慟 !! 實聯制 ?! 
我們交出去的個資跑到哪裡去了no？

UCCU Hacker 成員 / Vic Huang
東吳大學法律學博士候選人 / Joy Ho (何念修)

目錄

實聯制系統

① 實聯制與自主開發系統
② 常見的實聯制系統設計
③ 外國類似的實聯制
④ 真實案例的實聯制系統漏洞(台灣)
⑤ 簡訊的另類攻擊方式 - 山不轉路轉
⑥ 實聯制系統對攻擊者有多香?

實聯制資訊的應用在個人資料保護法上的議題

① 實聯制：從一篇法官的投書談起
② 個資法怎麼說
③ 實聯制措施指引內涵
④ 合法的目的外利用 v. s. 違法的目的外利用
⑤ 實聯制下的法律關係拆解
⑥ 個資外洩或事故發生時……

講者簡介

Vic Huang

UCCU Hacker 成員

資安從業人員，鑽研 Web / Mobile / Blockchain / Privacy 等領域
曾分享於 DEFCON village , CODE BLUE , HITB , HITCON Community與 Pacific , 台灣資安大會等國內外研討會

Joy Ho (何念修)

東吳大學博士候選人

目前為執業律師，研究科技領域中資料保護的法律議題與隱私議題
曾分享科技偵查法、委外管理與個資事故處理等相關議題於國內外研討會

實聯制系統

疫情爆發的短短幾天...

2021.05.12

確診人數16人創下高峰，全台進入第二級警戒，所有餐廳賣場必須要有實聯制

2021.05.15

行政院早上八點的記者會，雙北面臨突然其來的180個本土案例與第三級警戒

2021.05.16

疫情升溫，全台尤其台北萬華與鄰近新北地區擴散，單日本土案例來到205

2021.05.17

本土案例再增加到333，雙北高中以下停課

2021.05.19

本土案例267例，全國進入三級警戒

實聯制與實名制

實名制

- 需填寫真實姓名與聯絡方式(電話)
- 2020年國內公務機關與一些場館都已開始實施

實聯制

- 需填寫可以聯絡的方式(電話)即可
- 2020年05月28號開始倡導將實名制改為實聯制，減少填寫非必須個人資料(姓名)的風險

在疫情升溫與沒有官方版的情形下

縣市政府與官方

- mycode 實聯制系統(整合台北通)
- 雲林Nubi-扭一下
- 台中市政府實聯制系統
- 疾管家實聯制系統

民間公司

- 防疫實聯衝衝衝
- 防疫門神
- Ragic
- 防疫實聯得來速
- 疫起簽

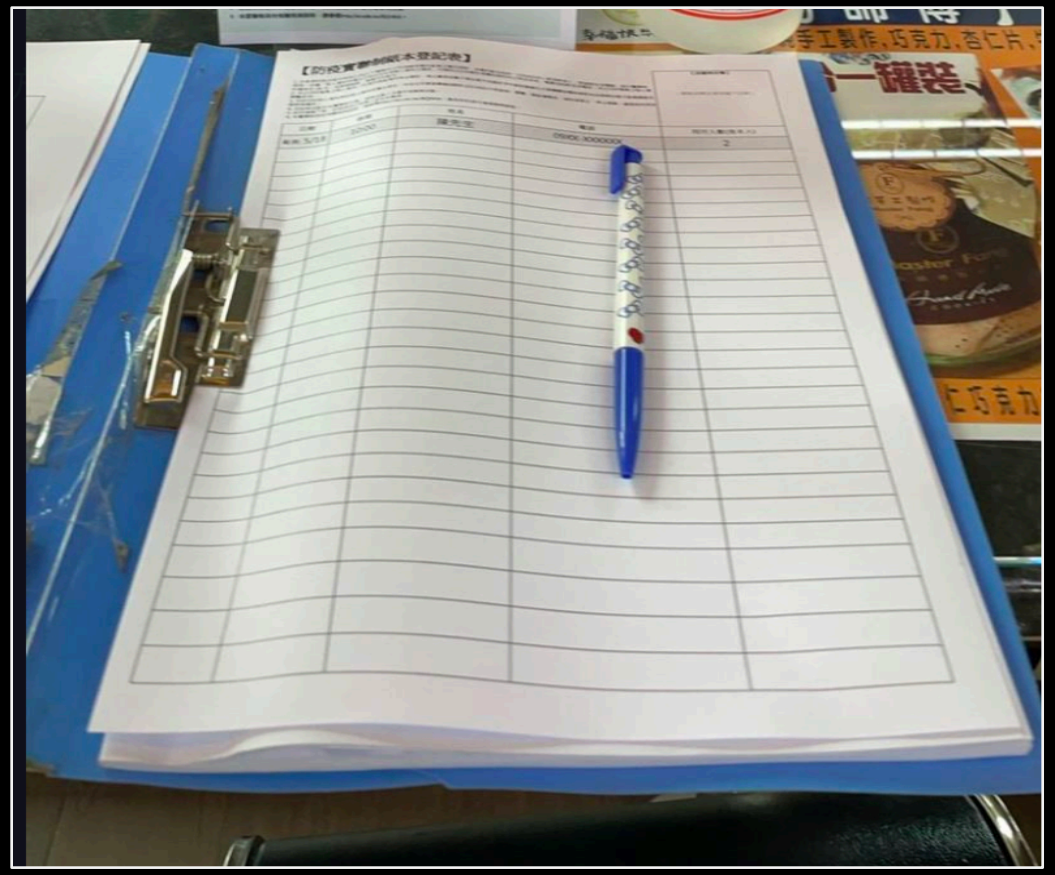
既有的系統疊加

- Google 表單
  - 工作室協助店家建立
  - 自製Plugin
- Survey Cake

開發者開源

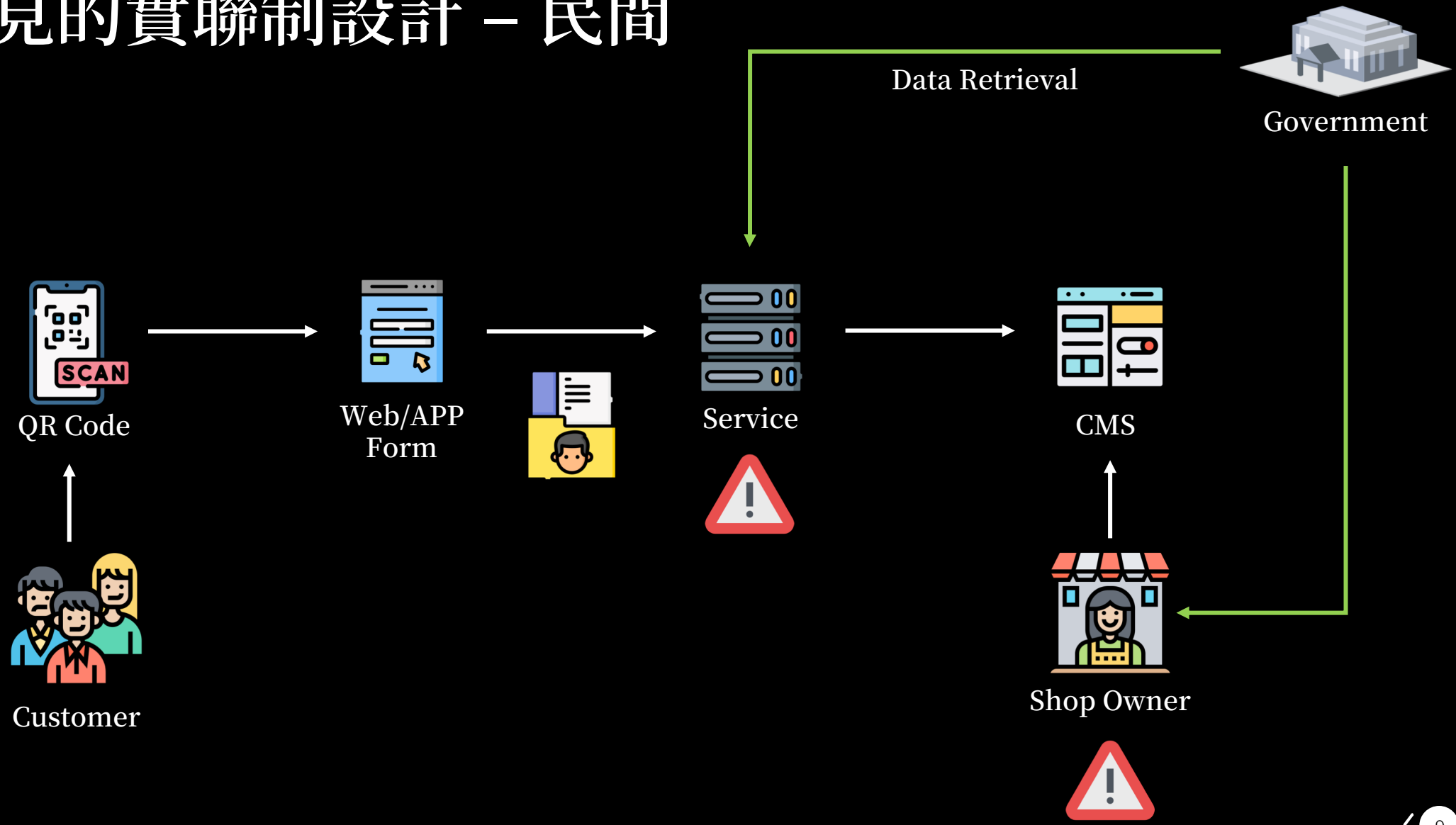
- Mutix-co COVID-19
- twlink.app

常見的實聯制設計

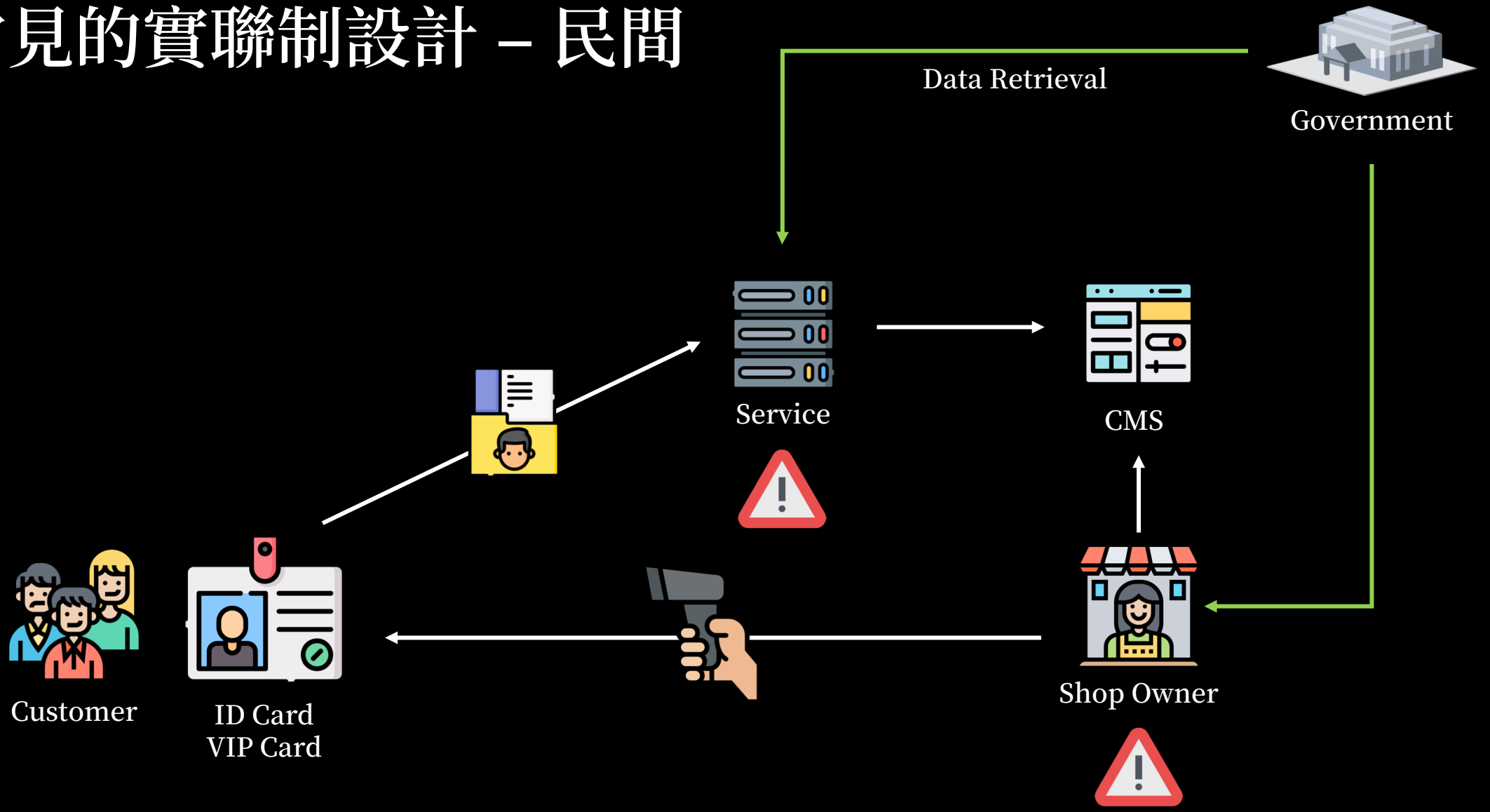



試算表
簡報
表單
建立精美的表單
Tom
個人
Google 表單可以幫您收集及整理資料，無論資料多寡都能幫您輕鬆搞定，而且完全免費。
前往 Google 表單
企業
Google Workspace
您喜愛的 Google 表單，加上專為團隊而設的額外安全保障和控制功能。
瞭解詳情

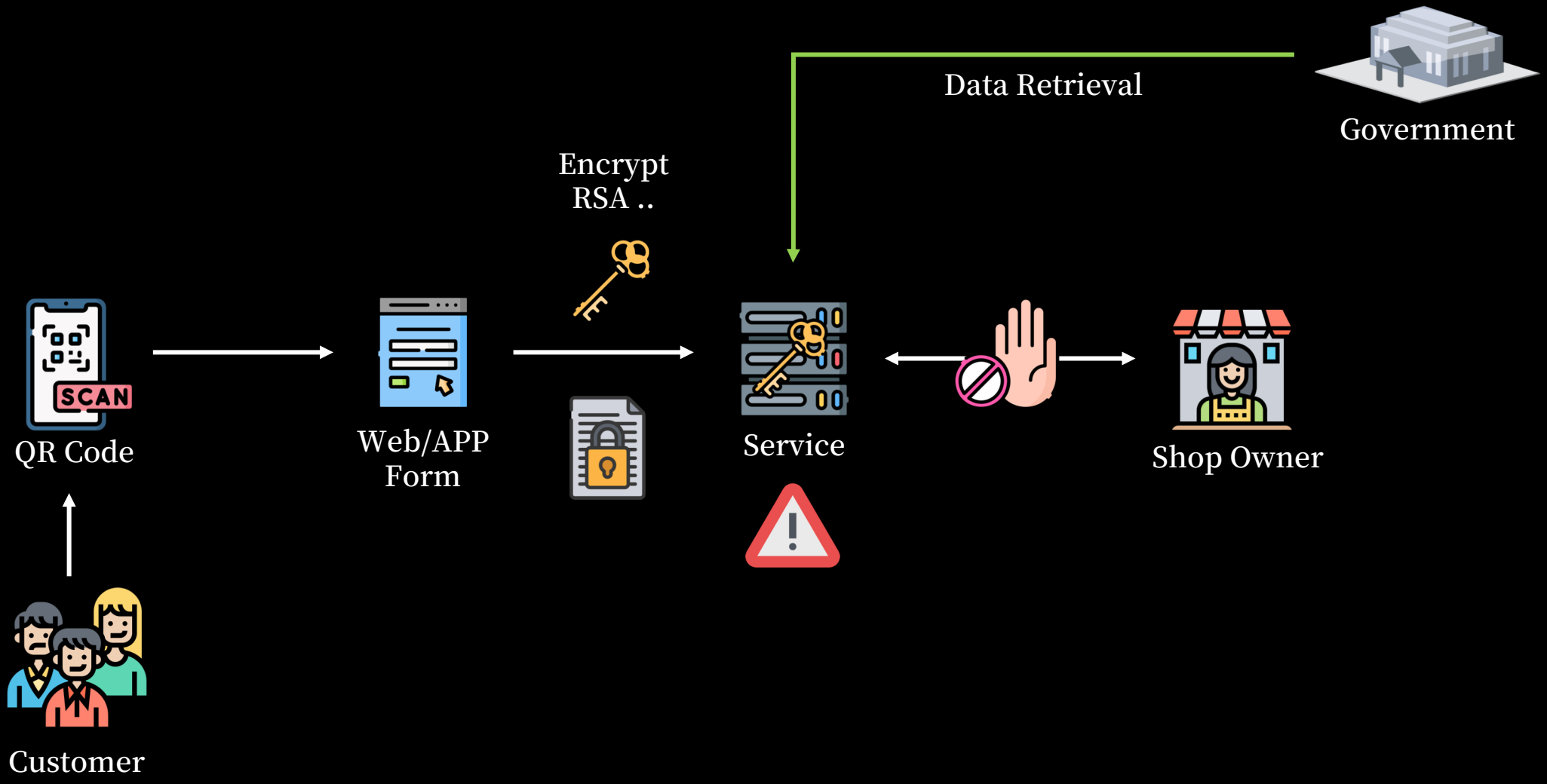
常見的實聯制設計 – 民間


Data Retrieval
Government
SCAN
QR Code
Web/APP
Form
Service
CMS
Customer
Shop Owner

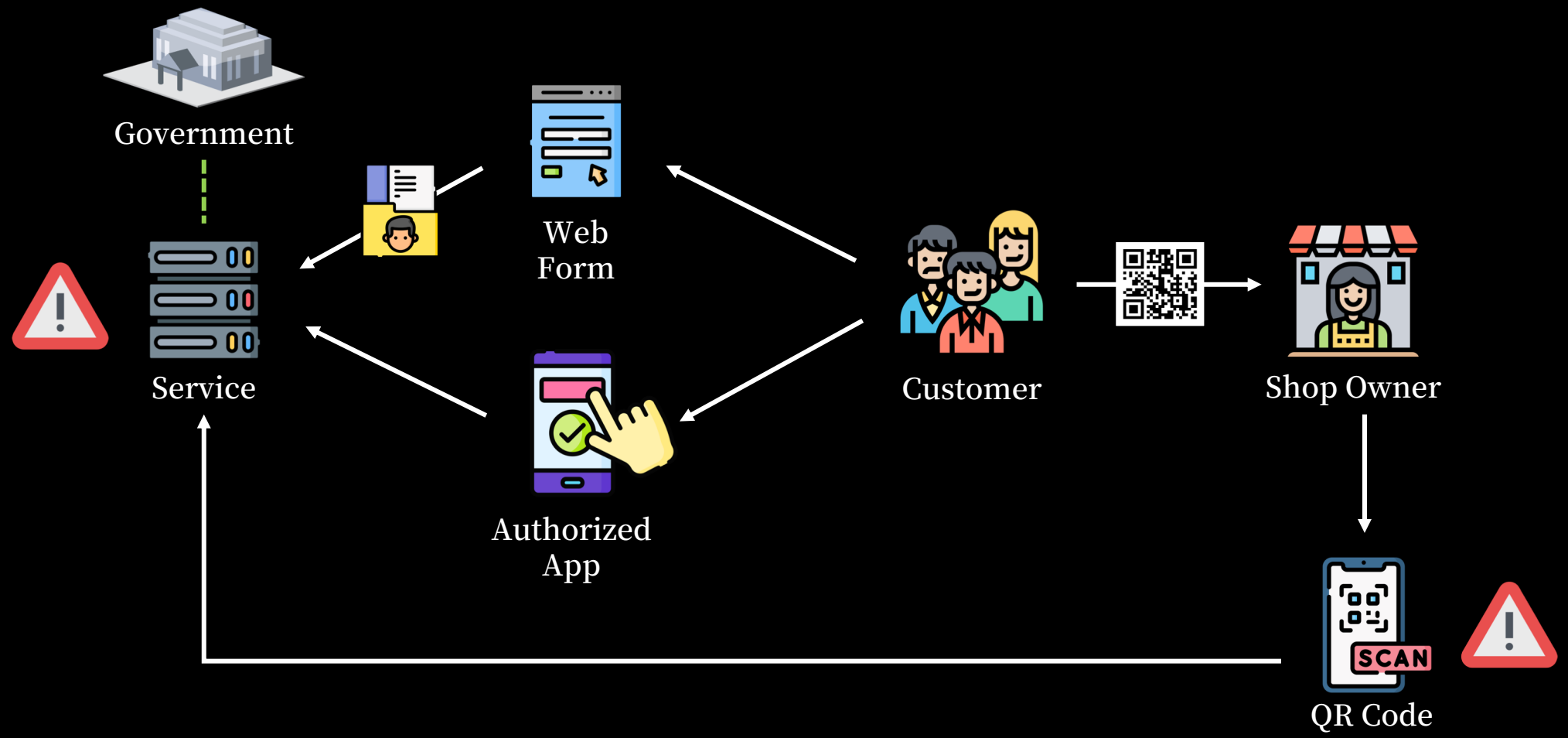
常見的實聯制設計 – 民間


Data Retrieval
Government
Service
CMS
Customer
ID Card
VIP Card
Shop Owner

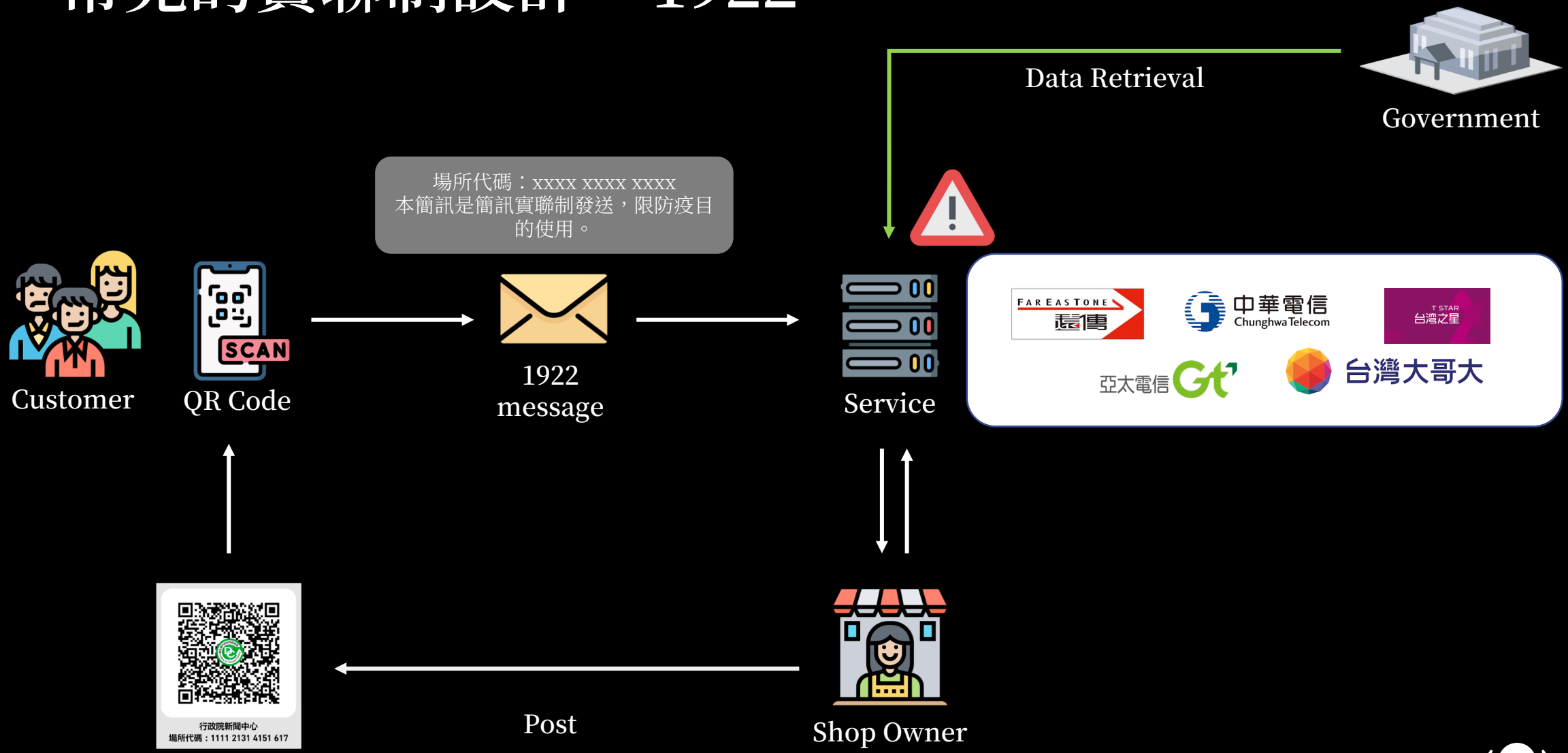
常見的實聯制設計 – 開源


Data Retrieval
Government
Encrypt
RSA ..
SCAN
QR Code
Web/APP
Form
Service
Shop Owner
Customer

常見的實聯制設計 – 縣市政府



常見的實聯制設計 – 1922



實聯制的資安風險

HITCON Zero Day 上回報的民間實聯制漏洞

- https://zeroday.hitcon.org/vulnerability/ZD-2021-00260
- https://zeroday.hitcon.org/vulnerability/ZD-2021-00274
- https://zeroday.hitcon.org/vulnerability/ZD-2021-00253
- https://zeroday.hitcon.org/vulnerability/ZD-2021-00247
- https://zeroday.hitcon.org/vulnerability/ZD-2021-00266

實聯制的資安風險

敘述

1. 註冊實名制管理系統後台帳號
2. 選擇問卷清單管理
3. 創建問卷後可得一組{number} 為問卷id
4. 透過IDOR修改id可任意變更他人實聯制問卷並可放入XSS等
   [redacted]/mgr/form/edit/{number}
5. 觀看問卷答案即可取得大量個資
   [redacted]/mgr/answer/index/{number}

實聯制的資安風險

社會

2021.05.26 05:58 臺北時間

【獨家】【實聯資安陷阱多1】「防疫實聯衝衝衝」使用人數破百萬　疑個資外洩急下架

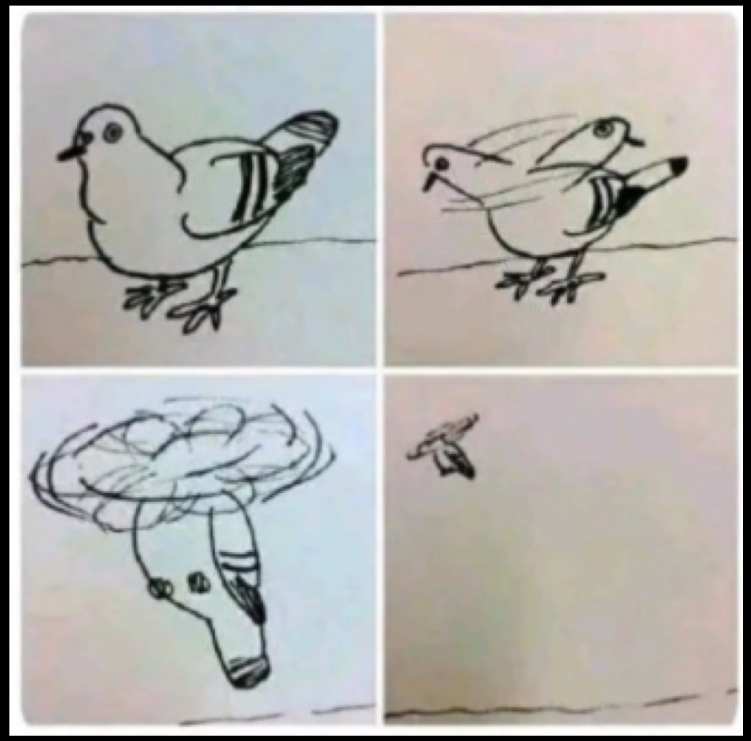
文｜劉文淵　攝影｜周永受

Reference : https://www.mirrormedia.mg/story/20210525soc002/

實聯制的資安風險

實聯制系統對攻擊者有多香?

- 漏洞發現與實現的難度低
- 為了搶市占率，多採用隕石開發
- 最新的個人資料(排除填寫假資料者)
  - 姓名
  - 手機
  - 行蹤與地理位置
  - email (option)
  - SNS ID (option)

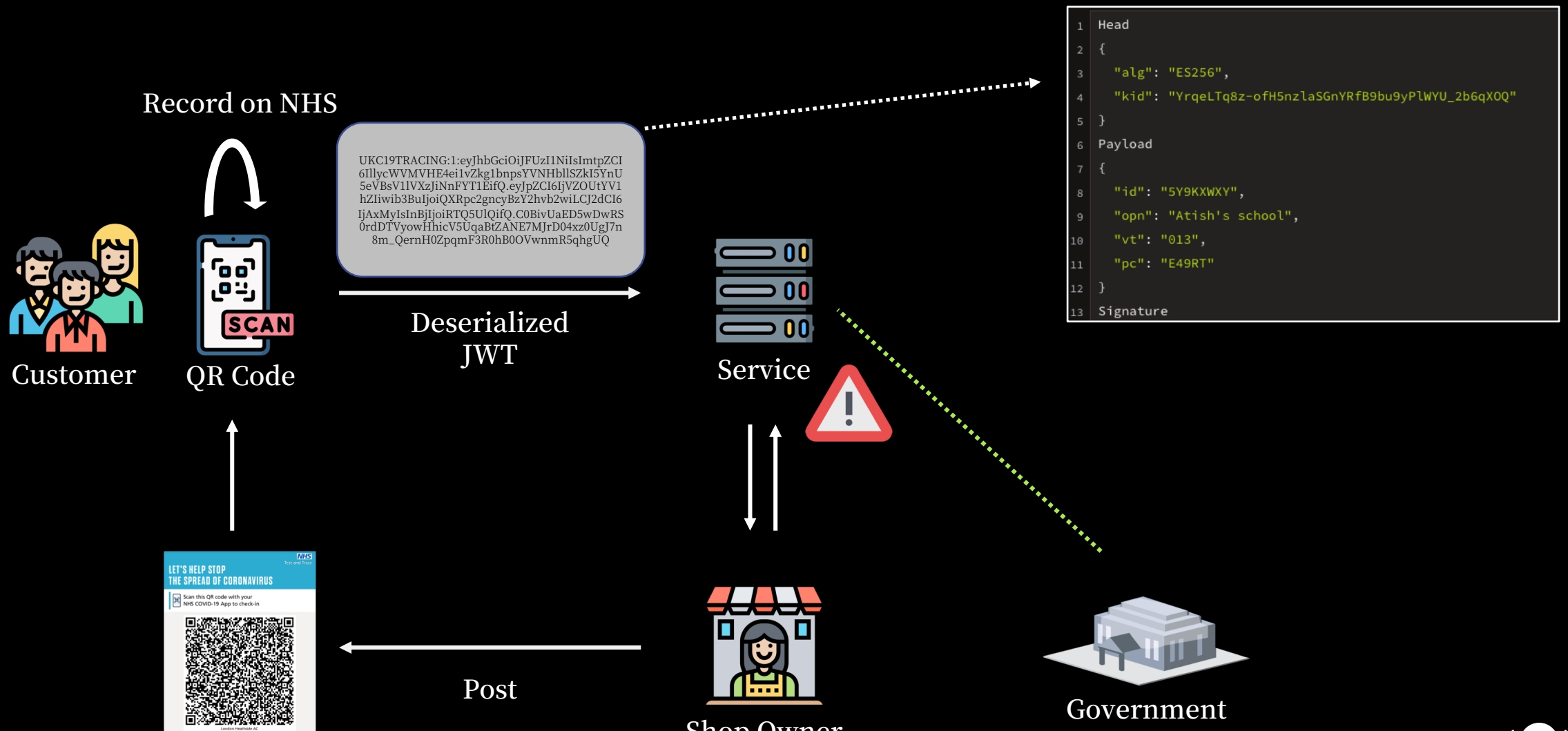


外國的實聯制系統

Nepal	COVIRA ("COVID-19 Risk Assessment tool")	Individual and regional risk assessment	web	Science Hub	In use	GNU GPLv3 compatible with open source OpenTrace		https://www.covira.info
New Zealand	NZ COVID Tracer	Point-of-interest journal, contact tracing, medical reporting, information	iOS, Android	Ministry of Health	in use	AGPLv3[304]	QR code and Exposure Notifications System	https://tracing.covid19.govt.nz
North Macedonia	StopKorona!	contact tracing	iOS, Android	Ministry of Health (North Macedonia), Nextsense		Proprietary	Bluetooth	stop.koronavirus.gov.mk/en
Norway	Smittestopp	contact tracing, route tracking	iOS, Android	Simula Research Laboratory / Norwegian Institute of Public Health (FHI)	in use	Proprietary	Exposure Notifications System	https://helsenorge.no/smittes

Reference : https://en.wikipedia.org/wiki/COVID-19_apps

外國的實聯制設計 – 以英國為例



QR code 存在的風險

若店家的QR code遭到置換或利用

- 連結至惡意或其他目的URL網頁
- 連結至惡意檔案下載
- 寄送簡訊~~至高額付費號碼~~
  - 獲得手機號碼作為釣魚用
- 撥打至高資費電話
  - 傳統的有0204、跨國電話

商家需要注意

- 需要不定期檢查是否遭人更換、掉包
- 注意張貼連結的正確性

民眾需要注意

- 注意電話號碼是否是1922
- 對於QR code對應的各種實聯制系統需有警覺

小結

QR code流程不同大致分為兩大類

- 商家申請後出示QR code，資訊由使用者輸入
- 使用者透過已經認證身份的服務產生QR code，讓商家掃描

服務本身的資安強度是一個顧慮

- 服務中儲存的資料本身就是個人資料
- 提供實聯制資料給商家存取的必要性
- 不良的開發，不透明的系統架構、權限控管、儲存與刪除資料
- QR code 的釣魚等容易誘騙一般人上當

實聯制資訊的應用在個人資料保護法上的議題

實聯制：從一篇法官投書談起

「我必須成為吹哨者：「簡訊實聯制」資訊遭利用，指揮中心請儘速反應」

- 時間：2021.06
- 中央流行疫情指揮中心強調簡訊只會傳送給電信公司，且只保留28天，並僅限作為疫調使用。
- 刑事警察局在搜索票聲請書中，利用嫌犯以簡訊實聯制發送的簡訊來鎖定嫌犯行蹤。
- 只要申請搜索通訊紀錄就可取得嫌犯發送的所有簡訊內容，包括1922實聯制簡訊。

政策

我必須成為吹哨者：「簡訊實聯制」資訊遭利用，指揮中心請儘速反應

作者 張淵森　2021-06-23

近日發生「簡訊實聯制」資料被拿來使用在疫調之外的情形，只有在指揮中心積極面對目前的缺失並修正改進後，才能重拾民眾對政府的信任，繼續支持簡訊實聯制。

圖片來源：聯合報系資料照。

行政院自5月19日推出「簡訊實聯制」，由民眾用手機掃描店家的QRCode，即會出現「場所代碼：0000 0000 0000 0000 本簡訊是簡訊實聯制發送，限防疫目的使用」的

涉及什麼議題？

實聯制資料拿來偵查犯罪是合法的嗎？

- 指揮中心說實聯制資料僅限於疫調使用，實聯制指引上也禁止目的外利用。
- 但是檢調機關拿來做為偵查犯罪使用，這樣是合法的嗎？

誰可以決定實聯制資料的使用目的？誰應該當責？

- 在實聯制的架構下，誰負責管理好我的個人資料？
- 當個資被濫用、受侵害時，誰應該當責？

當我發現我的資料遭到不當使用時，我有哪些主張我權利的手段？

個資法怎麼說

什麼叫做個資？

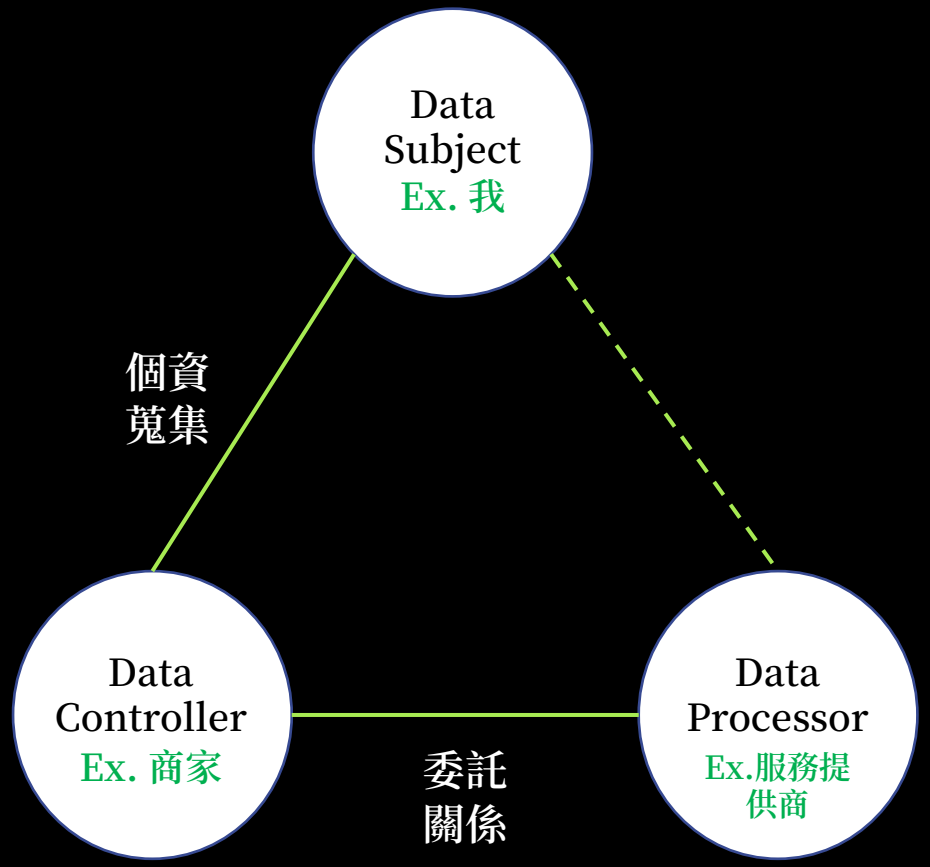
- 得以直接或間接識別個人之資料

先區別不同的法律主體

- 個資主體 (Data Subject)
  - 民眾
- 個資蒐集機關 (Data Controller)
  - 商家(紙本)、政府(1922)
- 受委託蒐集、處理的機關 (Data Processor)
  - 服務提供者

不同的法律行為

- 蒐集、處理、利用



個資法下的特定目的

目的明確化原則 (Purpose Specification)

- 蒐集個資須明確其目的

利用限制原則（Use Limitation principle）

- 蒐集、處理、利用個資必須扣緊特定目的
- 未得資料當事人之同意或法律另有規定者，所蒐集之個資不得為蒐集時所定目的外之利用

目的外利用

- 個資法第20條

實聯制措施指引內涵

蒐集前告知

為增加整體防疫措施之透明性、提高民眾之信賴，機關蒐集民眾個人資料時，應明確告知下列事項：

(一) 蒐集機關之名稱。

(二) 蒐集之目的：防疫目的，依據「個人資料保護法之 特定目的及個人資料之類別」為代號 012 公共衛生或傳染病防治之特定目的，且不得為目的外利用。

(三) 蒐集之個人資料項目：蒐集資料應符合最少侵害 原則，如電話號碼。

(四) 個人資料利用之期間：自蒐集日起 28 日內。

(五) 個人資料利用之對象及方式：為防堵疫情而有必要時，得提供衛生主管機關依傳染病防治法等規定進行疫情調查及聯繫使用。

(六) 當事人就其個人資料得依個人資料保護法規定， 向蒐集之機關行使權利，包括查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止處理或 利用、請求刪除，及行使方式。

(七) 當事人不同意提供個人資料對其權益之影響，如 無法進入場館或參與活動。 告知時可採取「多層次告知」方式，將重要事項於明顯 處揭示，並以 QR Code 或網址連結提供其他細節事項。

實聯制措施指引內涵

資料安全維護義務之實踐

- 以紙本供當事人填具個人資料時，應以遮蔽或其他適當方式保護填寫者之個人資料，避免後填寫者得閱覽先填寫者之個人資料。

資訊安全風險評估

- 機關以資訊系統或 APP 實施實聯制者，應進行資訊安全風險評估，採行相符安全控制措施，確保系統安全防護水準。

實聯制措施指引內涵

28日的保存期限與刪除承諾

- 各機關對於蒐集之個人資料僅可保存 28 日，屆期即應主動將個人資料予以刪除或銷毀，並應留存執行刪除或 銷毀之項目及日期等軌跡紀錄。

分析：

- 個資法對資料保存期限留有彈性，交由各資料蒐集主體依據特定目的定之。指引中的28日保存期限，是較個資法更嚴格之規定，本應能降低資料外洩之風險，提供更有效的保護。

法律漏洞：

- 告知28日之保存期限 v.s. 告知更長的保存期限

實聯制措施指引性質

實聯制措施指引是法律嗎？

- 詳查實聯制措施指引的內容，顯然是立基於個人資料保護法，並加上一些原則性指導。實聯制措施指引，係一宣導、鼓勵性質的文件，若資料蒐集時未能遵循該指引並不會產生相應的罰則。
- 但應注意者是，實聯制指引的內容多數是來自於我國個資法的規定，因此若違反指引內容時，很可能因為同時違反個資法的規定而受到處罰。

違反指引內容，但不違反個資法	不罰
違反指引內容，也違反個資法	罰(因為個資法)
不違反指引內容，但違反個資法	罰(因為個資法)

合法的目的外利用 V.S. 違法的目的外利用

合法的目的外利用

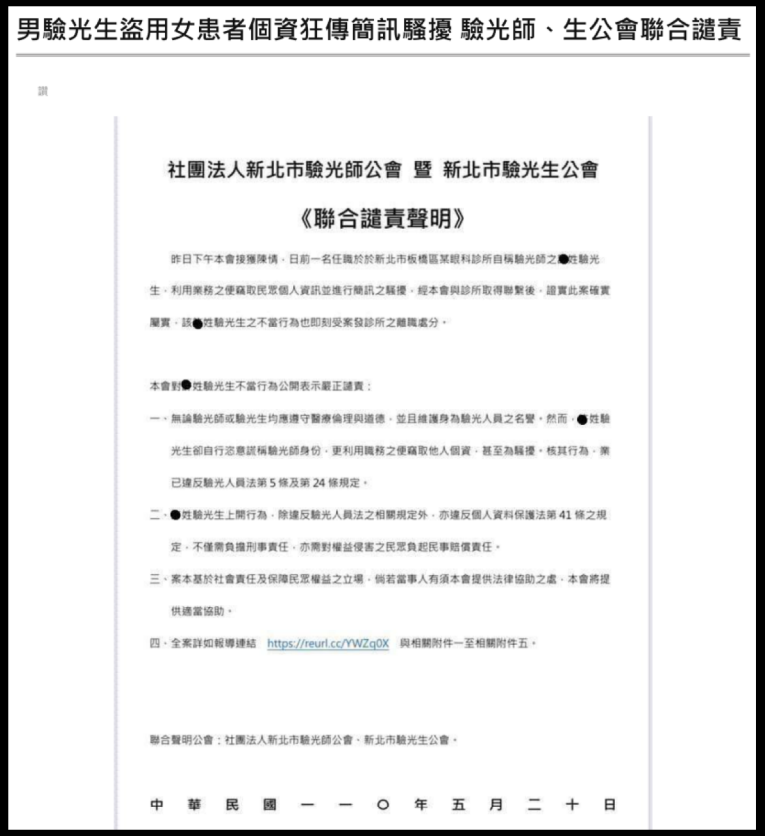
- 蒐集個資須有明確目的、且須明確告知。
- 目的外利用屬於例外，應符合個資法第20條的規定：
- 例外條件：法律明文規定；公共利益；免除當事人之生命、身體、自由或財產上之危險；防止他人權益之重大危害；統計或學術研究；當事人同意；有利於當事人權益。
- 常見情形：檢調查緝犯罪

違法的目的外利用

- 驗光生案例

個資濫用：驗光生案例

- 時間：2021.05
- 事件摘要：女性患者至眼科就診，因需實聯制填寫姓名電話等個資，卻遭診所男驗光生盜用並連發簡訊騷擾。
- 涉及法條：個資法第41條「意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或……，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。」



男驗光生盜用女患者個資狂傳簡訊騷擾 驗光師、生公會聯合譴責

社團法人新北市驗光師公會 暨 新北市驗光生公會

《聯合譴責聲明》

昨日下午本會接獲陳情，日前一名任職於於新北市板橋區某眼科診所自稱驗光師之●姓驗光生，利用業務之便竊取民眾個人資訊並進行簡訊之騷擾，經本會與診所取得聯繫後，證實此案確實屬實，該●姓驗光生之不當行為也即刻受案發診所之離職處分。

本會對●姓驗光生不當行為公開表示嚴正譴責：

一、無論驗光師或驗光生均應遵守醫療倫理與道德，並且維護身為驗光人員之名譽，然而，●姓驗光生卻自行恣意謊稱驗光師身份，更利用職務之便竊取他人個資，甚至為騷擾，核其行為，業已違反驗光人員法第 5 條及第 24 條規定。

二、●姓驗光生上開行為，除違反驗光人員法之相關規定外，亦違反個人資料保護法第 41 條之規定，不僅需負擔刑事責任，亦需對權益侵害之民眾負起民事賠償責任。

三、案本基於社會責任及保障民眾權益之立場，倘若當事人有須本會提供法律協助之處，本會將提供適當協助。

四、全案詳如報導連結 https://reurl.cc/YWZq0X 與相關附件一至相關附件五。

聯合聲明公會：社團法人新北市驗光師公會、新北市驗光生公會。

中 華 民 國 一 一 〇 年 五 月 二 十 日

實聯制指引與個資法

實聯制個資用作疫調之外的目的，合法嗎？

- 指引怎麼說？- 蒐集係為了防疫目的，不得為目的外利用。
- 個資法怎麼說？-只要符合第20條的規定，並無不可。

其他假設案例

- 案例1：商家蒐集實聯制個資時，在告知事項額外說明「實聯制所蒐集之個資，另將用於行銷目的」並取得當事人同意。並將實聯制所蒐集之個資用以寄送廣告訊息。
- 案例2：商家使用自己APP新增實聯制功能，並且在其中附上實聯制指引，刪除不得作目的外利用等字。商家將APP內蒐集之個資用以做個人化分析與廣告推送。
- 案例3：商家蒐集實聯制個資時，在告知事項額外說明「實聯制所蒐集之個資，將與消費紀錄連結，故個資將保存五年」。商家保存個資超過28天。

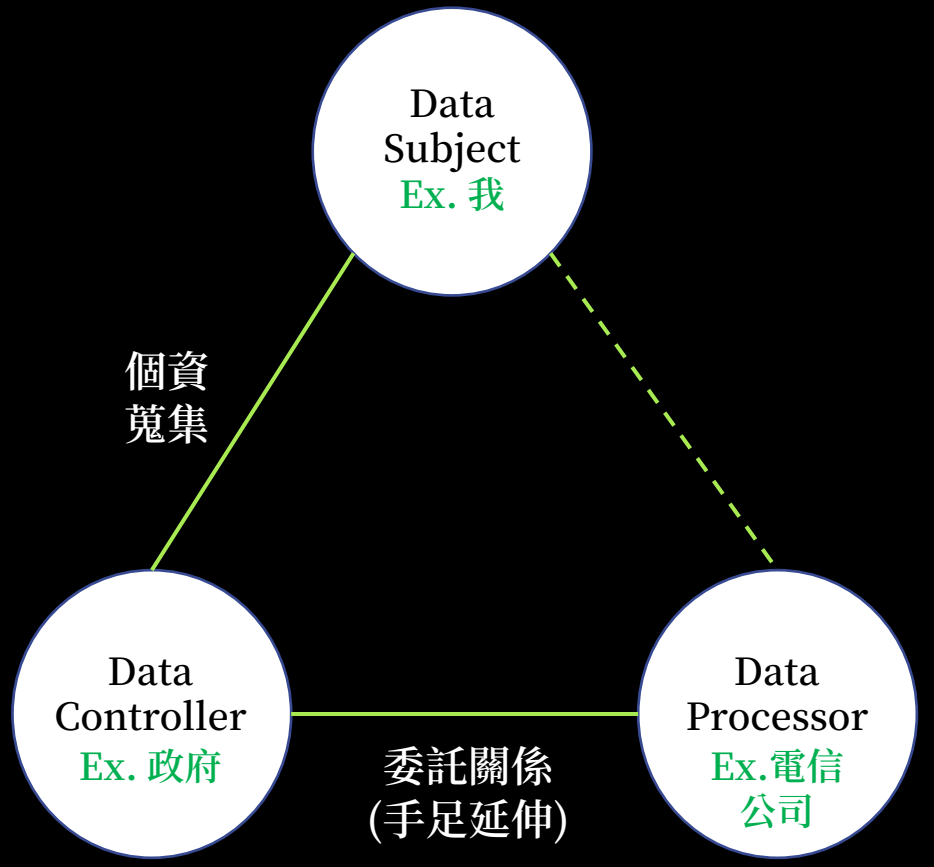
實聯制下的法律關係拆解

不同的法律主體

- 個資主體 (Data Subject)
  - 民眾
- 個資蒐集機關 (Data Controller)
  - 商家、政府(1922)
- 受委託蒐集、處理的機關 (Data Processor)
  - 資訊系統服務提供商、電信業者(1922)

再區別不同的法律行為

- 委託 + 蒐集、處理、利用



實聯制措施下個人資料之資料流

#	個人資料與實聯制資料流向	資料類型	對應系統設計	使用者同意項目
A	資料主體 → 商家	• 姓名 • 電話	• 紙本	• 實聯制指引
B	資料主體 → 商家 → 服務提供者	• 姓名 • 電話 • email	• Google 表單 • 民間實聯制系統 • 民間實聯制系統加密版 • 證件掃瞄	• 實聯制指引 • 服務提供者的 ToS (option)
C	資料主體 → 服務提供者(預先身份認證)	• 服務提供者可識別的代碼	• 記名 APP • 1922	• 記名 APP 或是加入會員的 ToS • 實聯制指引

委託機關與受託者各自的責任－以實聯制為例

委託機關（政府）	**監督義務**	實體內涵	預定蒐集、處理或利用個資之範圍、類別、特定目的及其期間、安全維護措施、複委託、委託關係終止時的刪除返還…
	定期查核紀錄	程序規範	委託人必須定期確認受託人執行狀況，並將確認結果紀錄之。
受託者（電信業者）	**契約義務**		受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。
	法遵通知義務		受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。

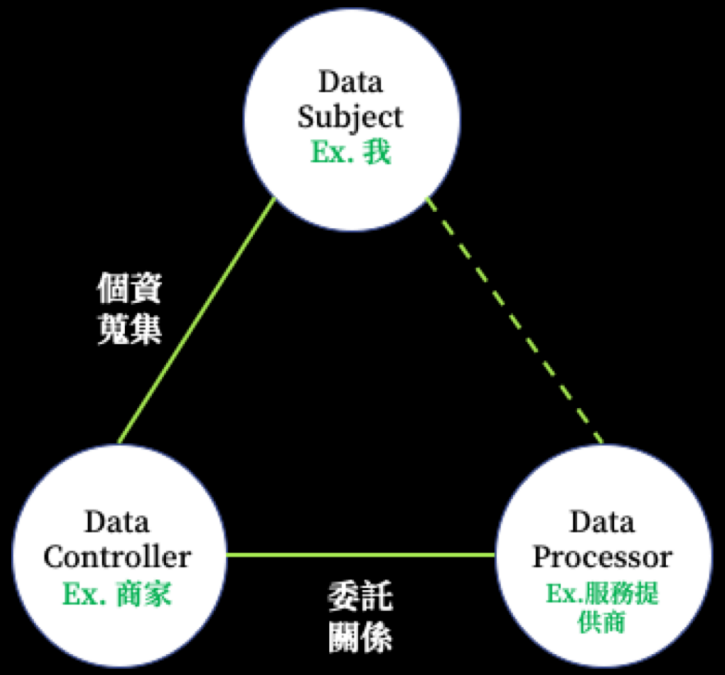
個資外洩或事故發生時……

誰該負什麼責任？

- 委託機關(ex.店家/政府)為責任承擔者
  - 管理之個人資料，如有被竊取、洩漏、竄改或其他侵害者，應於於查明後通知當事人（個資法第12條）
- 受委託者(ex.資訊服務提供者/電信業者)該做什麼？
  - 通知委託機關
  - 通知當事人？ 必須依照委託機關之指示進行

個資主體可以跟誰求償？

- 委託機關(ex.店家/政府)負擔損害賠償責任
- 此外，受委託者(ex.資訊服務提供者/電信業者)則對委託機關負擔契約責任



結論

- ~~大家都使用1922，本議題已經過氣~~
- 熱心公益之餘，請避免隕石開發導致大量漏洞的產生
- 實聯制由於蒐集的資料係屬個人資料，在系統與機制上面應以最小限度存取為原則，並且注意是否有其他機制可能導致資料用於疫調外的目的
- 實聯制指引實際上並不具有法律效力，對個資的保護仍以個資法的規定為準
- 若有個資外洩或侵害事故發生，民眾可以向個資蒐集機關主張權利

謝謝您的聆聽

Vic Huang / UCCU Hacker 成員
soulfood9487@gmail.com

Joy Ho / 東吳大學法律學博士候選人
joydxg@gmail.com