爭對手以非營業秘密，製造「意圖犯罪」之事實，作為打擊對手之手段，發生觸法之情事。

經濟間諜法所帶來的另一省思，便在於喚起國內業者重視智慧財產權，並就相關技術移轉時所可能涉及的

法律風險應一併規畫、防範之。職是，本文第五章援引外國企業經驗與學者見解，分別就企業與政府兩方面，提供經濟間諜法之因應對策，期能對於降低或避免經濟間諜法訴訟風險有所助益。就企業而言，由於經濟間諜法所規範之經濟間諜罪或竊取營業秘密罪，均以被告明知所竊取之資訊屬營業秘密為前提。對此，於訴訟上雖不致完全無法證明，但卻是對被告最有利的抗辯事項。因此欲排除經濟間諜法中所規定之「明知」要件，業者內部須規畫並執行「營業秘密管理系統」，且在從事國際技術合作計畫或延攬歸國人才時，應採取主動、積極的態度，對於契約過程牽涉的各個層面，例如授權人或授權技術之合法性、員工對前雇主之義務等事項，一一檢驗。企業如能有尊重他人智慧財產權的基本認知，以合法的心態，正當的手段取得他人合法的技術，即無觸法的困擾，亦無須擔心因他人構陷而致刑罰上身，將外力當做是一種督促，用正面、建設性的心態，去面對、提供自己對智財權的尊重，則經濟間諜法風波在短期內或許是一場風暴，但長期看來，卻可能利多於弊，誠屬業者自保之最佳之道。至於在政府方面，應透過建置智慧財產權諮詢服務、定期舉辦法規研討會等方式輔導業者瞭解經濟間諜法，提昇業者訴訟因應之能力，並與企業共同結合推動智財權之管理與保護。

一連串智財權訴訟之出現，顯現法律已經成為高科技產業主要的競爭手段。祈藉由本文之研究，能更深入瞭解美國經濟間諜法，我國企業與政府在面對智財權商業風暴，應廣泛瞭解外國法令，記取國內、外案例前車之鑑教訓，審慎規畫智慧財產權之管理，嚴格執行，防範侵害他人之智財權及可能指控之發生，同時也應該積極推動提昇自行研發能力，不再依賴外國技術移轉或開發協助，治標治本，自能有效消弭侵權指控，並符合世

界經濟發展之趨勢。

參考資料

壹、中文書目及期刊論文(依作者姓氏筆劃)

一、書目

1. 林山田，刑法特論（上），自版，民國 78 年 9 月。
2. 林嘉彬，營業秘密之概念及其侵害行為類型之研究，輔仁大學法律研究所碩士論文，民國 83 年 7 月。
3. 林慧蓉，論網際網路資訊安全與隱私權之保護-以營業秘密保護為中心，東海大學法律學研究所碩士論文，民國 87 年 12 月。
4. 徐玉玲著，徐火明主編，營業秘密的保護-公平法與智產法系列二，三民書局出版，民國 82 年 11 月初版。
5. 徐遵慈，論營業秘密保護之立法及其與不正競爭之關係，東吳大學法律學研究所碩士論文，民國 84 年 7 月 18 日。
6. 張沛元譯，大盜入侵-你不能不之道的企業間諜商戰實錄，商業週刊，民國 87 年初版。
7. 曹永遊，論專門技術在我國營業秘密法之保護，中興大學法律研究所碩士論文，民國 86 年 7 月。
8. 黃榮堅，刑法問題與利益思考，月旦出版公司，1995 年初版。
9. 馮震宇，了解營業秘密法-營業秘密法的理論與實務，永然文化府份有限供公司，民國 87 年 7 月初版。

10. 黃俊英、劉江彬著，「智慧財產的法律與管理」，華泰文化事業出版，民國 87 年 5 月 2 版。
11. 劉承愚，賴文智合著，「技術授權契約入門」，智勝文化事業有限公司，民國 88 年 7 月初版。
12. 鄭穎，營業秘密侵害在刑事法上之研究，中興大學法律學研究所碩士論文，民國 87 年 8 月。
13. 資策會 MIC 智慧財產權研究小組，智慧財產權管理手冊，民國 81 年。

二、期刊

1. 辛志中，日本不正競爭防止法簡介，公平交易季刊，第 5 卷第 1 期，民國 86 年 1 月。
2. 吳念祖，樊治齊，新產品開發之專利權管理策略與作法，1999 全國智慧財產權研討會，國立交通大學法律中心主編，民國 88 年 11 月。
3. 林行、樊治齊、張勤敏，從永豐及四維公司等相關人員涉嫌竊取營業秘密案談從事引進技術工作人員的自保之道，1997 全國智慧財產權研討會論文集，國立交通大學法律中心主編，民國 86 年。
4. 林能中，商業間諜對國際高科技交流影響，1998 技術貿易研討會升級之契機論文集，民國 87 年 3 月。
5. 吳景源，談營業秘密法關於營業秘密之保護，萬國法律第 107 期，民國 88 年 10 月。

6. 郭懿美，論台灣高科技工業如何因應美國經濟間諜法-技術移轉 V.S.竊取營業秘密，1997 全國智慧財產權研討會論文集，國立交通大學法律中心主編，民國 86 年。
7. 郭懿美，兩岸智財權保護環境之發展淺析，1999 全國智慧財產權研討會論文集，國立交通大學法律中心主編，民國 88 年 11 月 25 日。
8. 邵瓊慧，營業秘密之保護-兼談企業如何擬定相關條款，月旦法學雜誌，第 46 期，1999 年 3 月。
9. 張心悌，智慧財產權保護之法律經濟分析，律師雜誌，第 211 期，民國 88 年 4 月。
10. 張靜，我國營業秘密法介紹，<http://www.moeaipo.gov.tw/nbs12/ipo3a.htm>
11. 張凱娜，由近年國內發生之案例談企業保護營業秘密，1997 全國智慧財產權研討會論文集，國立交通大學法律中心主編，民國 86 年。
12. 陳家駿，公平交易法對營業秘密保護之評析，公平交易季刊，第 2 卷第 1 期，民國 83 年 1 月。
13. 馮震宇，資訊時代之新挑戰-論營業秘密之保護，月旦法學雜誌，第 8 期，民國 84 年 12 月。
14. 馮震宇，論美國經濟間諜法與營業秘密之保護趨勢，1997 全國智慧財產權研討會論文集，民國 86 年。
15. 馮震宇，從美國經濟間諜法案論外國立法例對營業秘密之保護，工業財產權與標準，第 54 期，民國 86 年 9 月。

16. 馮震宇，論營業秘密之保護、查核與管理，工業財產權與標準，第 57 期，民國 86 年 12 月。
17. 馮震宇譯，竊取營業秘密的刑事責任-美國 1996 經濟間諜法，1998 技術貿易研討會產業升級之契機論文集，民國 87 年。
18. 馮震宇，從永豐判決論美國經濟間諜法之適用，萬國法律，第 107 期，民國 88 年 10 月。
19. 馮博生，技術移轉之型態與契約解析，1999 全國智慧財產權研討會論文集，，國立交通大學法律中心主編，民國 88 年 11 月。
20. 馮博生，營業秘密的定義及營業秘密法之保護客體，
<http://www.apipa.org.tw/apipa/b5/paper/tradeseecret/ts3.htm>
21. 湯明輝，營業秘密保護理論之探討，律師通訊第 163 期，民國 82 年 4 月。
22. 湯明輝，談美國營業秘密之構成要件，公平交易季刊，第 2 卷第 1 期，民國 83 年 1 月。
23. 董浩雲，美國經濟間諜法執行上的幾個問題-從永豐案的觀察，資訊法務透析，民國 88 年 5 月。
24. 黃家珍，美國九六年經濟間諜法簡介，通訊雜誌，民國 86 年 11 月。
25. 黃朝義，論經濟犯罪及其對策，法學叢刊第 169 期，民國 87 年 1 月。

26. 黃俊英、凌儀玲撰，「企業內部營業秘密之保護措施-兼論智慧財產權下的員工管理」，1998 全國智慧財產權研討會論文集，民國 87 年 11 月 19 日。
27. 楊靜宜，網路行為管轄權爭議問題之初探，資訊法務透析，民國 88 年 6 月。
28. 勤玉華，美國經濟間諜法案例與順從程序之運用，<http://www.moeaipo.gov.tw/nbs12/ipo3j.htm>
29. 劉博文，美國經濟間諜法簡介，<http://www.moeaipo.gov.tw/nbs/2/ipo3i.htm>
30. 駱志豪，TRIP 對營業秘密之保護，公平交易季刊，第 4 卷第 3 期，民國 85 年 7 月。
31. 謝銘洋，營業秘密侵害之類型觀察與責任分析，資訊法務透析，民國 81 年 8 月。
32. 蘇宏文，從永豐公司商業間諜案看我國營業秘密之保護(上)，網路資訊，第 69 期，民國 86 年 9 月。
33. 蘇宏文，從永豐公司商業間諜案看我國營業秘密之保護(下)，網路資訊，第 70 期，1997 年 11 月。
34. 工研院智慧財產管理及運用綱要，<http://www.itri.org.tw/feature/fe-0880420.html>
35. 智財權管理 ISO 化-雙效合一，智慧財產權管理季刊，第 21 期，民國 88 年 6 月。

36. Autodesk, Inc 竊用 Vermont Microsystems Inc.營業秘密之判決剖析，電通所法務智權園地，民國 86 年 1 月 16 日，<http://www.csl.itri.org.tw/Text/law/86008.htm>

貳、外文期刊論文

1. Ablondi, Foster Sobin & Davidow, p.c., "The Economic Espionage Act of 1996", July 2, 1997.
2. Arthur Wineburg and Timothy J. Klima, "Current Issues in Trade Secret Law: The New U.S. Economic Espionage Act", <http://www.pillsburylaw.com/publications/economic-espionage.html>.
3. Barry R. Shapiro, "Economic Espionage", Marketing management, Spring, 1998.
4. Edwin Fraumann, "Economic Espionage: Security Missions Refined", Public Administration Review, Vol.57, No.4, July / August, 1997.
5. "Economic Espionage Act Criminalizes Trade Secret Theft ", <http://www.sf-law.com/espionage.htm>.
6. "Economic Espionage:The Looting of America's Economic Security in the Information Age", <http://www.cmahg.com/infosphere/news/issues/issues/issues-articles/issues-espionage.htm>
7. "Economic Espionage Explosion", Security, May,

1998.

8. "Federal Prosecution of Violations of Intellectual Property Rights",
<http://www.usdoj.gov/criminal/cybercrime/intell-prop-rts/SectV.htm>
9. "Federal Prosecution of Violations of Intellectual Property Rights",
<http://www.usdoj.gov/criminal/cybercrime/intell-prop-rts/SectV.htm>
10. Linda K. Stevens, "The Economic Espionage Act, New Criminal Penalties for Trade Secret Misappropriation",
<http://www.schiffhardin.com/econact.htm>.
11. Louis J. Freeh, "Hearing on Economic Espionage",
<http://www.fbi.gov/congress/econom/ecespion.htm>,
1996.
12. Gerald J. Mossinghoff, J. Derek Mason, Ph.D. and David A. Oblon, "The Economic Espionage Act: A New Federal Regime of Trade Secret Protection",
<http://www.oblon.com/pub/mason-120.htm>
13. Gillian Flynn, "Raid the Competition for Workers, Not Their Secret", workforce, December 1998.
14. Irvin B. Nathan and Nancy L. Perkins, "Tough Enforcement of New U.S. Economic Espionage Act Reveal Need for Strict Compliance", 國際技術移轉管理面面觀-美國經濟間諜法及我國業者技轉因應之道補充資料, 民國 88 年 7 月。

15. James Pooley , "Criminal Consequences of Trade Secret Theft:The Economic Espionage Act of 1996", 1998 技術貿易研討會產業升級之契機論文集。
16. Joseph N. Hosteny, "The Economic Espionage Act: A Very Mixed Blessing", <http://www.hosteny.com>
17. Marco E. Brown, Electronic Business, "When employees leave" , June 1998.
18. Mark D.Seltzer and Angela A. Burns,"Criminal Consequence of Trade Secret Misappropriation: Does the Economic Espionage Insulate Trade Secrets from Theft and Render Civil Remedies Obsolete", May 25, 1999, <http://www.bc.edu/bc-org/avp/law/st-org/iptf/articles/content/1999052501/html>.
19. R.Mark Halligan,Esq.,"Reported Criminal Arrest under the Economic Espionage Ac of 1996", <http://www.execpc.com/~mhalign/indict.html>
20. Sorojini J. Biswas, "The Economic Espionage Age of 1996", <http://www.carolinapatents.com-articles/trade-secret4.htm>.
21. "The Economic Espionage Act of 1996", <http://www.nhdd.com/hot/wh11.htm>.
22. <http://thomas.gov/cgi-bin/cpguery>
23. <http://www.nacic.gov/cind/cind196.htm>
24. <http://www.security.management.com/library/000/91.html>
25. <http://www.nsi.org/library/comm/commpricrcy.txt>

26. <http://www.usdoj.gov/criminal/cybercrime/intell-prop-rts/app-l-m.htm>

27. <http://www.nhold.com/hot/hh11.htm>

附錄

THE ECONOMIC ESPIONAGE ACT OF 1996:

Title I -

Protection of Trade Secrets

Sec. 101. Protection of Trade Secrets

(a) In General. - Title 18, United States Code, is amended by inserting after

chapter 89 the

following:

Sec.

1831. Economic espionage.

1832. Theft of trade secrets.

1833. Exceptions to prohibitions.

1834. Criminal forfeiture.

1835. Orders to preserve confidentiality.

1836. Civil proceedings to enjoin violations.

1837. Conduct outside the United States.

1838. Construction with other laws.

1839. Definitions.

Chapter 90-

Protection of Trade Secrets

Section 1831 Economic espionage

(a) In General - Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly -

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret,

(3) receives, buys, or possesses a trade secret, knowing the same to have been

stolen or appropriated, obtained, or converted without authorization,

(4) attempts to commit any offense described in any of paragraphs (1) through (3), or

(5) conspires with one or more other persons to commit

any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection

(b), be fined not more than \$500,000 or imprisoned not more than 15 years, or both.

(B) Organizations - Any organization that commits any offense described in subsection (a) shall be fined not more than \$ 10, 000, 000.

Section 1832. Theft of trade secrets.

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and

intending or knowing that the offense will injure any owner of that trade secret, knowingly -

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be

fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall

be fined not more than \$5,000,000.

Section 1833. Exceptions to prohibitions.

This chapter does not prohibit -

(1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; or

(2) the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a

political subdivision of a State, if such entity has lawful authority with respect to that violation.

Section 1834. Criminal forfeiture.

(a) The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentence imposed, that the person forfeit to the United States -

(1) any property constituting or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

(2) any of the person's or organization's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation,

if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.

(b) Property subject to forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse

Prevention and Control Act of 1970 (21 U.S. C. 853), except for subsections

(d) and (e) of such section, which shall not apply to

forfeitures under this section.

Section 1835. Orders to preserve confidentiality

In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to

preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United

States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

Section 1836. Civil proceedings to enjoin violations

(a) The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this section.

(b) The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.

Section 1837 Applicability to conduct outside the United States

This chapter also applies to conduct occurring outside the United States if

(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the

United States or a State or political subdivision thereof, or

(2) an act in furtherance of the offense was committed in the United States.

Section 1838 Construction with other laws

This chapter shall not be construed to preempt or displace any other remedies,

whether civil or criminal, provided by United States Federal, State,

commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employees under section 552 of title 5 (commonly known as the Freedom of Information Act).

Section 1839 Definitions

As used in this chapter

(1) the term 'foreign instrumentality' means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government:

(2) the term 'foreign agent' means any officer, employee, proxy, servant, delegate, or representative of a foreign government:

(3) the term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns,

plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically,

electronically, graphically, photographically, or in writing if

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value,

actual or potential,

from not being general known to, and not being readily ascertainable through

proper means by the public, and

(4) the term 'owner', with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to or license in, the trade secret is reposed."

(b) Clerical Amendment. The table of chapters at the beginning part I of title

18, United States

Code, is amended by inserting after the item relating to chapter 89 the

following:

"90. Protection of trade secrets 1831"

(c) Reports. - Not later than 2 years and 4 years after the date of the

enactment of this Congress of this Act, the Attorney General shall report to

Congress on the amounts received and distributed from
fines for offenses under

this chapter deposited in the Crime Victims Fund
established by section 1402 of

the Victims of Crime Act of 1984 (42 U.S. C. 10601).

Passed by Congress: October 2, 1996

Signed by the President : October 11, 1996