個人隱私面面觀

Bo Cheng
鄭伯炤
bcheng@ccu.edu.tw

INSA
Information Networking Security and Assurance Lab
National Chung Cheng University

Conclusion

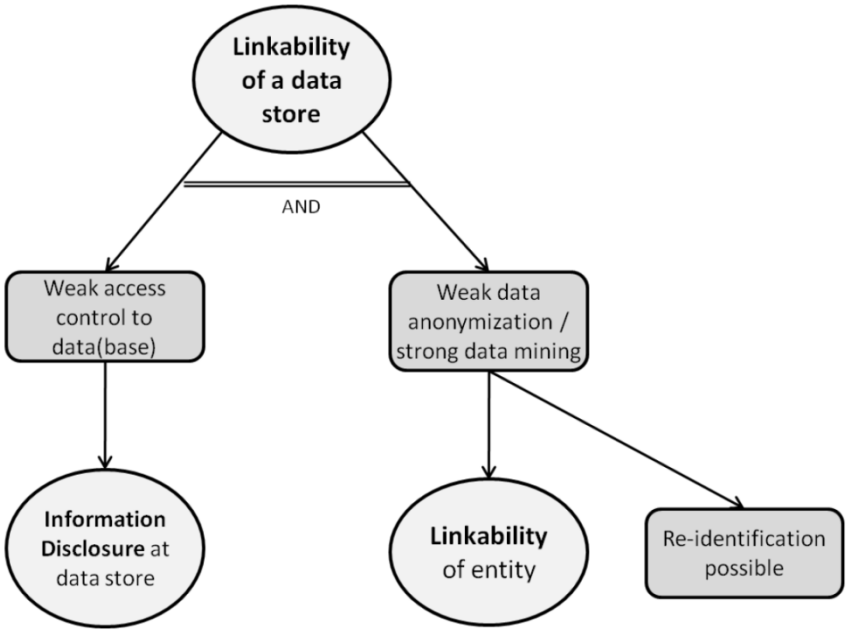
以上內容純屬演講，

如有疑問純屬專家問題！

The Relations between Privacy and Security

• *Linkability of entity refers to an attacker can sufficiently distinguish* whether two or more entities are related or not within the system.

• *Identifiability of entity refers to an attacker can sufficiently identify the* entities within the system.



Security ≠ Privacy

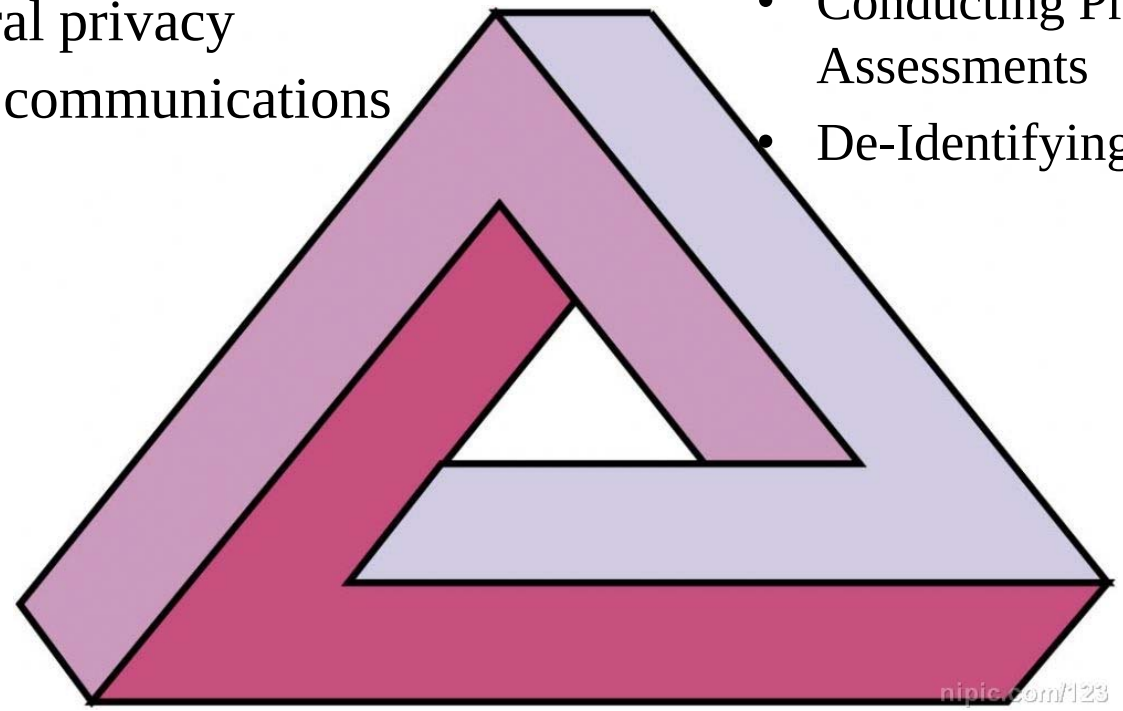
Privacy

Four dimensions of privacy

- Personal information (個資)
- Personal privacy
- Behavioral privacy
- Personal communications privacy

Privacy-Specific Safeguards

- Minimizing the Use, Collection, and Retention of PII
- Conducting Privacy Impact Assessments
- De-Identifying Information



Law Enforcement

個人資料

指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以**直接**或**間接**方式識別該個人之資料。

本法第二條第一款所稱得以間接方式識別該個人之資料，指僅以該資料不能識別，須與其他資料對照、組合、連結等，始能識別該特定個人者。但查詢困難、需耗費過鉅或耗時過久始能特定者，不在此限。

電腦處理個人資料保護法之個人資料類別 (I)

http://mojlaw.moj.gov.tw/LawContentDetails.aspx?id=FL010631

代　　號　**識別類**：

Ｃ○○一　辨識個人者。

例如：姓名、職稱、住址、工作地址、以前地址、住家電話號碼、相片、指紋、電子郵遞地址及其他任何可辨識資料本人者等。

Ｃ○○二　辨識財務者。

例如：銀行帳戶之號碼與姓名、信用卡或簽帳卡之號碼、個人之其他號碼或帳戶等。

Ｃ○○三　政府資料中之辨識者。

例如：身分證統一編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等。

電腦處理個人資料保護法之個人資料類別 (II)

代　　號　**特徵類**：

Ｃ○一一　個人描述。

例如：年齡、性別、出生年月日、出生地、國籍等。

Ｃ○一二　身體描述。

例如：身高、體重、血型等。

識別類	受僱情形
特徵類	財務細節
家庭情形	商業資訊
社會情況	健康與其他
教育、技術或其他專業	其他各類資訊

間接方式識別個人之資料

Name	Age	Zipcode	Disease
Bob	21	12000	dyspepsia
Alice	22	14000	bronchitis
Andy	24	18000	flu
David	23	25000	gastritis
Gary	41	20000	flu
Helen	36	27000	gastritis
Jane	37	33000	dyspepsia
Ken	40	35000	flu
Linda	43	26000	gastritis
Paul	52	33000	dyspepsia
Steve	56	34000	gastritis

爲保護個人資料，有些資料雖未直接指名道姓，但一經揭露仍足以識別爲某一特定人，乃規定間接方式識別個人之資料之意義。

K-Anonymity

An adversary

Name	Age	Zipcode
Bob	21	12000

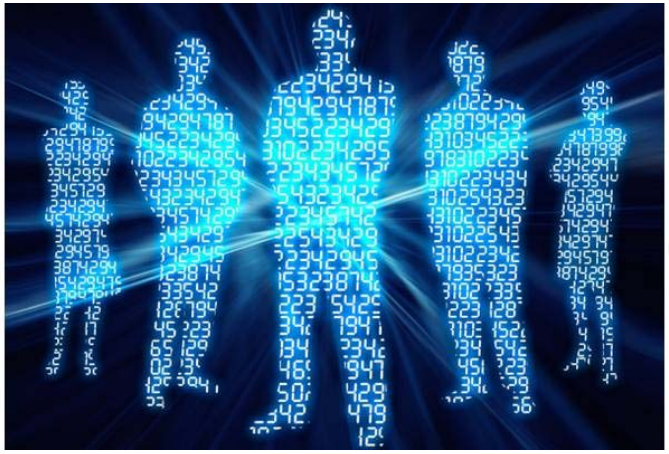
Published table

Age	Zipcode	Disease
21	12000	dyspepsia
22	14000	bronchitis
24	18000	flu
23	25000	gastritis
41	20000	flu
36	27000	gastritis
37	33000	dyspepsia
40	35000	flu
43	26000	gastritis
52	33000	dyspepsia
56	34000	gastritis

Quasi-identifier (QI) attributes

特種資料

- 有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。
- 前項第四款個人資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法，由中央目的事業主管機關會同法務部定之。



一、法律明文規定。
二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。
三、當事人自行公開或其他已合法公開之個人資料。
四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，爲統計或學術研究而有必要，且經一定程序所爲蒐集、處理或利用之個人資料。

個資法第22條

- 中央目的事業主管機關或直轄市、縣（市）政府認有必要或有違反本法規定之虞
  - 得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。
  - 檢查時，可為證據之個人資料或其檔案，得扣留或複製之。
  - 無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。

Q1：個人資料保護法的主管機關有哪些？

- 法務部
  - 負責個資法施行細則之擬定及法律解釋等事宜
- 各行業之中央目的事業主管機關或地方政府負責
  - 個資法令之執行及以行業別區分之法規命令
    - 例如，中小企業如屬環保業者，主管機關爲行政院環保署；如屬網路零售業，主管機關爲經濟部商業司。

http://law.moeasmea.gov.tw/modules.php?name=km&catid=39

Other 3 Privacy Dimensions

- Privacy of the person. This is the right to control the integrity of one's own body. It covers such things as physical requirements, health problems, and required medical devices.
- Privacy of personal behavior. This is the right of individuals to keep any knowledge of their activities, and their choices, from being shared with others.
- Privacy of personal communications. This is the right to communicate without undue surveillance, monitoring, or censorship.

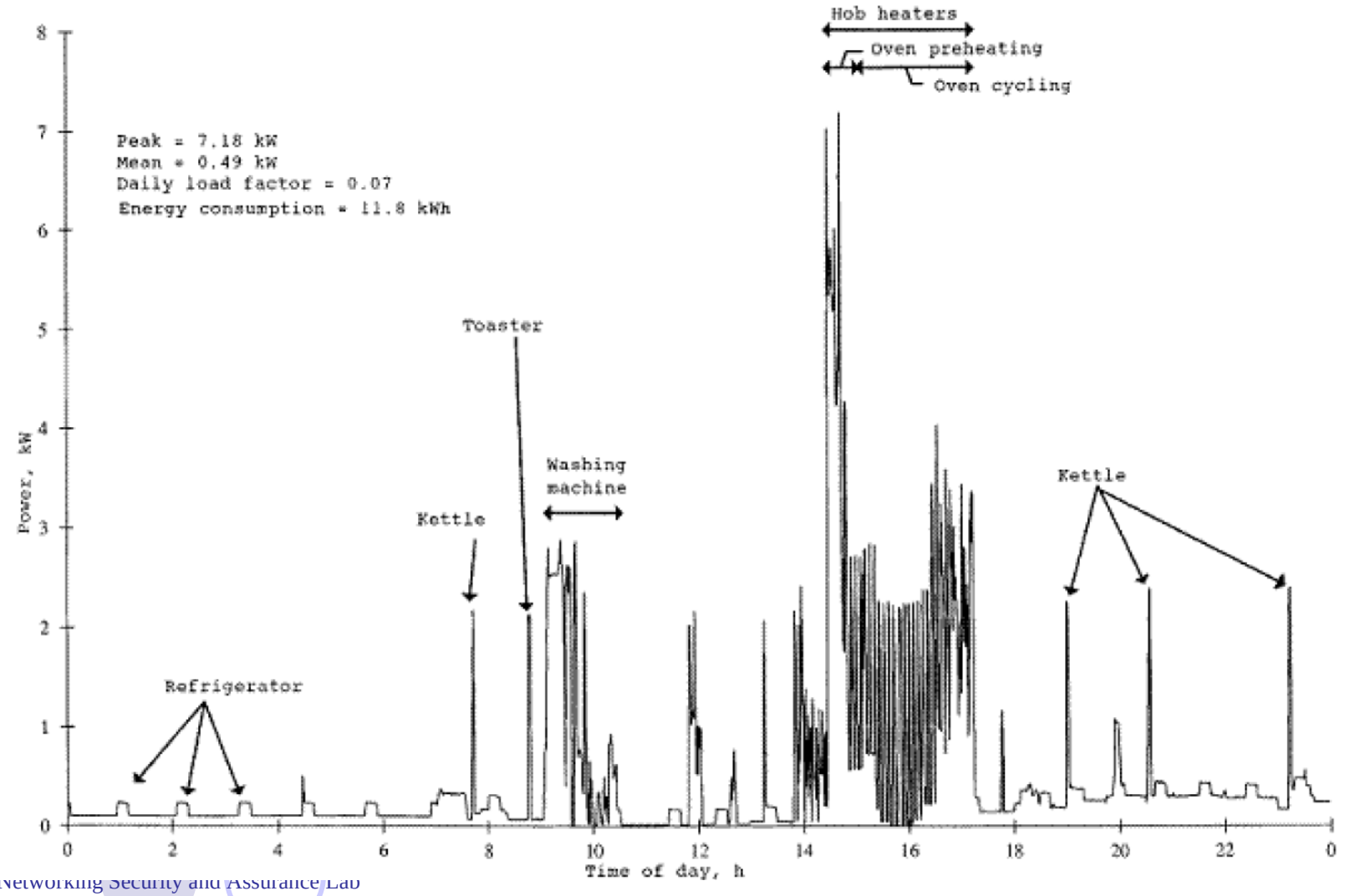
太離譜 萬芳醫院爆洩病歷、隱私

【聯合晚報／記者林進修、李樹人/台北報導】 2011.08.04 02:57 pm

一位病患日前到台北市立萬芳醫院就醫，到某科服務台詢問相關就醫資訊時，志工給他的便條紙，背面竟然有另一名病患的就醫資料，姓名、年齡、體重、就醫科別等資訊都清清楚楚，病患隱私全曝光。

違反醫療法72條「醫療機構及其人員因業務而知悉或持有病人病情或健康資訊，不得無故洩漏」，醫院已明顯疏失；衛生署將行文給台北市衛生局開罰，依規定該院必須面對5萬元以上、25萬元以下的罰鍰。未來在醫院評鑑時，評鑑委員們也將特別要求院方提出說明以及改進方式。

Power Usage to Personal Activity Mapping



AMI Privacy Risk

Power Company

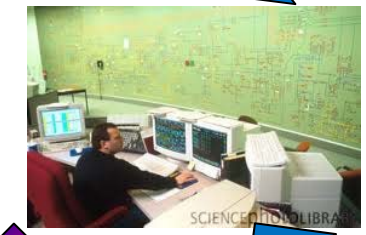
- Collected information which is related to a particular household or business

every 15 to 60 minutes

- meter identifier,
- timestamp,
- usage data

- Marketing: e.g., pricing, profitable customers
- Billing
- Outage management,
- Load forecasting,
- Workforce management

- When they were present,
- What they were doing



Appliance manufacturer

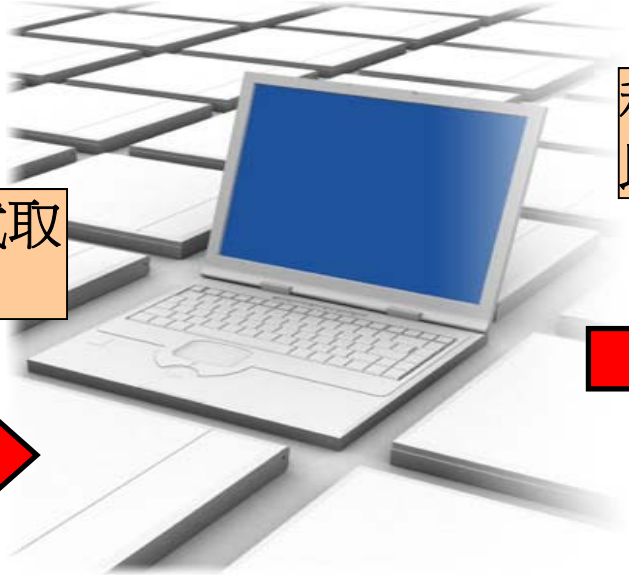
- Outage,
- Voltage,
- Phase,
- Frequency data
- Status and diagnostic information

Retailers of appliances

Insurers

個資蒐集、處理、利用

第 1 條 為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人 資料之合理利用，特制定本法。



蒐集：指以任何方式取得個人資料。

處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

利用：指將蒐集之個人資料為處理以外之使用。

對個人資料之蒐集或處理時 .....

公務機關

一、執行法定職務必要範圍內。

二、經當事人書面同意。

三、對當事人權益無侵害。

非公務機關

一、法律明文規定。
二、與當事人有契約或類似契約之關係。
三、當事人自行公開或其他已合法公開之個人資料。
四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過 提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。
五、經當事人書面同意。
六、與公共利益有關。
七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

親愛的朋友，您好：

請您填妥下列的問卷調查表，交於敦陽攤位工作人員，詳細填妥問卷之前 200 名可獲贈一份我們特別爲您準備的小禮物，謝謝！

Info Security 2012 台北國際資訊安全科技展 研討會問卷表

議題：「黑海時代揭幕—偉大閘道防護的起點」 場次：IS-702，4/20 11:00–11:40

1. 請問您的工作性質？（單選）
   ☐ 企業經營階層 ☐企業資安人員 ☐ 企業資訊人員 ☐ 企業一般員工
   ☐ 資安廠商技術顧問/工程師
2. 請問貴公司已經採用的安全管理機制或方案為何？
   ☐ 應用程式防火牆 ☐防火牆 ☐ 入侵偵測系統 ☐ SSL-VPN
   ☐ 防毒系統 ☐DLP ☐日誌管理系統☐資料庫安全稽核系統
   ☐ 內容安全(網頁瀏覽、即時通訊管理) ☐無線網路
   ☐ 網管監控 ☐ 郵件安全系統☐ 其他_____
3. 請問貴公司或個人對於安全管理機制或方案有興趣？
   ☐ 應用程式防火牆 ☐防火牆 ☐ 入侵偵測系統 ☐ SSL-VPN
   ☐ 防毒系統 ☐DLP ☐日誌管理系統☐資料庫安全稽核系統
   ☐ 內容安全(網頁瀏覽、即時通訊管理) ☐無線網路
   ☐ 網管監控 ☐ 郵件安全系統☐ 其他_____
4. 請問貴公司是否曾導入資安專業服務？如果「是」請選擇：
   ☐ 企業安全防護規劃建置 ☐ 弱點評估 ☐ 滲透測試 ☐ 內部安全評估
   ☐ 安全監控中心規劃建置 ☐ 記錄分析服務 ☐ 緊急應變處理
   ☐ 安全資訊通報服務 ☐ 其他 _____
5. 請問貴公司或個人對於哪一類的資安專業服務有興趣？
   ☐ 企業安全防護規劃建置 ☐ 弱點評估 ☐ 滲透測試 ☐ 內部安全評估
   ☐ 安全監控中心規劃建置 ☐ 記錄分析服務 ☐ 緊急應變處理
   ☐ 安全資訊通報服務 ☐ 其他 _____
6. 請問今天的研討會內容是否對您有幫助？（單選）
   ☐ 很有幫助 ☐ 有幫助 ☐ 沒有幫助 ☐ 其他_____
7. 請問貴公司是否目前或曾經是敦陽客戶？（單選）
   ☐ 是的，與資安產品/服務有關 ☐ 是的，但與資安無關 ☐ 不是
8. 請問您未來是否願意考慮找敦陽科技為貴公司規劃與建置資安方案？（單選）
   ☐ 是的，會考慮資安產品建置 ☐ 是的，會考慮資安專業服務
   ☐ 是的，資安產品或專業服務都會 ☐ 暫不考慮

基本資料：(煩請詳細填寫 or 附上名片)

姓名：_____ 公司：_____

部門職稱：_____/_____E-MAIL：_____

電話：_____

蒐集個人資料時

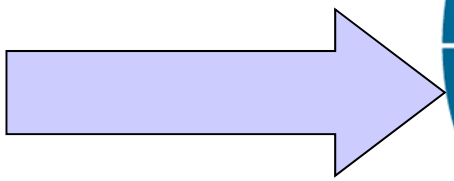
- 應明確告知當事人下列事項：
  - 一、公務機關或非公務機關名稱。
  - 二、蒐集之目的。
  - 三、個人資料之類別。
  - 四、個人資料利用之期間、地區、對象及方式。
  - 五、當事人依第三條規定得行使之權利及方式。
  - 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。
- 有下列情形之一者，得免爲前項之告知：
  - 請參閱下頁

電腦處理個人資料保護法之特定目的

代號	特定目的項目
○○一	人身保險業務
○○二	人事行政管理
…	
○二一	行銷 (不包括直銷至個人)
○二二	行銷 (包括直銷至個人)
…	
○四五	個人資料之交易
…	
○七九	學生資料管理
…	
一○一	其他諮詢與顧問服務

行使之下列權利

一、查詢或請求閱覽。
二、請求製給複製本。
三、請求補充或更正。
四、請求停止蒐集、處理或利用。
五、請求刪除



蒐集個人資料時免告知

- 一、依法律規定得免告知。
- 二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
- 三、告知將妨害公務機關執行法定職務。
- 四、告知將妨害第三人之重大利益。
- 五、當事人明知應告知之內容。

Example: 中華電信 (I)

http://www.cht.com.tw/aboutus/personal_data.html

1. 申請機構名稱：中華電信股份有限公司
2. 總公司所在地：台北市信義路一段 21 之 3 號
4. 代表人姓名：呂學錦
6. 個人資料檔案名稱：客戶基本資料檔、客戶應收帳款檔
7. 保有之特定目的：

022/行銷（包括直銷至個人）、037/客戶管理、060/統計調查與分析、065/資訊與資料庫管理、074/經營電信業務與電信加值網路業務、080/徵信、097/其他合於營業登記項目或章程所定業務之需要、101/其他諮詢與顧問服務。

Example: 中華電信 (II)

8. 個人資料之類別：

C001/辨識個人資料、C002/辨識財務者、C003/政府資料中之辨識者、C011/個人描述、C093/財務交易

9. 個人資料之範圍：各項業務客戶及計畫往來或洽談中之客戶個人資料

10. 個人資料檔案之保有期限：永久保留

11. 個人資料之搜集方法：當事人提供

Example: 中華電信 (III)

12. 個人資料檔案之利用範圍：

    (1)於蒐集之特定目的必要範圍內爲之

    (2)合於「電腦處理個人資料保護法」第二十三條但書規定，爲特定目的外之利用

13. 國際傳遞個人資料之直接收受者：無

Q2. 企業需要保護哪些個資？

- 個資定義:包括了個人的姓名、出生年月日、身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動，以及其他可以直接或間接識別出個人的資料都屬於個資法的保護範圍。
- 第5條規定:個資檔案包括備份檔案及軌跡資料
  - 軌跡資料:個人資料在蒐集、處理、利用過程中，所產生非屬於原蒐集個資本體的衍生資訊（Log檔案）
  - Log 包括（但不限於）當事人的帳號、存取時間、設備代號、網路IP位址等等。

違反本法規定

公務機關

致個人資料遭不法蒐集、處理、利用或其他侵害 當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所 致者，不在此限。

非公務機關

致個人資料遭不法蒐集、處理、利用或其他侵 害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此 限。

必須自行舉證沒有違反個資法

- 規範對象:公務機關、自然人、企業法人、其他團體（三人以上即可視爲團體）。代理蒐集機關則視同委託者。
- 企業必須舉證說明自己沒有過失或故意違反法律
- 經濟部商業司已經規畫隱私權標章
  - 作爲企業非故意或過失違反的舉證之一

損害賠償與罰則

- 損害賠償

  - 當事人可向違反個資法的企業求償，每人每次5百元～2萬元，相同原因合計最高求償金額2億元。
- 罰則
  - 違法蒐集、處理或利用個資而產生損害時，處2年以下有期徒刑、拘役或併科20萬元以下罰金。
  - 違法蒐集、處理或利用個資，意圖營利者處5年以下有期徒刑、拘役或併科100萬元以下罰金。

- 行政罰鍰
  - 主管機關並得爲下列處分：
    - 禁止蒐集、處理或利用個人資料。
    - 命令刪除經處理之個人資料檔案。
    - 沒入或命銷燬違法蒐集之個人資料

11項適當安全維護措施

指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之必要措施

- 成立管理組織，配置相當資源
- 界定個人資料之範圍
- 個人資料之風險評估及管理機制
- 事故之預防、通報及應變機制
- 個人資料蒐集、處理及利用之內部管理程序
- 資料安全管理及人員管理
- 認知宣導及教育訓
- 設備安全管理
- 資料安全稽核機制
- 必要之使用紀錄、軌跡資料及證據之保存
- 個人資料安全維護之整體持續改善

以所須支出之費用與所欲達成之個人資料保護目的符合適當比例者為限。

TPIPAS (http://www.tpipas.org.tw)

- 臺灣個人資料保護與管理制度規範 (Taiwan Personal Information Protection and Administration System, TPIPAS) 是使事業以「PDCA方法論(Plan-Do-Check-Act)」，建立一套將個人資料保護與事業營運連結之系統化管理制度。
- 對於事業之個人資料管理制度進行內部控管、外部評量，及用以核發事業「資料隱私保護標章」(Data Privacy Protection Mark, DP Mark) 之依據。

Other Privacy Certifications & Standards

European Privacy Seal

https://www.european-privacy-seal.eu/

英國BS10012

Privacy Mark

日本JISQ15001

http://privacymark.org/

個資法施行日期

http://www.ithome.com.tw/itadm/article.php?c=70500

- 個資法施行細則草案:法務部2011年10月27日在官方網站公布
- 新版個資法修正施行之日起一年內必須完成對當事人的告知義務
  - 要能做到「一對一」的告知，得以書面、電話、傳真、電子文件或其他適當方式爲之
- 行政院會於2012年2月聽取法務部提出《個人資料保護法》施行規劃與展望報告
  - 擴大刑事處罰、以致刑事責任過重，特種個人資料適用要件過嚴、實務運作有困難，間接蒐集的個人資料應於1年內告知才能處理或利用、難以執行等

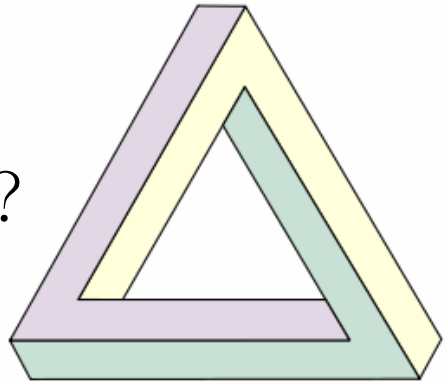
The Review

蒐集個資時 –

•告知當事人蒐集個資之目的、利用範圍等相關資訊。

•如需要蒐集特種個資，是否有引用的法源依據？

•避免過度個資內容，應與其使用之目的相關。



處理個資時 –

•制訂個資處理流程，以回應當事人行使個資權利的。

•有適當的安全措施(如11項適當安全維護措施)。

•在個資外洩時，有適當的事件處理方式，降低後續可能的損害。

利用個資時 –

•符合當初的蒐集目的，並在合理的範圍內使用。若不符，重新取得當事人的書面同意。

•作跨國的傳輸有適當的保護措施，並要求對方盡到個資保護責任

Source: http://jackforsec.blogspot.com/search/label/%E5%80%8B%E8%B3%87%E4%BF%9D%E8%AD%B7

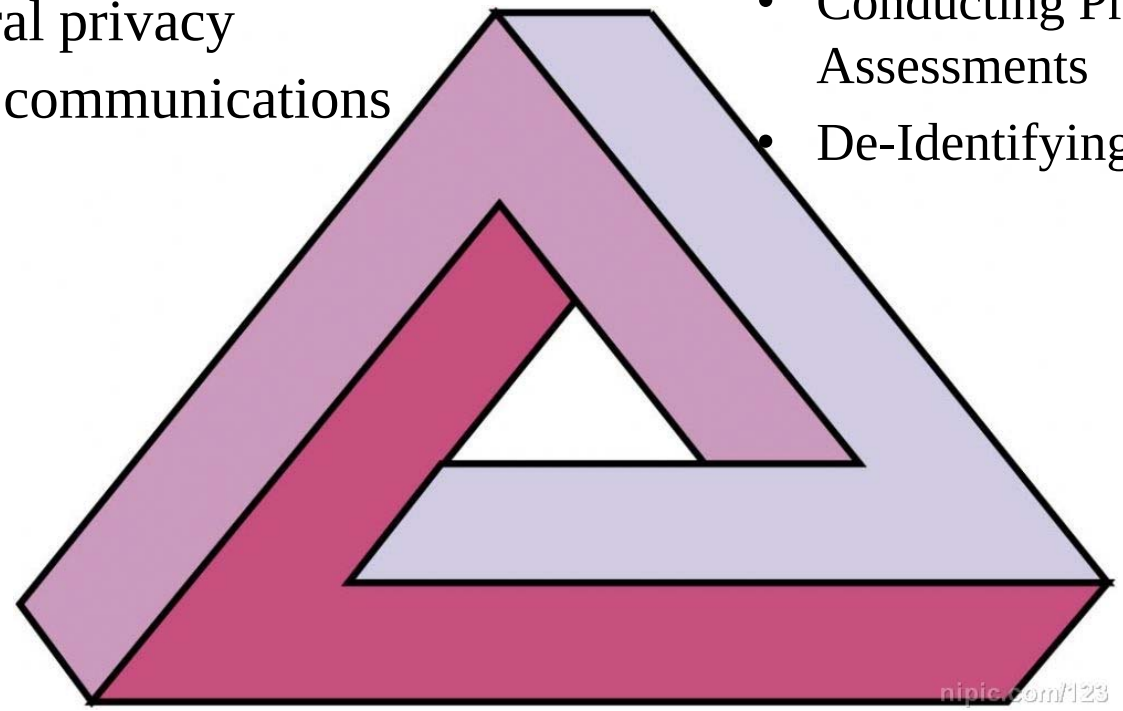
Privacy

Four dimensions of privacy

- Personal information (個資)
- Personal privacy
- Behavioral privacy
- Personal communications privacy

Privacy-Specific Safeguards

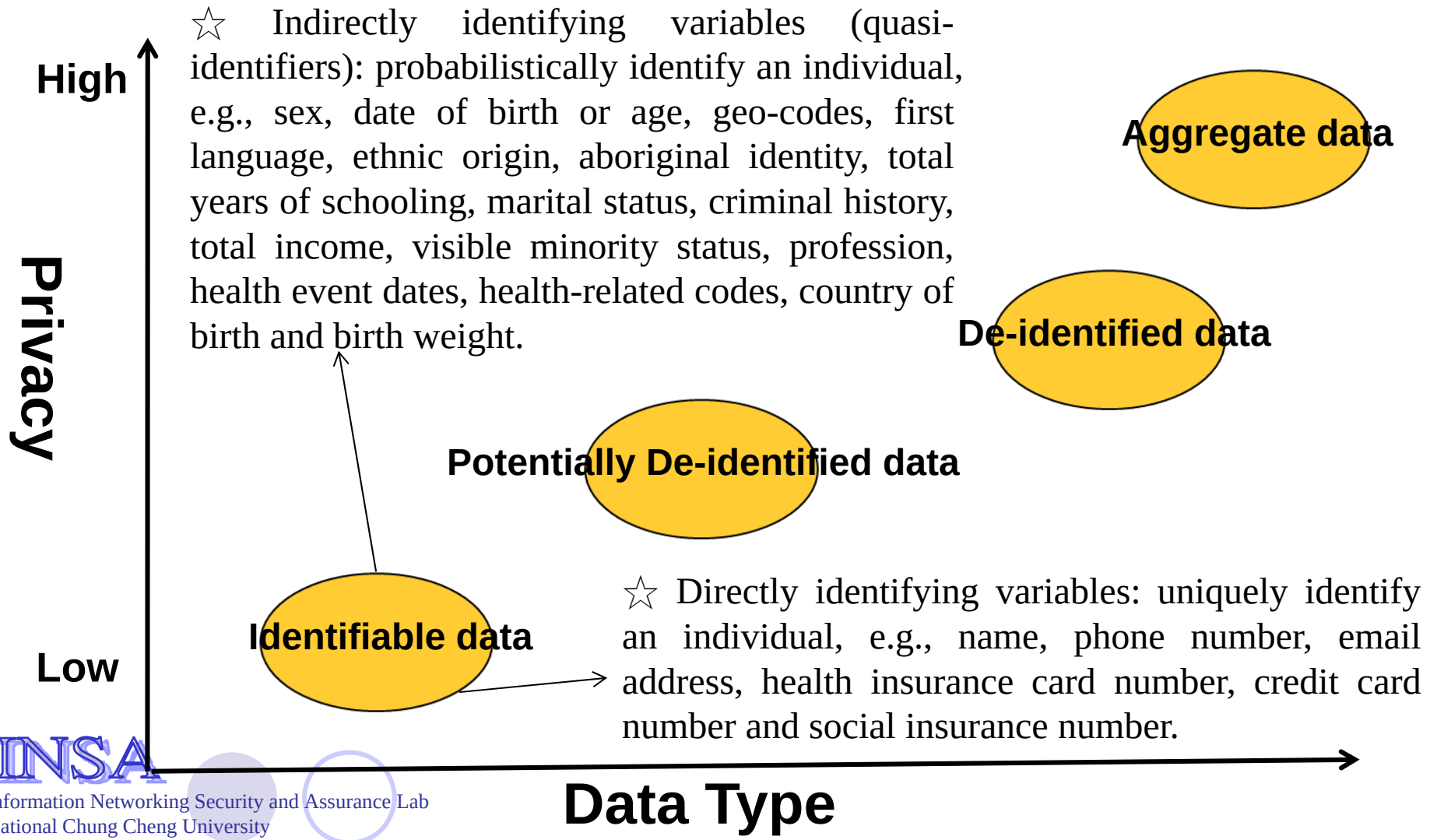
- Minimizing the Use, Collection, and Retention of PII
- Conducting Privacy Impact Assessments
- De-Identifying Information



Law Enforcement

De-Identification Techniques

De-Identification with Re-ID Risk



Suppression

- Suppress data information by removing or modifying data value

Name	Gender	Age
Bob	M	24
Alice	F	29
Jack	M	33

Name	Gender	Age
?	M	[21-25]
?	F	[26-30]
?	M	[31-35]

Generalization

- Modify data value to reduce data informative information based hierarchical attributes

Name	Telephone	Zip Code	Address
Alice	05-2720351	62102	嘉義縣民雄鄉三興村7鄰大學路一段168號

Name	Telephone	Zip Code	Address
Alice	05-2720	621	嘉義縣民雄鄉三興村

Perturbation

- Add noise or change data value
  - Add new record into database as a ‘noise’
  - Randomize change data value

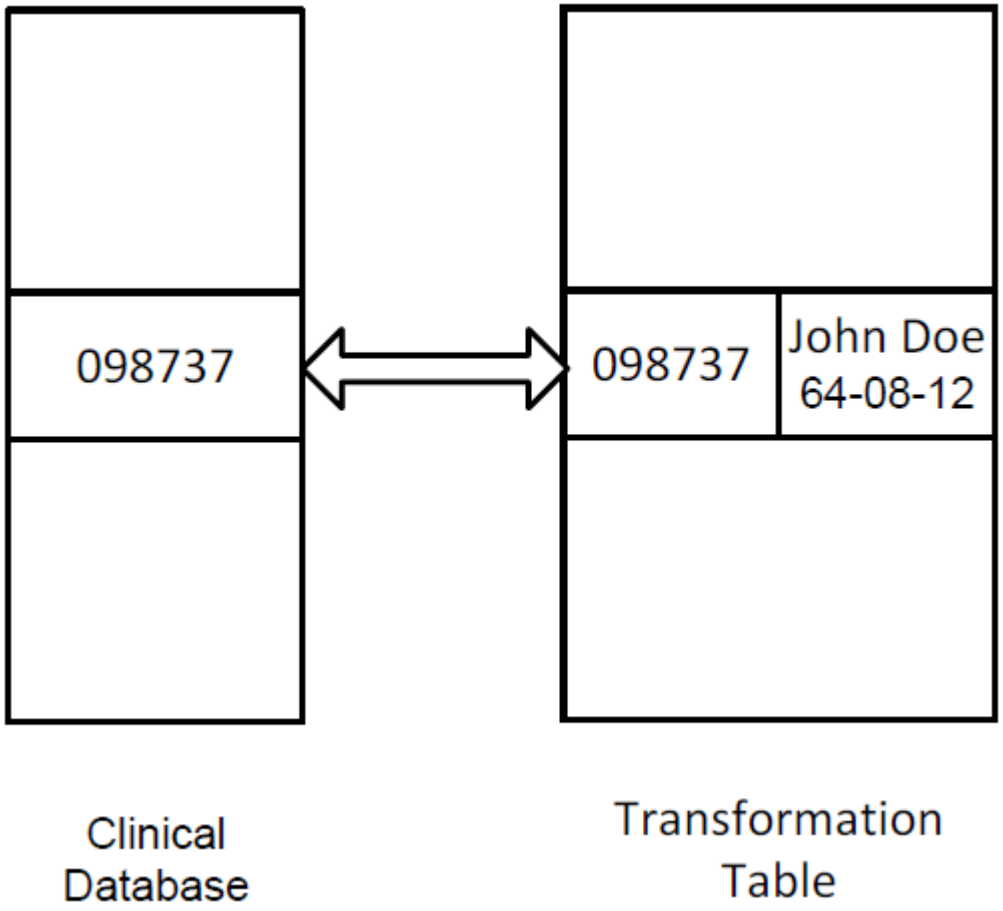
Name	Height	Weight	Age
Alice	160	49	20

Name	Height	Weight	Age
Alice	169	56	28
Bill	176	69	33

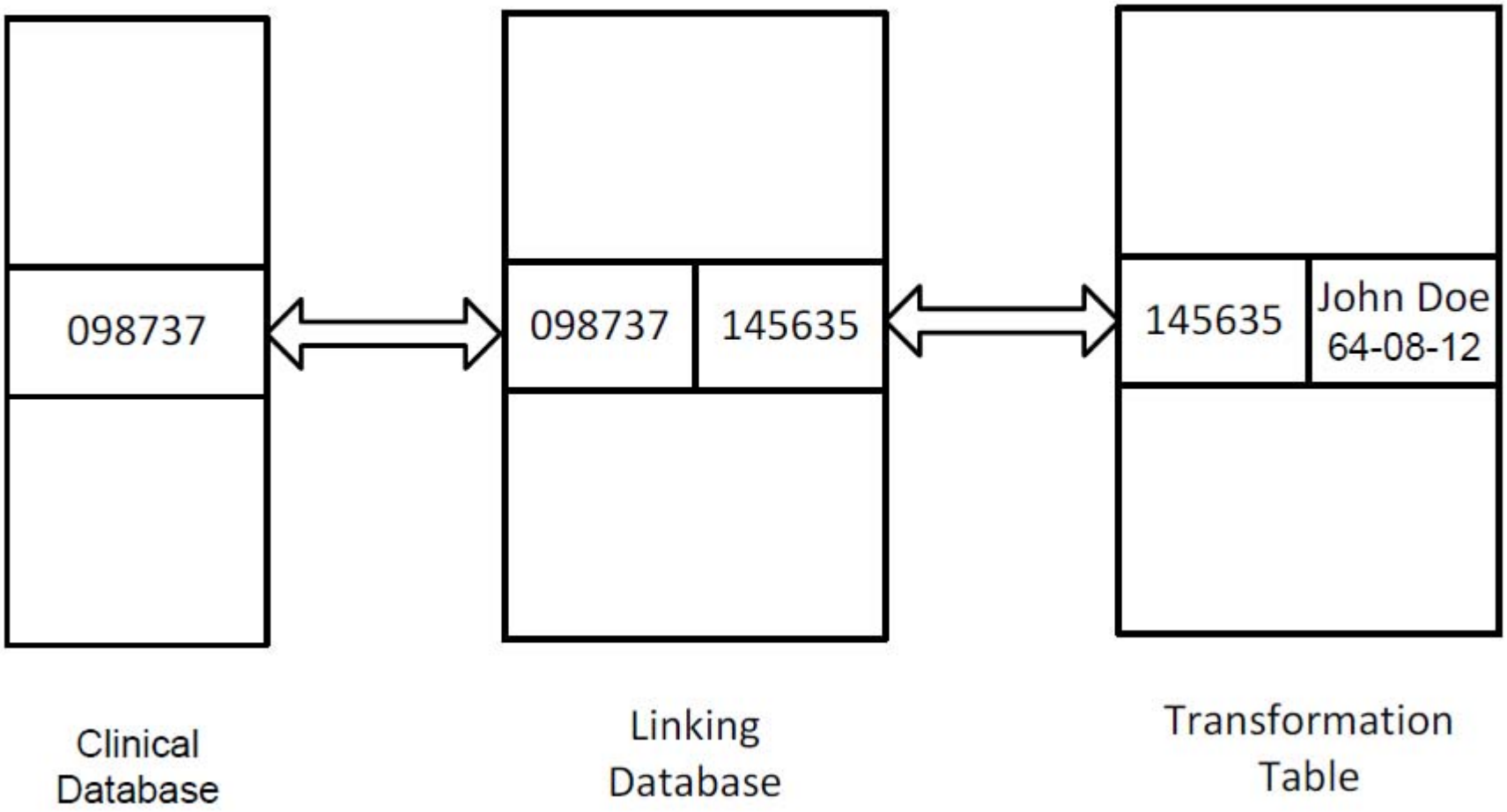
Pseudonymisation

- Using pseudonyms instead of real direct identifier
  - Single Coding
  - Double Coding
- Example
  - Original Data: ‘telephone number’ + ‘Age’ + ‘Zip code’
  - Replacing Data by a pseud-Id ‘1a2b3C4D’

Single Coding



Double Coding



Conclusion

以上內容純屬演講，

如有疑問純屬專家問題！