110 年委託研究報告

110 年度電信事業運用數據資料提供創新應用服務治理模式之研究
期末報告

計畫委託機關：國家通訊傳播委員會

中華民國 110 年 11 月

110 年委託研究報告

PG11004-0171

110 年度電信事業運用數據資料提供創新應用服務治理模式之研究
期末報告

受委託單位

財團法人資訊工業策進會

計畫主持人

顧振豪

共同主持人　協同主持人

葉奇鑫　　張乃文

研究人員

邱映曦、孫鈺婷、阮韻蒨、張恩若、許嘉芳

本報告不必然代表國家通訊傳播委員會意見

中華民國 110 年 11 月

目次

目次 V

表次 X

圖次 XI

提要 XIII

第一章 整體說明 1

第一節 研究緣起 1

第二節 研究方法 3

第三節 工作項目 5

第二章 電信事業配合執行維護國家安全公共利益電信資料應用研析 10

第一節 愛沙尼亞 10

第二節 美國 18

第三節 英國 24

第四節 日本 30

第五節 韓國 49

第六節 小結 59

第三章 電信服務業創新應用現況實際應用案例與政策法制研析 ..63

第一節 愛沙尼亞 63

本報告之智慧財產權屬於國家通訊傳播委員會

第二節　德國 68
第三節　美國 71
第四節　英國 74
第五節　日本 81
第六節　韓國 88
第七節　小結 92
第四章　電信事業運用數據資料創新應用服務治理模式研析（網路公眾意見諮詢與2場實例分享座談會） 96
第一節　網路公眾意見諮詢 96
第二節　實例分享座談會 98
第三節　初步建議 107
第五章　電信事業運用數據資料提供創新應用服務治理模式研究建議（解決方案座談會） 115
第一節　解決方案座談會執行摘要 115
第二節　座談會議題討論與解決方案建議 128
第六章　諮詢服務 137
第一節　議題一：向電信事業蒐集收視行為統計資料適法性研析 137
第二節　議題二：電信事業之定型化服務契約條款研析 147

本報告之智慧財產權屬於國家通訊傳播委員會

第三節　議題三：電信事業提供政府合理利用個資於跨領域共享.....163
第四節　議題四：異業合作涉及跨領域業務資料應用促進當事人資料自主運用.....173
第五節　議題五：中國大陸個人信息保護法簡介.....182
第七章　電信事業運用數據資料提供創新應用服務治理模式之相關決策作業流程標準之建議.....195
第一節　決策流程建議.....196
第二節　法規面建議.....198
第三節　政策與資料治理面建議.....204
第八章　執行與研究發現.....213
第一節　電信事業配合執行維護國家安全公共利益電信資料應用研析.....213
第二節　電信服務業創新應用現況實際應用案例與政策法制研析.....214
第三節　電信事業運用數據資料創新應用服務治理模式研析（網路公眾意見諮詢與 2 場實例分享座談會）.....216
第四節　電信事業運用資料創新應用服務治理模式研析217
第五節　諮詢服務.....218

本報告之智慧財產權屬於國家通訊傳播委員會

第六節　電信事業運用數據資料提供創新應用服務治理模式之相關決策作業流程標準之建議.....222
第九章　結論 224
附錄 231
附錄 1： 電信加值應用大調查問卷.....231
附錄 2： 電信加值應用大調查問卷結果.....245
附錄 3： 110 年 8 月 2 日座談會（一）會議紀錄.....253
附錄 4： 110 年 8 月 4 日座談會（二）會議紀錄.....272
附錄 5： 110 年 10 月 13 日座談會簡報.....290
附錄 6： 日本電信通訊事業個人資料保護指引.....299
附錄 7： 日本新冠肺炎密切接觸者應用程式使用規則....318
附錄 8： 日本新冠肺炎密切接觸者應用程式隱私保護方針.. 324
附錄 9： 日本 KDDI 個人隱私政策摘要.....330
附錄 10： 日本 NTT Docomo 個人資料憲章.....333
附錄 11： 日本 NTT Docomo 隱私政策 335
附錄 12： 日本 NTT Docomo 行動空間統計指引 339
附錄 13： 韓國大數據個人情報保護準則.....342
參考書目 354
中文參考資源 354

本報告之智慧財產權屬於國家通訊傳播委員會

外文參考資源 356

本報告之智慧財產權屬於國家通訊傳播委員會

表次

表 1 資通訊技術傳輸資料維護國家安全公共利益應用案例與相關法規配套之整理.....61

表 2 各國電信事業運用數據資料創新應用案例與相關法規配套整理.....94

表 3 110 年 8 月 2 日座談會專家名單.....99

表 4 110 年 8 月 4 日座談會專家名單.....100

表 5 110 年度電信事業運用數據資料提供創新應用服務治理模式座談會討論摘要表.....104

表 6 110 年 10 月 13 日座談會專家名單.....116

表 7 110 年 10 月 13 日座談會議程.....116

表 8 各國電信事業配合維護國家安全、公共利益提供電信資料案例整理.....128

表 9 可能阻礙資料共享議題對應座談會討論整理.....131

表 10 電信事業資安與個資驗證之相關國際與我國國家標準.....134

表 11 告知之形式上要求檢查清單.....151

表 12 《個人資料保護法》第 8 條要求之告知事項檢查清單.....154

表 13 有效同意之要件.....159

表 14 草擬《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》修正草案條文對照表.....199

本報告之智慧財產權屬於國家通訊傳播委員會

圖次

圖 1　計畫研究方法論 3

圖 2　DATA EXCHANGE LAYER X-TEE.....11

圖 3　HOIA 運作方式 14

圖 4　PMD 實時顯示人口移動變化 16

圖 5　NHS COVID-19 簡介與功能 25

圖 6　COCOA 使用說明 32

圖 7　KDDI 人口動態分析預測系統 35

圖 8　KDDI 支援國家與自治團體對於災害因應之資料系統.....37

圖 9　行動空間統計說明 38

圖 10　GEPP 技術運用概念圖 51

圖 11　KT 與東非最大電信業者 SAFARICOM PLC 合作.....53

圖 12　PARGI.EE 使用介面.....64

圖 13　TELIA 人口流動分析.....67

圖 14　M25 電信與交通大數據應用.....78

圖 15　英國國家資料戰略整體架構.....79

圖 16　行動空間統計運用意象圖 82

圖 17　車廂內之數位動態車輛螢幕.....83

圖 18　行動空間統計應用於提升購物便利性區域循環巴士.....84

本報告之智慧財產權屬於國家通訊傳播委員會

圖 19　110 年 8 月 2 日座談會 105
圖 20　110 年 8 月 4 日座談會 106
圖 21　110 年 10 月 13 日座談會-1.....126
圖 22　110 年 10 月 13 日座談會-2.....127
圖 23　短中長期解決方案規劃建議 135
圖 24　過去與未來申請銀行貸款之差異 175
圖 25　日本資料（情報）銀行運作架構 211

本報告之智慧財產權屬於國家通訊傳播委員會

提要

電信產業作為未來數位轉型重要推手，並積極發展跨域整合應用服務。然各國電信事業皆採取高度監管模式，對於電信資料創新應用，除需遵循電信事業規範外，還應遵循現行資料保護相關法規。目前國際上對於電信資料甚至是消費者資料應用，於法制方面涉及隱私與資料合理利用權衡與跨域創新應用複雜情況下，需要考量資料流通、隱私保護與資料安全，還有市場競爭等議題。我國現有之監理沙盒機制目前仍針對金融領域，若是電信資料應用為維護國家安全或公共利益狀況下應如何應用，以及借鏡現階段國際上電信業者之實務應用。透過本計畫研析國際相關政策、案例，以及公眾意見諮詢、座談會等意見徵集，綜整提出電信事業與目的事業主管機關在資料創新應用服務、資料治理相關決策流程建議，作為主管機關擬訂相關政策之參考。

關鍵詞：電信事業、資料、創新、治理、公眾意見諮詢

本報告之智慧財產權屬於國家通訊傳播委員會

Abstract

As an important promoter of digital transformation in the future, the telecommunications industry is actively developing cross-domain integrated application services. However, the telecommunications industry is highly regulated in various countries. For the innovative application of telecommunication data, in addition to complying with the regulations of the telecommunication industry, the current data protection-related laws and regulations should also be followed. At this stage, application issues such as telecommunications data and even consumer-related information, when it comes to the situation of the trade-off between privacy and the proper use of data, also cross-domain innovative applications, need to consider data circulation, privacy protection, and security, as well as market competition issues.

Taiwan's current regulatory sandbox mechanism is aimed at the financial sector. If the application of data from telecommunications enterprises is necessary for ensuring national security or the public interest, we hope to study and analyze relevant international policy decisions, cases, public consultations, and symposiums. Through the research, we will comprehensively and put forward suggestions on the decision-making process related to innovative application services, data utilization, and governance of telecommunications enterprises and the government authority. It is also used as a reference for the competent authority to formulate relevant policies.

Keywords: telecommunications enterprise, data, innovation, governance, public consultation

本報告之智慧財產權屬於國家通訊傳播委員會

第一章 整體說明

第一節 研究緣起

面對數位轉型浪潮席捲全球，各國政府對數位經濟之重視，以及5G、物聯網（IoT）、區塊鏈（BlockChain）、大數據（big data）、人工智慧（AI）等技術之蓬勃發展，電信產業不再侷限於提供基本的電信與網路服務，而是在萬物聯網時代下，成為技術發展的核心。同時，電信產業面臨著消費者行為與需求改變，以及核心業務營收下滑，為了提供更高品質的服務，以及更好的客戶體驗，利用先前所累積大量資料進行分析，不論是客戶個人資料、服務使用情況，或是電信服務中所衍生巨量電信數據資料、商業行為資料、機器所產生資料，皆是數位轉型應用之關鍵。透過 AI 處理分析大資料，作為新產品和服務依據，改善營運並增加收入。

2021 年 1 月歐洲電信網路營運業者協會（European Telecommunications Network Operators' Association, ETNO）提出之數位通訊最新報告（The State of Digital Communications）[1]，指出歐洲在關鍵數位指標落後，如在關鍵網路部署和數位投資指標（包括 5G、AI 和網路之投資）方面大幅落後美國和亞洲，儘管歐洲大型電信業者已擴大投資，仍力有未逮。歐洲 5G 人口涵蓋率從 2019 年的 12.9%增長到 2020 年第三季的 24.4%，卻仍遠落後美國的 76%以及南韓的 93%。歐洲電信公司面對全球激烈競爭，透過 AI 技術應用擴展業務領域，如資料應用、雲端服務、資訊安全等，期能弭平創新差距。報告也發現歐洲從數位服務（例如企業解決方案、安全性等）獲得的電信收入，預計從 2017 年的 650 億歐元（約 2 兆台幣），增長到 2021 年的 1004 億歐元（約 3.2 兆台幣）。然而與其他大型科技公司的競爭壓力仍相當大，且歐盟 2020 年 12 月提出數位服務法（Digital Services Act, DSA）與數位市場法（Digital Markets Act, DMA）等草案，保護

[1] New Report: Europe behind on key digital metrics, telcos essential to achieve leadership, ETNO, https://etno.eu/news/all-news/8-news/694-state-of-digi-2021-pr.html (last visited Aug. 13, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

數位服務使用者，以及數位市場競爭規範，電信業者未來也需思考相關因應策略。

此外，Deloitte US 就 2021 年電信行業前景報告（2021 Outlook for the US Telecommunications, Media, and Entertainment Industry）[2]，說明電信產業長期面臨結構性挑戰，因應新冠肺炎（COVID-19）疫情，需要思考復甦策略，如重新關注客戶需求，融合娛樂體驗，探索直接面向消費者（direct-to-consumer）的新產品、服務；應用 5G 技術發展新產品、服務與商業模式重新定位電信服務，且報告預估 5G 將達到 7000 億美元（約為 19 兆台幣）經濟價值，68%的市場由零售、政府和金融應用主導。

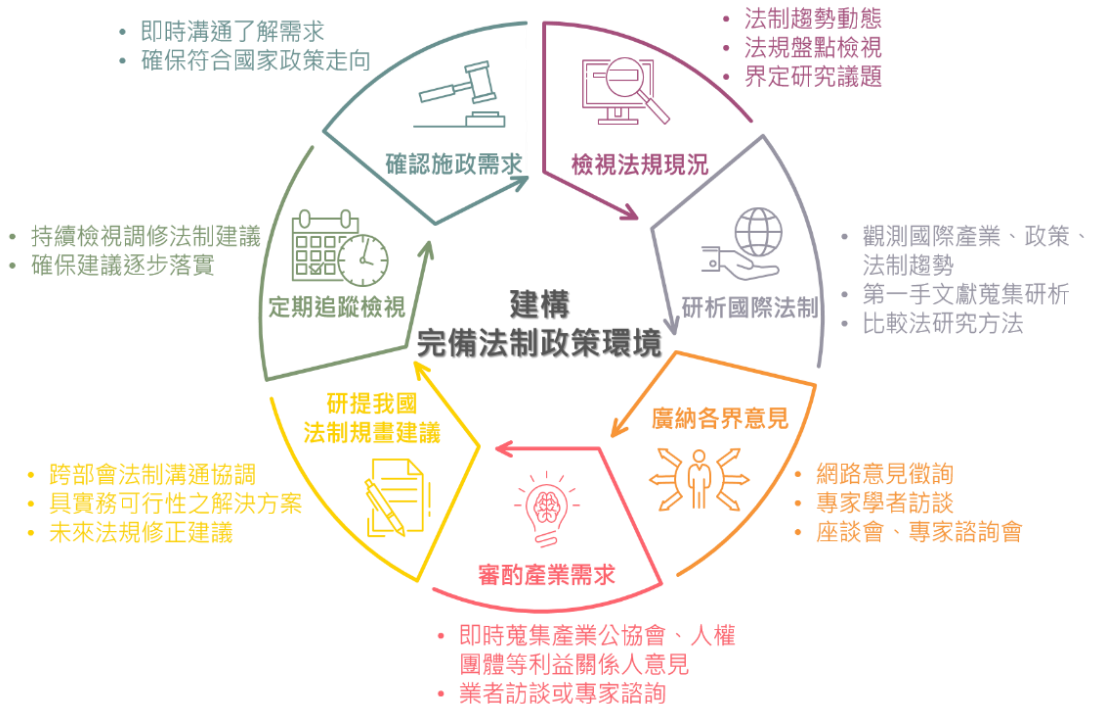
而我國電信事業跨界應用趨勢亦如火如荼進行中，針對聯合企業夥伴、跨領域合作，在智慧金融、醫療、零售、製造、倉儲、展演娛樂等，發展創新應用場景虛實整合，促成生態系逐步轉型開創 5G 新紀元。電信產業作為未來數位轉型重要推手，該產業已開始思考並著手發展跨域整合應用，然而電信事業於各國皆受到高度的監管，對於電信事業所掌握之資料進行創新應用時，除需遵循電信事業規範外，還應遵循資料保護相關法規。目前國際上對於電信數據資料，甚至是消費者資料之應用，於法制面上當涉及隱私與資料合理利用權衡與跨域創新應用複雜情況下，需要考量資料流通、隱私保護與資料安全，還有市場競爭等議題。我國現有之監理沙盒機制，目前仍針對金融領域，若是電信業者資料應用，在為維護國家安全或公共利益狀況下，冀望透過本計畫研析國際相關政策、案例，以及公眾意見諮詢、座談會等意見徵集，綜整並提出電信事業與目的事業主管機關在創新應用服務、資料運用及治理之相關決策流程之建議，作為目的事業主管機關擬訂相關政策之參考。

[2] 2021 telecommunications industry outlook, Deloitte US, https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/telecommunications-industry-outlook.html (last visited Aug. 13, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

第二節 研究方法

本計畫依循執行團隊所建立的研究方法論，進行相關研究（參圖1）。此一研究方法論主要立基於比較法之研究，其實施步驟主要為：確認需求（即研究議題）、國際相關政策、法規與措施研析、我國政策與法制現況檢視，以及透過廣納各界意見，如專家學者座談、網路意見徵詢，作為推動措施或法規調適建議依據，並提出研提相關之政策、推動措施建議。



資料來源：本計畫整理

圖1 計畫研究方法論

一、確認施政需求

計畫團隊於履約期間與通傳會密切聯繫合作確認研究範圍、方向等相關細節。於執行期間隨時配合通傳會就研究主題範圍內之諮詢，提出相關個案資料蒐集及研析建議。

二、國際相關政策、法規與措施研析

透過文獻蒐集等方式，檢視追蹤國際產業、政策或法規之趨勢，

本報告之智慧財產權屬於國家通訊傳播委員會

觀測主題主要如下：

(一)蒐集主要地區或國家之電信事業配合有關機關執行維護國家安全或公共利益時，蒐集、處理及利用電信資料，在所涉及相關隱私保護之適法性評估、參考指引等政策決策過程，透過資料研析勾畫資料創新應用服務治理模式架構。

(二)蒐集主要國家或地區之電信服務業者對其電信服務所產生之數據資料，在創新應用現況或是異業合作模式實際應用案例，研析產業在活化資料利用或運用於商業模式之治理情形。

(三)蒐集主要地區或國家之資料經濟政策發展、相關法制、規管現況、協商及決策流程或指導規範等作為，分析對於電信事業運用數據資料提供創新應用服務可能造成之影響。

(四)就蒐集、案例及法制等資料開始分析、歸納及整理出主管機關所採取的相關政策或措施及未來趨勢。

三、我國產業、政策或法規之現況檢視

透過為期 14 天網路公眾意見諮詢，還有邀集包含電信事業、利益關係人、人權團體等，進行意見交流座談會議，以蒐集我國現行法規及現行作法，與國外作法分析，預期處理的議題如下：

(一)電信事業利用其所產生之數據資料之相關數據資料種類、應用態樣、應用時可能面臨發生之問題及其解決過程。

(二)電信事業利用其所產生之數據資料，並對其資料運用、治理、保護與創新應用服務等，國內相關法令限制及挑戰、政府與企業責任、未來法規修正或決策流程。

(三)資料經濟政策於我國現行法令下，在電信領域之資料運用、加值、保護與創新應用服務之可行作法、相關法令限制及挑戰、未來法規修正等相關決策作業流程標準。

四、研提相關之政策、推動措施或法規調適建議

本於前揭之研究基礎，提出我國關於電信事業運用數據資料提供創新應用服務治理模式之建議，並提出相關具體調適建議，以作為未來政策之參考。

本報告之智慧財產權屬於國家通訊傳播委員會

採取前揭之研究方法，可以掌握委託單位之需求，能為研究方向進行設定與適時調整。其次是可以透過比較法與標竿國際經驗，作為我國推動措施研擬之參考。最後是透過文獻資料之蒐集，可以掌握國內產業所面臨之問題或政策措施之缺口，同時也可以就所研擬推動之措施廣納意見並凝聚共識，強化相關措施建議之有效性。

第三節 工作項目

國家通訊傳播委員會（下稱通傳會）委託本團隊執行「110 年度電信事業運用數據資料提供創新應用服務治理模式之研究案」（以下簡稱本案），依需求書所載，本案共計六項工作項目，分別為：

一、蒐集主要國家或地區（歐盟、美國、英國、日本、韓國等）之電信事業配合有關機關執行維護國家安全或公共利益時，針對蒐集、處理及利用電信資料，在所涉及相關隱私保護之適法性評估、參考指引等政策決策過程情形，提出研析報告。

二、蒐集主要國家或地區（歐盟、美國、英國、日本、韓國等）之電信服務業者對其電信服務所產生之資料（例如裝置及位置資訊、消費紀錄、電信紀錄、身分驗證...等），在創新應用現況上的 5 個以上不同類型（其中包括 3 項與異業合作模式）之實際應用案例，以及研析其產業在活化資料利用或運用於商業模式之治理情形，並研析當地政府對其資料經濟政策發展、相關法制、規管現況、協商及決策流程或指導規範等作為。

三、依前揭研析實際案例資料（工作項目一、二），辦理下列項目：

(一)研擬並評估實際案例可能面臨問題及建議解決方案，辦理網路公眾意見諮詢（諮詢期間以 14 天為原則），並就公眾諮詢所得意見蒐集並整理。

(二)邀集國內電信事業、合作產業、相關產業、消保及人權團體、專家學者等，進行 2 場以上之座談會實例分享及討論（包含前揭公眾意見諮詢），以瞭解電信事業已運用或有意規劃利用其所產生之數據資料，並對其資料運用、治理、保護與創

本報告之智慧財產權屬於國家通訊傳播委員會

新應用服務等情形，探討國內相關法令限制及挑戰、政府與企業責任、未來法規修正或決策流程建議等議題。

(三)彙整本項成果資料，並提出團隊之初步建議，其中至少包含應用面、法規面及治理面等研析。

四、針對前揭所蒐集資料、發展趨勢、公眾意見諮詢及座談會意見蒐集後，辦理下列項目：

(一)進行研析並提出相關成果報告、具體意見及決策流程之建議，報告內容應研析包括相關數據資料種類、應用態樣、應用時可能面臨發生之問題及其解決過程之建議內容。

(二)按前揭解決方案建議，敬邀國內電信事業、合作產業、相關產業、消保及人權團體、專家學者等，進行 1 場次以上之座談會討論其解決方案（草案）內容之可行性具體意見，提供目的事業主管機關參考。

五、提供相關諮詢服務，於履約期間，提供通傳會就研究範圍內之業務諮詢及相關資料蒐集及分析。

六、綜整並研析本案相關委託工作事項，針對資料經濟政策，檢視我國現行法令下，在電信領域之資料運用、加值、保護與創新應用服務之可行作法、相關法令限制及挑戰、未來法規修正等相關決策作業流程標準之建議，以提供我國目的事業主管機關未來政策方向參考。

期中報告內容依前揭委託辦理之工作項目一、二、三、五，完成如下：

一、完成蒐集主要國家（愛沙尼亞、美國、英國、日本、韓國等）之電信事業配合有關機關執行維護國家安全或公共利益時，針對蒐集、處理及利用電信資料，在所涉及相關隱私保護之適法性評估、參考指引等政策決策過程情形，完成研析報告。

二、完成蒐集主要國家或地區（愛沙尼亞、德國、美國、英國、日本、韓國等）之電信服務業者對其電信服務所產生之數據資料，在創新應用現況上多種類型與異業合作模式之實際應用案例共 12 例，以及研析其產業在活化資料利用或運用於商業模式之治理情

本報告之智慧財產權屬於國家通訊傳播委員會

形，並研析當地政府對其資料經濟政策發展、相關法制、規管現況、協商及決策流程或指導規範等作為。

三、依前揭研析實際案例資料，完成下列項目：

(一)110 年 7 月 19 日至 8 月 1 日完成網路公眾意見諮詢，並就公眾諮詢所得意見蒐集並整理。

(二)110 年 8 月 2 日及 8 月 4 日辦理 2 場座談會。

(三)完成本項成果資料彙整提出初步建議。

四、完成諮詢服務 3 項議題，包含向電信事業蒐集收視行為統計資料適法性研析、電信事業之定型化服務契約條款研析、電信事業提供政府合理利用個資於跨領域共享等。

期中審查會議於 110 年 10 月 6 日辦理，本團隊已依照委員意見調整報告內容。從報告形式面，團隊已整體檢視確認報告中第一次出現外語文字或簡稱時，提供完整中譯與說明，並就報告內容調整錯漏或冗字/詞，並全面檢視圖表調整使之清晰及中文化，引述外幣金額時，一併提供相應之新臺幣金額。至於從報告內容實質面來說，從特定用語之研析補充，如 LBS、廣告應用推廣、行動支付、監理沙盒、資料銀行、韓國 GEPP 平台等，並持續關注國際趨勢與相關法規、指引、措施等更新。而關於委員提到運用資料的執法機關、個資專責機關及電信監管機關之間的三方權責，主要補充說明於第二章各國關於主管機關之間權責與法規；電信事業運用資料之模式之適法性及可行性建議，亦已補充於第七章；關於已辦理完成之兩場座談會所蒐集的意見所研擬之短中長期建議，如何進行溝通及可行性驗證，已補充於報告第七章。期末報告就政府部門採取發展模式，以及關於數位發展推動與個資專責機關權責劃分，參照期中研析內容亦提出建議於第九章結論。最後於附錄 6 至附錄 13 參照委員意見擇較具參考指引翻譯整理供參考。

期末報告內容依前揭委託辦理完成所有工作項目如下：

一、完成蒐集主要國家（愛沙尼亞、美國、英國、日本、韓國等）之電信事業配合有關機關執行維護國家安全或公共利益時，針對蒐集、處理及利用電信資料，在所涉及相關隱私保護之適法性評估、

本報告之智慧財產權屬於國家通訊傳播委員會

參考指引等政策決策過程情形，完成研析報告。

二、完成蒐集主要國家或地區（愛沙尼亞、德國、美國、英國、日本、韓國等）之電信服務業者對其電信服務所產生之數據資料，在創新應用現況上多種類型與異業合作模式之實際應用案例共 12 例，以及研析其產業在活化資料利用或運用於商業模式之治理情形，並研析當地政府對其資料經濟政策發展、相關法制、規管現況、協商及決策流程或指導規範等作為。

三、依前揭研析實際案例資料，完成下列項目：

(一)110 年 7 月 19 日至 8 月 1 日完成網路公眾意見諮詢，並就公眾諮詢所得意見蒐集並整理。

(二)110 年 8 月 2 日及 8 月 4 日辦理 2 場座談會。

(三)完成本項成果資料彙整提出初步建議。

四、針對前揭所蒐集資料、發展趨勢、公眾意見諮詢及座談會意見蒐集後，辦理下列項目：

(一)完成成果報告、具體意見及決策流程之建議，包括相關數據資料種類、應用態樣、應用時可能面臨發生之問題及其解決過程之建議內容。

(二)110 年 10 月 13 日辦理 1 場座談會討論其解決方案（草案）內容之可行性具體意見，提供目的事業主管機關參考。

五、完成諮詢服務 5 項議題，包含向電信事業蒐集收視行為統計資料適法性研析、電信事業之定型化服務契約條款研析、電信事業提供政府合理利用個資於跨領域共享、異業合作涉及跨領域業務資料應用促進當事人資料自主運用、國際最新個資法趨勢研析等。

六、完成檢視我國現行法令下，在電信領域之資料運用、加值、保護與創新應用服務之可行作法、相關法令限制及挑戰、未來法規修正等相關決策作業流程標準之建議，以提供我國目的事業主管機關未來政策方向參考。

期末審查會議於 110 年 12 月 15 日辦理，團隊已依照委員意見調整，如整體檢視並修正報告缺漏字或語意不明之部分，與章節調整補充比較表如表 1 與表 2，以及將附錄 13 韓國大數據個人情報保護準

本報告之智慧財產權屬於國家通訊傳播委員會

則註明主管機關及發布年月。此外，補充關於安維辦法草案中提到之「加值應用」、「去識別化」之定義，並針對電信事業資安與個資驗證之相關國際與我國國家標準整理如表 10。還有就報告中提到電信事業參考開放銀行、「當事人動態同意」、日本資料銀行現況運等補充說明。

本報告之智慧財產權屬於國家通訊傳播委員會

第二章 電信事業配合執行維護國家安全公共利益電信資料應用研析

從 2019 年開始至今全球受到 COVID-19 疫情衝擊，各國面臨不同階段疫情考驗，為了防疫考量，疫苗施打提升群體免疫，甚至是社交距離等相關政策與措施，政府需要輔以民間資料協助決策。而面對未來疫情發展與科技演進，電信事業所保管的資料（或電信系統所產生的資料）及其應用，在以維護國家安全或公共利益為目的之若干情境下，也成為要角。國際上對於如接觸者追蹤、行動位置資料應用於防疫相關措施所涉及隱私保護議題，各國所關注資料保護之重點與適法性評估、指引等皆值得探討。因此以下就愛沙尼亞、美國、英國、日本、韓國等政策措施與相關規範進行蒐整研析。

第一節 愛沙尼亞

根據 2020 年 7 月聯合國電子化政府調查報告（UN E-Government Survey 2020）之「電子化政府發展指標」（E-Government Development Index, EGDI）評比，愛沙尼亞在 193 個聯合國會員國名列第三，該國擁有相當高的公民數位參與率，人民信賴政府數位公共服務以及資料應用，並擁有值得信賴之數位身分證系統[3]。愛沙尼亞自 2002 年開始推行數位身分證（eID），2005 年時更曾為全世界第一個使用網路投票（I-Voting）的國家，而到 2013 年已成為人均新創產業之世界之最。

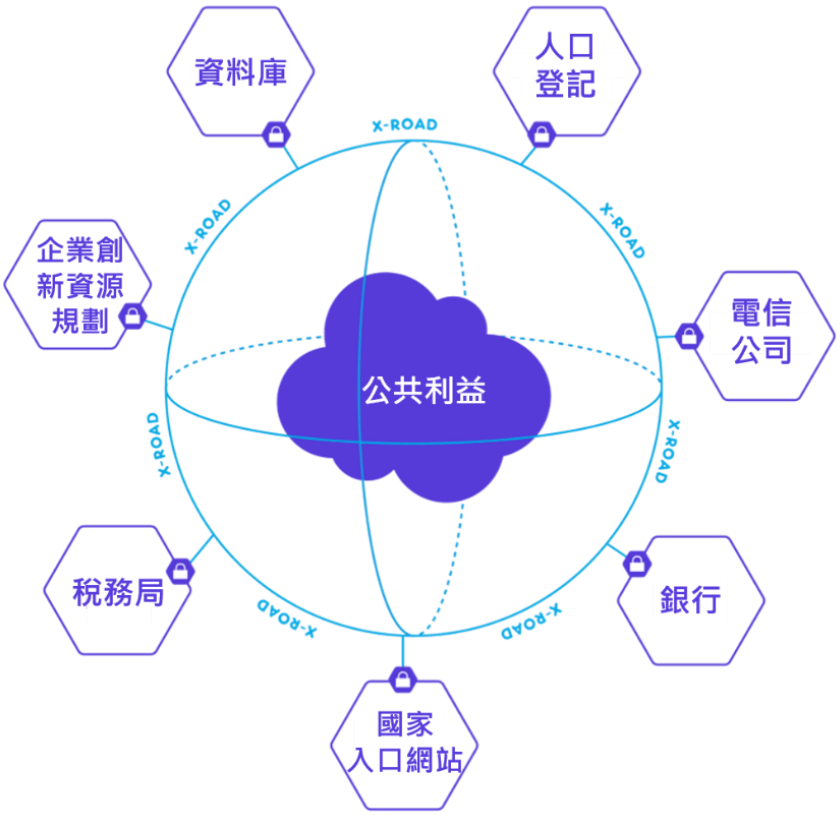
愛沙尼亞數位政府成功關鍵在於 X-tee 和數位身分。依據 2020 年愛沙尼亞數位化議程（Digital Agenda 2020 for Estonia）建構公私部門（如人口登記、稅務、銀行、電信等）資料交換架構 X-tee[4]，作為 e-Estonia 的骨幹（參圖 2）。根據該國公開資訊法（Public Information Act）規定之一次性原則禁止重複蒐集資料，若人民已向相關權責機關提供相關資料，則其他政府機關皆不得再次向人民要求提供資料。

[3] UN E-Government Survey 2020, United Nations, https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf (last visited June 20, 2021).

[4] X-tee 是愛沙尼亞使用的資料交換架構，2018 年前都是用英語命名為 X-Road。但自 2018 年之後 X-Road 僅用於指愛沙尼亞和芬蘭共同開發的技術。

本報告之智慧財產權屬於國家通訊傳播委員會

而各機關如果需要取得人民的相關資料，必須透過政府資料交換架構 X-tee 來取得。透過此系統，公私部門資訊能夠相互介接取用，且以高規格的點對點加密以及區塊鏈技術儲存資料交換紀錄，並確保資料傳輸安全且不會被任意竄改。隱私保護亦是 X-tee 的核心，藉由去中心化的政府資料結構來保障人民的隱私，使資料當事人能確實成為自己資料的最終所有者，並有效分散資安風險。另外，eesti.ee 網站[5]提供查詢存取個人資料紀錄，任何未經授權的存取可能成立刑事犯罪。



資料來源：本計畫編譯自 Information System Authority

圖2 Data Exchange Layer X-tee

愛沙尼亞身分認證機制除了 eID-card，還有 E-Residency、Mobile-ID，以及 Smart-ID。eID-card 結合健保卡、數位簽章，並得用於投票、檢查病歷資料、繳稅、登入銀行帳戶，以及歐洲旅遊證件。E-Residency

[5] eesti.ee 網站，詳參 https://www.eesti.ee/et。

本報告之智慧財產權屬於國家通訊傳播委員會

則是跨國數位身分，可以在愛沙尼亞以此身分設立公司及申請銀行帳戶進行商業活動。Mobile-ID 則是於 2007 年由愛沙尼亞電信公司提供之服務，以手機作為 eID Card。當時對於電信業者而言，Mobile-ID 可謂服務創新應用。而 Smart-ID 則是用於智慧裝置中沒有 SIM 卡，但需要以安全方式驗證身分的替代方法。

關於愛沙尼亞各項數位政府業務之管理屬於分散式管轄，由各政府部門各自管轄其權限範圍內的電子政務項目實施。而有關協調與資訊及通訊科技（Information and Communications Technology, ICT）和訊息技術的營運有關的所有基礎設施，例如政府入口網站、中間系統 X-tee、政府骨幹網路 EEBone、國家資訊管理系統（Riigi Infosüsteemi Haldussüsteem, RIHA），以及資訊系統安全監理，包含關於電信服務提供業者的資訊系統等，則是由資訊系統管理局（Information System Authority, RIA）負責。而關於電信業者則是依電子通訊法（Electronic Communications Act）規範確保服務安全性和完整性。

以上說明關於愛沙尼亞數位政府架構與相關機制，可知該國政府數位化與資料於公部門相關應用。而以下則針對愛沙尼亞政府因應疫情提出接觸者追蹤應用程式，以及要求電信業者提供匿名電信移動資料應用的實際案例說明如下。

一、 應用案例

(一) HOIA APP

愛沙尼亞於 2020 年 8 月 20 日推出由社會事務部（Sotsiaalministeerium）和民間[6]共同開發的 COVID-19 應用程式 HOIA，當接觸感染者後將會通知使用者，並強調相關資料不會被其他使用者、國家、甚至 HOIA 的開發人員辨識，且不會監控使用者位置以及透露被感染者真實身分[7]。HOIA 採用分散式隱私保護接近追蹤（Decentralized Privacy-

[6] 包括 Iglu OÜ、Cybernetica AS、Osaühing IceFire、GuardTime OÜ、Velvet DP OÜ 、Mobi Lab OÜ、Mooncascade OÜ、Fujitsu Estonia AS、FOB Solutions OÜ、HEISI IT OÜ，以及 ASA Quality Services OÜ。

[7] The Estonian coronavirus mobile APPlication HOIA is now available for download, Republic of Estonia Ministry of Social Affairs (Aug. 20, 2020), https://www.sm.ee/en/news/estonian-coronavirus-mobile-APPlication-hoia-now-available-download (last visited June 20, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

Preserving Proximity Tracing, DP-3T）的去中心的隱私保護接觸追蹤技術，為每個使用者產生一組短期匿名代碼並定期更改代碼，手機透過藍芽接收訊號，只要兩支手機接觸時間夠長就會儲存對方的匿名代碼，而當有人確診後，設備上的匿名代碼就會將資料上傳到中央伺服器，並通知相關使用者查看及下載（參圖 3）。

此應用程式將資料分為三類：密切接觸者（close contact）、感染者（infection）及行為準則（code of conduct）。所謂密切接觸是指接觸至少 15 分鐘且距離小於 2 公尺，被認定是密切接觸者後 HOIA 會發出通知，但此通知並不會告知感染者身分或是接觸的時間及地點，意即無法間接識別感染者身分，以保護個人隱私。

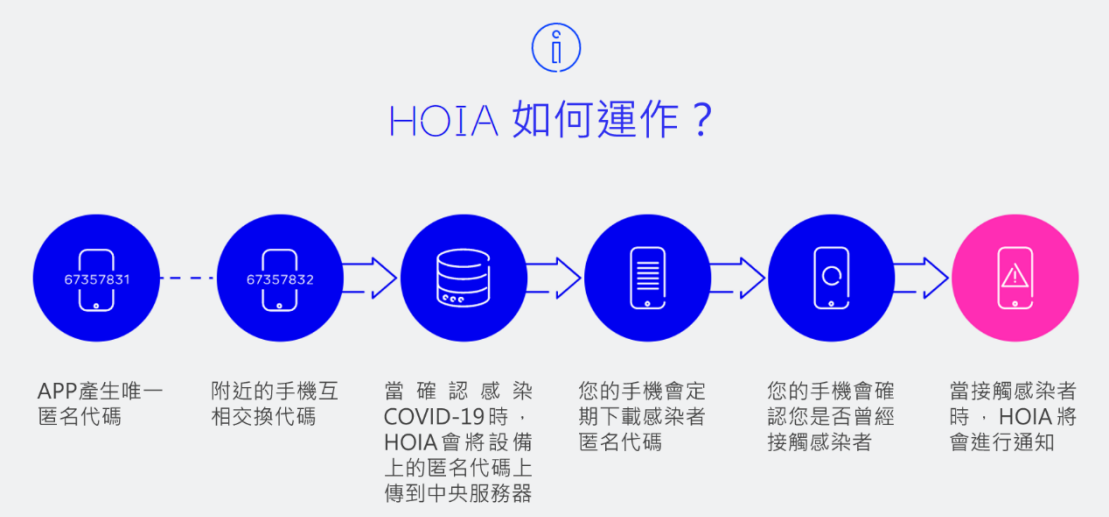
HOIA 之健康資料及資料交換系統之法律依據為衛生資料系統法（Tervise infosüsteemi põhimäärus），該法係依據醫療保健服務組織法（Tervishoiuteenuste korraldamise seadus）第 59 條第 3 項所訂定。目的在於處理與醫療保健領域相關的資料，以訂立和履行提供醫療保健服務的契約，確保醫療保健服務的品質和患者（即資料主體）的權利，保護公眾健康和維護健康登記資料、衛生統計和衛生保健管理[8]。

依衛生資料系統法第 5 條規定醫療保健服務提供者作為資料提供者，應提供有關門診醫療資料、住院資料與轉診資料，並在傳輸資料時遵守有關健康資料系統的標準規範。關於資料保存期間，根據衛生資料系統法第 8 條規定，除法律另有規定外，醫療紀錄應在衛生資料系統中保存 30 年，惟根據 HOIA 服務條款，使用者之資料僅會保存 14 天即刪除，並不會儲存在 APP 中。根據衛生資料系統法第 14 條規定，社會衛生部或其他官方管理資料分析所執行有關衛生

[8] Tervishoiuteenuste korraldamise seadus, Riigi Teataja, https://www.riigiteataja.ee/akt/118062021008?dbNotReadOnly=true#para59b1lg3 (last visited Aug. 13, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

政策、管理或統計而需近用或建立相關衛生資料系統者，該系統之資料不得識別個人資料（包括生日、國籍、個人身分、性別、教育水平或是否有健保等）、醫療保健服務提供者資料、住院醫療服務資料、醫療門診服務資料、診斷資料、描述個人健康狀況的指標資料（例如牙齒狀況、輸血反應、身高體重、懷孕與否等）、使用醫藥資料，或任何有關執行操作、分析、檢查與程序資料。因此，HOIA 無法近用該使用者手機上的任何資料，當使用者回報確診後，HOIA 會將使用者導向相關健康單位進行通報，並不會將健康資料回傳 HOIA，而政府單位亦僅在通報時得知，並無法透過 HOIA 取得使用者的感染情況或與他人的聯繫狀況[9]。HOIA 唯一目的在於通知使用者當其與確診者接觸時，做出即時因應措施，以斷絕病毒傳播。資料主體得依衛生資料系統法第 16 條規定近用應用程式所蒐集的個人資料並查閱之，並根據衛生資料系統法第 19 條資料主體有權拒絕醫療保健服務提供者近用其資料。



資料來源：本計畫編譯自 HOIA- protect yourself and your clostest ones

圖3 HOIA 運作方式

[9] HOIA-protect yourself and your clostest ones, https://hoia.me/en/ (last visited June 20, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

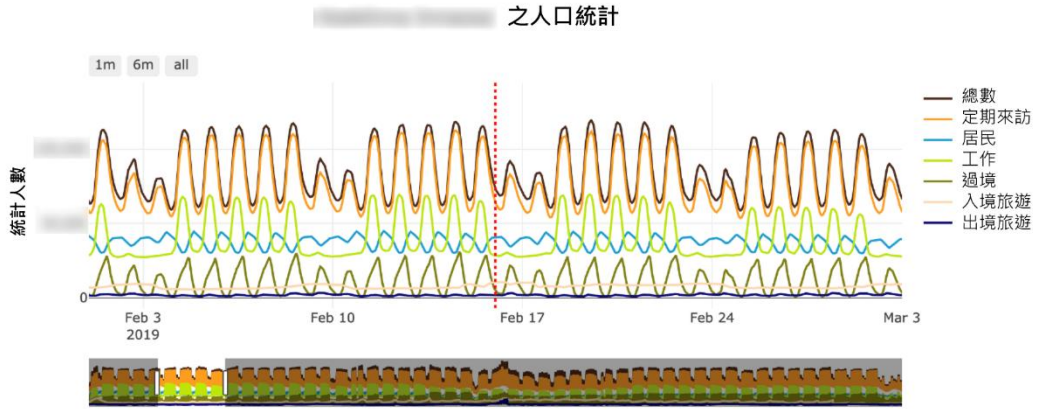
(二) 行動定位資料（mobile positioning data, MPD）

愛沙尼亞政府為掌握因政治、經濟、個人職業變化、自然災害或旅遊等原因導致的人口流動及遷徙模式，透過行動定位資料（mobile positioning data, MPD）評估相關因素所造成人口移動。近兩年來因 COVID-19 大流行，政府則是希望藉由手機位置資料之應用，預測及避免病毒傳播加劇。

此外，愛沙尼亞於地理位置上會遭受到季節性暴風雨及暴風雪等自然災害，而網路空間亦常受到資安攻擊，對於該國經濟影響皆相當重大。因此愛沙尼亞救援委員會（Estonian Rescue Board）和塔圖（Tartu）大學合作，由愛沙尼亞資料分析公司 Positium 建立 MPD 系統，以即時追蹤行動電話位置來統計移動定位資料[10]，透過視覺化顯示時常出現在同一個地區的人數和類型（在該地區居住、工作或經常路過的人、國內遊客、外國遊客等）；不同區域之間移動的方向和次數；於災難疏散之情況下，在該地區擁有第二居所的人數，以及第二居所與原來所在空間的距離；以及每日、每周和季節性交易量變化和移動模式等（參圖 4），準確地評估各區域風險，並預測危機發生前的疏散需求，更妥適地進行資源規劃以及預測危機期間的人口移動行為[11]。

[10] Rein Ahas1, Margus Tiru, Erki Saluveer, Christophe Demunter, Mobile telephones and mobile positioning data as source for statistics: Estonian experiences, at 4.
[11] Building resilience through mobile positioning data in Estonia and Indonesia, Positium (July 12, 2021), https://positium.com/blog/resilience-mobile-phone-data-estonia-indonesia (last visited Aug. 4, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會



資料來源：本計畫編譯自 Positium

圖4 PMD 實時顯示人口移動變化

為掌握人口流動以追蹤 COVID-19 傳播方向，愛沙尼亞統計局與 Positium 合作，依據歐盟第 223/2009 號規則(EC regulation 223/2009)關於統計資料授權之法律規定，賦予歐盟成員國之統計機關各自行政系統內近用所有行政紀錄之權利，自 2020 年 2 月起要求電信業者特利亞（Telia）[12]、Tele2[13]和 Elisa[14]提供匿名之電信移動資料，透過 MPD 系統分析出人口流動變化。結果顯示，愛沙尼亞的人們每天平均在其主要活動地點，例如家中停留 20 小時，每天平均行駛的距離也從 27.5 公里減少到 17.6 公里，且除了愛沙尼亞國民外，也可以分析在愛沙尼亞停留的旅客資料，並分析旅客來自的國家[15]。透過位置統計資料精確且快速的方式評估人口流動性。

[12] 為瑞典電話公司和行動網路營運商、前身是國營的瑞典電報局及芬蘭電訊（Sonera），主要服務於瑞典、芬蘭、挪威、丹麥、立陶宛、拉脫維亞和愛沙尼亞。

[13] 成立於 1993 年，總部位於瑞典斯德哥爾摩希斯塔，是北歐和波羅的海周邊國家的主要電信服務供應商之一。

[14] Elisa 電信(芬蘭語：Elisa Oyj)為芬蘭電信公司，成立於 1882 年。原稱赫爾辛基電話(Helsingin Puhelin，至 2000 年 7 月）及 Elisa 通信公司（Elisa Communication Oyj，至 2003 年）。Elisa 經營電信、ICT 和在線服務，業務範圍主要在芬蘭和愛沙尼亞。

[15] COVID-19 Mobility Analysis of Statistics Estonia: Collaborating with mobile network providers during an emergency situation, measuring human mobility under social distancing measurements, MIGRATION DATA PORTAL (Apr. 28, 2021), https://www.migrationdataportal.org/data-innovation/covid-19-mobility-analysis-statistics-estonia-collaborating-mobile-network (last visited Aug. 27, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

二、 愛沙尼亞電子治理法制規劃

愛沙尼亞一直是國際推動電子治理之典範，其擁有被世界銀行稱為全球最成功的數位身分證系統，並且成為聯合國評比下公民數位參與率最高的國家。愛沙尼亞政府結合公私部門，研發數位化服務，例如電子健保、電子處方箋、線上開辦銀行帳戶，試圖讓 eID 融入民眾日常生活，目前已有 99%的政府服務數位化，並有 70%的民眾透過 eID 來取得政府服務，而其成功的關鍵在於與時俱進的規範框架。愛沙尼亞認為發展電子治理不需針對特定領域建立全面性立法體系[16]，理由在於法規修訂往往難以與技術發展俱進，應針對資料敏感性等重要議題，在保持技術中立性的情況下，透過分析現行法並找出差異，以及法律可能對電子治理發展造成障礙的領域，逐步檢視調修，並建議在規劃過程中應諮詢法律專家，及早進行法律風險分析，避免監管障礙，同時政策應避免過度監管。

為促進電子通訊網路及服務的發展及保障電子通訊使用者之權利，在 2004 年 8 月通過電子通訊法，確保通訊服務提供商的多元化，以及所提供服務之安全性和完整性[17]。針對電信資料之資料保護，電子通訊法第 102 條規定電信業者對於通訊服務過程中所產生的所有資料皆應該保密。電信業者有權處理使用者之位置資料，但應依同法第 105 條之規定對使用者身分進行匿名處理，除非在取得使用者同意之情況下，才能於必要範圍與期限內以未匿名的方式處理資料或提供服務，並且給予使用者拒絕將資料提供給第三方業者之權利。對於利用電信資料行銷之情形，第 103 條規定電信業者應通知使用者用於行銷之目的及使用期限並取得使用者同意，而後向其提供資料使用狀況之詳細說明。如果政府認為為了公共秩序或國家安全等公共利益之目的而有必要時，允許政府將此類資料的保留期限延長甚至永久保存[18]。

針對資訊系統中資料交換層的使用與維護規範，即對 X-tee 建立安全與可驗證之網路資訊交換技術的基礎架構與環境。愛沙尼亞制定

[16] Digital Government Factsheet 2019, European Commission, at 20.
[17] Electronic Communications Act, art. 40.
[18] Electronic Communications Act, art. 111.

本報告之智慧財產權屬於國家通訊傳播委員會

資料交換層法（Data Exchange Layer Act），其中包括對 X-tee 之管理應具備平台與結構之獨立性、多邊性、開放性與標準化，以及安全性；加入 X-tee 之資格條件；並須確保資料交換之安全及標準化要件，以建立安全的資料交換管道及確保電子簽章資料交換的完整性[19]。

愛沙尼亞除了既有的電子化政府措施之外，更大範圍布建免費網路提升寬頻速度，以及打造政府部門間的資料交換網，讓政府內部先數位化。再者，去中心化的政府資料結構除了保障人民隱私外同時分散資安風險，當各項資料散見在各個不同的行政機關，駭客想取得個人完整資料，則必須駭入各機關方能完整拼湊。愛沙尼亞政府開放民眾得上網查閱相關文件，透過個人資料監測系統（Personal Data Usage Monitor）以開放原始碼的方式，讓人民得以監督政府，並掌握自己的資料在何時被何機關以何理由使用。而當民眾認為資料被不當利用時，亦可向資料保護監管機關（Data Protection Inspectorate, DPI）進行申訴。最後，除了成熟的技術外，更有相應的完整法律架構，配合政府之相關數位政策。透過公開透明的機制和監督政府的獨立機關，以提高人民之數位素養及對政府之信任。

第二節 美國

美國目前尚無聯邦層級統一的隱私與資料保護法規，而是散見於聯邦法或州法中。聯邦層級法規例如健康保險可攜與責任法（Health Insurance Portability and Accountability Act, HIPAA），規範醫療機構對健康資料之使用；通訊法（Communications Act）則是規範電信營運商對客戶資料之使用；以及聯邦貿易委員會法（Federal Trade Commission Act, FTC Act）禁止公司從事欺騙性或不公平的資料保護等措施。而州法層級如加州政府於 2020 年 1 月開始施行之加州消費者隱私保護法（California Consumer Privacy Act, CCPA）為美國各州首部一般性之個人資料保護法，賦予加州消費者新的隱私權，包括調取資料權（right to request information）、刪除權（right of deletion）、

[19] Infosüsteemide andmevahetuskiht, Riigi Teataja, https://www.riigiteataja.ee/akt/106082019017 (last visited June 20, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

退出權（right to Opt-Out）、反歧視權（right to non-discrimination）等。而後，加州更於2020年11月3日通過加州隱私權法（California Privacy Rights Act, CPRA），作為CCPA之附錄，旨在加強加州民眾的權利，限制關於使用個人資料的商業法規，建立新的保護規範。

在美國隱私保護規範框架下，可知該國對於資料保護雖尚無聯邦層級規範，但各州政府陸續展開立法。而美國社群媒體平台、電子商務公司不僅掌握美國消費者資料甚至是全世界使用者資料，美國人民對於隱私保護意識相當高，至於該國電信事業配合政府維護在公共利益前提下對於當事人位置資料追蹤，以及遠距醫療服務案例，分別說明如下。

一、 應用案例：位置資料追蹤

美國四大電信業者之一的AT&T於2018年6月遭揭露與美國國家安全局（National Security Agency, NSA）有密切合作。AT&T在美國境內設立多個網路節點[20]，提供 NSA 查詢或攔截經過相關節點的資料權限，包括網路通訊、電話、簡訊等個人隱私內容[21]。2019年1月 Motherboard 報導稱 AT&T、Sprint、Verizon 和 T-Mobile 向第三方業者出售用戶的即時位置資料[22]，雖然 AT&T 宣稱第三方業者違反公司政策，但 AT&T 銷售位置資料合法性仍有疑義。歷經美國聯邦通訊委員會（Federal Communications Commission, FCC）兩年的調查，認為四家電信業者都涉及把使用者位置資料出售給資料蒐集公司，而資料蒐集公司再把相關資料存取權出售給第三方且未獲得使用者之明確同意，故於2020年1月裁罰上述四家電信業者，總金額超過2億美元（約為55億台幣）[23]。

[20] 此節點分布在芝加哥、達拉斯、亞特蘭大、洛杉磯、紐約市、舊金山、西雅圖和華盛頓特區等八個主要城市。

[21] Taylor Hatmaker, AT&T collaborates on NSA spying through a web of secretive buildings in the US, TechCrunch (June 26, 2018), https://techcrunch.com/2018/06/25/nsa-att-intercept-surveillance/；Ryan Gallagher, Henrik Moltke, The Wiretap Rooms: The NSA's Hidden Spy Hubs in Eight U.S. Cities, The Intercept (June 25, 2018), https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/ (last visited June 20, 2021).

[22] Joseph Cox, I Gave a Bounty Hunter $300. Then He Located Our Phone, VICE (Jan. 9, 2019), https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile (last visited Aug. 6, 2021).

[23] FCC Proposes Over $200M in Fines for Wireless Location Data Violations, Federal

本報告之智慧財產權屬於國家通訊傳播委員會

此外，美國對於公共衛生與個人隱私之間的衡平長期以來處於緊張狀態，認為位置資料與健康資料可能會被惡意取得或用於政府監控。然而，突如其來的 COVID-19 大流行使得各國不得不加速思考科技應用與個人隱私、資料保護之間的關係。COVID-19 傳染速度驚人，因此需要進行接觸者追溯（contact tracing）。根據 2020 年調查，美國需要有 80%的智慧型手機用戶（約總人口的 56%），配合使用接觸追蹤應用程式，方能有效控制疫情。惟經民意調查約僅有 50%至 60%的美國民眾願意使用接觸追蹤應用程式，且僅 29%的民眾願意共享位置資料[24]。

美國電信法（Telecommunications Act of 1996）第 222 條規定，電信業者有義務保護關於消費者資訊的隱私，且依據無線通訊及公共安全法（Wireless Comminications and Public Safety Act）電信業者公開或使他人知悉用戶位置資訊前須經其同意，而美國無線通訊產業貿易協會（Cellular Telecommunications & Internet Association, CTIA）公佈之行動定位服務（location-based services, LBS）開發部署指南[25、26]，認為位置資料若在未經授權或使用者不知情的情況下被濫用或洩露，將會對使用者隱私造成重大威脅，故指南明確定義 LBS 價值鏈中（value chain）各角色（例如應用程式創建者/提供者、位置資料蒐集者、提供網路位置資料之營運者等）所需遵守之義務：

(一)LBS 提供者必須確保使用者收到有關如何使用、揭露和保護位置資料的有意義的通知，以便使用者可以自由做出是否使用 LBS 之

Communications Commission (Feb. 28, 2020), https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations (last visited Aug. 26, 2021).

[24] Kavya Sekar and Laurie A. Harris, Contact Tracing for COVID-19: Domestic Policy Issues, CRS In Focus IF11609, Aug. 3, 2020.

[25] Best Practices and Guidelines for Location Based Services, CTIA, https://www.ctia.org/the-wireless-industry/industry-commitments/best-practices-and-guidelines-for-location-based-services (last visited Aug. 26, 2021).

[26] 我國近期之 LBS 應用案例為口罩地圖以及防疫之人流管制，由公部門帶頭整合跨業者、跨平台的數據，結合 LBS 系統彙整，以達到疫情掌控與風險地區分級之效果。另外，交通部觀光局也在 2021 年 1 月 20 於台灣觀光資訊網新增 LBS 功能，當民眾到達旅遊地點時，透過手機網路連線瀏覽台灣觀光資訊網，即可自動定位其所在位置，並結合 Google Maps 地圖服務，提供最佳路線規劃及即時導航功能。同時，本項功能介接中央氣象局、環保署及公共運輸平台（PTX）資訊，即時提供如天氣/空氣品質、周邊交通場站、景點、活動、旅遊服務中心等周邊旅遊資訊。惟，我國目前針對 LBS 應用似暫無相關法規限制，針對如何在蒐集數據時不致侵犯個人隱私之議題，相關廠商與主管機關亦應提早進行規劃，以避免踩到紅線。

本報告之智慧財產權屬於國家通訊傳播委員會

決定。

(二)LBS 提供者必須確保使用者同意使用或揭露其位置資料，並且 LBS 提供者應承擔證明此類同意的責任，且使用者必須有權隨時撤銷同意或終止使用 LBS。

指南分別針對「通知」、「同意」與「保護措施」為具體說明如下：

(一)通知：LBS 提供者必須確保潛在使用者了解其的位置資料將如何使用、揭露和保護措施，以便使其能夠自行判斷是否使用之決定。指南未規定通知的形式、位置或方式，得以書面、電子形式或口頭告知，僅需以淺顯易懂之說明使其充分了解 LBS 之運作方式。若在取得同意後利用目的增加或變更，則必須重新通知使用者並使其知悉新的利用目的，且須告知其資料保存期間。如 LBS 提供者將提供資料給第三方，則必須揭露提供何種資料及提供給何第三方業者，讓使用者能了解可能帶來哪些風險。最後，應具使用者能自由選擇是否揭露其位置資料之隱私控制選項。

(二)同意：同意的形式可能因服務類型或其他情況而有差異，故不限定同意之形式或使用之方式。若是實際使用者與帳號使用者不同時（例如父母為帳號持有人，為兒童申辦手機），帳號持有人可以控制是否接受 LBS，但仍應確保已向每個使用者通知其正在使用位置資料追蹤。且應設有撤回同意之選項，使用者有權在任何時候中止或限制 LBS 的使用。

(三)保護措施：LBS 提供者以物理方式或技術保護措施避免使用者之位置資料被未經授權的近用、更改、破壞、使用或揭露，並保護使用者位置資料的安全性、完整性和隱私。關於資料保存僅在業務需要時保留，不使用之後應進行銷毀。若需長期使用的資料應使之聚合或匿名。應定期提供資料使用報告，避免資料濫用，並遵守其他有關使用或揭露位置資料之相關規範。

二、 美國開放政府相關法規

前述已整理關於美國資料保護規範，目前尚未有聯邦個資保護法，然而於開放資料方面，美國總統歐巴馬於 2009 年上任當日即簽

本報告之智慧財產權屬於國家通訊傳播委員會

署「透明與開放政府備忘錄」（Transparency and Open Government Memorandum），以「政府開放資料」（Open Government Data）為原則推動政府資料加值與創新應用，並在相關配套公布後，各機關逐漸發展出使用者參與及釋出資料程序。而為使政府運作更加透明，讓民眾得近用政府資料以進行參與及合作，針對政府所蒐集之資料，應依資訊自由法之規定，行政機關有向人民要求提供行政資訊的義務，人民亦可向行政機關請求取得行政資訊之權利。

2013 年 5 月歐巴馬再發布一項備忘錄[27]，呼籲所有政府機構應使用創新技術簡化服務，以降低成本、減化服務等待時間，並改善客戶體驗。為響應此備忘錄，聯邦資訊長（Chief Information Officer, CIO）發布「數位政府：建構 21 世紀更好的服務平台」（Digital Government: Building a 21st Century Platform to Better Serve the American People）[28]，目的是使一般人民和政府行政人員均能在任何設備上獲得所需要之政府資訊和服務。惟美國並沒有針對個人資料保護的專法，而是因應時代變化和領域採取個別式立法，屬於特定部門（sector-based）的保護模式。

資訊自由法（Freedom of Information Act）確立美國隱私權之概念，並使現有之聯邦政府資料向大眾公開，保障人民可以請求行政機關取得公開行政資料的權利，規範行政機關向人民要求提供行政資訊的義務。該法於 1966 年頒布，並於 1967 年 7 月 4 日生效，除了國家安全資訊、單純機關內部人事規範或運作有關資訊、機關內部意見溝通、其他依法不得公開資訊、商業機密、個人隱私、執法資訊、金融機構資訊及油井資訊等九項政府資料排除本法適用不須揭露之外，其他資料任何人皆有權向聯邦機構請求近用該紀錄。

而後為因應資訊科技（Information Technology, IT）產業發展，於 1974 年制定隱私法（Privacy Act of 1974），立法目的在於政府應在維

[27] Timothy Vollmer, Obama issues Executive Order in support of open data, Creative Commons (May 10, 2013), https://creativecommons.org/2013/05/10/obama-issues-executive-order-in-support-of-open-data/ (last visited Aug.6, 2021).

[28] Digital Government: Building a 21st Century Platform to Better Serve the American People, Digital Government, https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html (last visited Aug. 6, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

護個人資料與保護個人權利之間取得平衡，以防止個人資料於蒐集、處理、利用之過程中受到不必要的侵犯。隱私法規範之重點在於：(1)限制機構揭露其所保存之個人身分記錄;(2)給予個人更多近用其保留在行政機關之個人資料的權利；(3)給予個人修改其不正確、不完整或過時之資料；(4)制定公平資訊實施原則（Fair Information Practice Principles），要求機關遵守蒐集、處理、利用相關記錄的法定規範。然而，並非所有之資料均受到隱私法之保護，針對中央情報局（Central Intelligence Agency）保存的所有記錄，以及犯罪紀錄等資料不受隱私法之保護。另外，有關國防或外交之相關政策資料；出於執法目的之相關調查資料；為維護資料完整性或基於特定目的而有需要揭露時；總統或其他受特勤局保護之相關資料;法律規定應保留或留作統計之用之資料；軍事相關資料；公務人員考試或任用之資料等，亦不在隱私法保護範圍之內。

美國的開放資料源自於開放政府，透過開放政府資料來達到施政透明化並提升行政效能。而通訊主管機關 FCC 並未實際投入推動通訊傳播產業開放資料的作為，僅配合政府推動其智慧城市資料應用計畫[29]。從法制面觀察，美國的個人資料保護並無統一適用的專法，而是依照各個領域分門別類制定相關個資保護規範。而在 COVID-19 疫情的推波助瀾下，政府重新思考使用電信資料來評估人員流動所帶來的效益。此外，參酌聯合國統計委員會（UN Statistical Commission）2013 年提出的官方統計基本原則（Fundamental Principles of Official Statistics）第 6 條強調國家統計機關應將個人資料保護與資料共享視為首要任務，考量資料隱私及安全問題、資料取得成本、資料供應連續性，並分析使用資料的技術能力。而資料應用形式則取決於各國與電信業者的合作模式及國家監管框架。

通訊法（Communications Act）限制電信業者對用戶專有網路資訊（customer proprietary network information, CPNI）之使用，包括電

[29] The White House, Fact Sheet: The White House Launches "The Opportunity Project," Utilizing Open Data to Build Stronger Ladders of Opportunity for All (Mar. 7, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/03/07/fact-sheet-white-house-launches-opportunity-project-utilizing-open-data (last visited Aug. 6, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

信營運商的任何客戶訂閱的電信服務數量、技術配置、類型、目的地、位置和使用量等相關資料。即電信營運商不得向第三方揭露客戶的CPNI，或在未經客戶同意之情況下讓第三方近用客戶 CPNI，僅在需協助提供緊急服務以應對緊急情況時，才能向資料庫管理服務提供商揭露。惟針對 COVID-19 防疫資料之使用，美國法院雖針對 CPNI 是否包含手機之地理定位資料做出定義，但 FCC 認為，即使手機定位屬於 CPNI，但接觸式追蹤資料屬於緊急服務，而接觸式追蹤應用程式屬於訊息或資料庫管理服務提供者，此類揭露屬於例外範圍[30]。

第三節 英國

面臨 COVID-19 疫情衝擊與國際情勢發展，資料應用對於公私部門甚至個人都是決策關鍵依據。英國政府期望能釋放資料的力量，以負責任態度進行資料共享應用，以建構開放安全的資料環境，並促進創新與發展改善人民生活。2020 年英國政府提出國家資料戰略（National Data Strategy）[31]，制定政府在資料方面採取的行動框架，促進企業、政府、公民社會和個人之間能夠更好地應用資料。同時因應脫離歐盟後，為了能持續發揮對於全球資料經濟之影響力，以及因應 COVID-19 疫情之資料跨域應用合作。以下就英國政府因應疫情相關措施，為維護公共利益時所蒐集、處理及利用資料所關注重點進行研析。

一、 應用案例：NHS COVID-19 APP

2020 年 5 月英國衛生及社會關懷部（Department of Health and Social Care, DHSC）發表國家健康服務（National Health Service, NHS）COVID-19 應用程式（NHS COVID-19 APP），由英國國家醫療服務體系數位創新部門 NHSX 開發[32]，提供英國民眾確認是否與 COVID-19

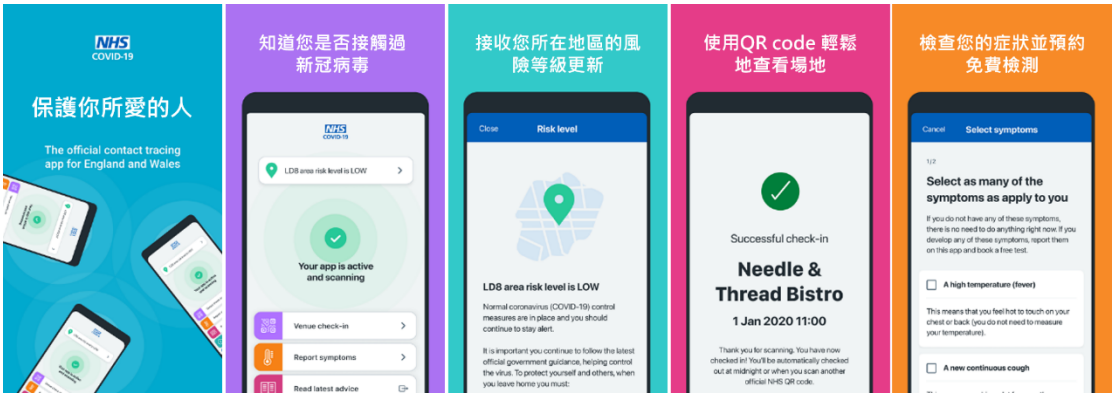
[30] Digital Contact Tracing and Data Protection Law, Congressional Research Service (Sep. 24, 2020), at 10.

[31] Department for Digital, Culture, Media & Sport, National Data Strategy, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy (last visited June 20, 2021).

[32] 開發團隊來自 Accenture、Alan Turing 研究所、NHS Digital、NHSx、牛津大學、VMware Pivotal Lab 和 Zuhlke Engineering，也有國家網路安全中心（National Cyber Security Centre）協助關於資

本報告之智慧財產權屬於國家通訊傳播委員會

陽性病患接觸風險的方式。該 APP 功能包含追蹤接觸風險、所在區域警報通知、場所登記、症狀說明與檢測、檢測試劑訂購、自我隔離倒數與相關建議（參圖 5）。該 APP 協助 NHS 了解病毒是否正在特定地區傳播，以利於地方政府可以迅速反應，阻止病毒傳播。



資料來源：本計畫編譯自 NHS COVID-19

圖5 NHS COVID-19 簡介與功能

該 APP 對於使用者身分之保護，對於使用者的位置或身分相關資料採取匿名化處理。而 APP 運作原理則是透過使用者開啟手機藍芽，與接觸過的其他使用者交換隨機產生的加密代碼，確定使用者是否曾與感染者距離 2 公尺且相處超過 15 分鐘，APP 即發送警報，代碼也會在 14 天後刪除。可能涉及個資為使用者提供郵遞區號，一旦所在區域變成高風險區，便會收到 APP 警報[33]。

然而該 APP 的開發與版本更新的過程，仍伴隨著隱私保護和資料安全問題[34]。初期 APP 開發人員承認即使 APP 對使用者身分進行匿名化處理，但仍可能重新識別當事人，以及先前並未進行資料保護影響評估[35]。英國民間團體建議政府應提供一個強有力的法律框架確保資料安全，並建立監督機制確認資料之使用以及確保資料安全相關

安技術諮詢。

[33] NHS, COVID-19 APP support, https://www.covid19.nhs.uk/ (last visited June 20, 2021).

[34] The Use of Digital Measures to Combat COVID-19, Northern Ireland Assembly, at 15, http://www.niassembly.gov.uk/assembly-business/committees/2017-2022/health/research-papers-2020/the-use-of-digital-measures-to-combat-covid-19/ (last visited June 18, 2021).

[35] 目前皆已完成 NHS COVID-19 隱私聲明和隱私保護影響評估，詳參 https://www.gov.uk/government/publications/nhs-covid-19-APP-privacy-information (last visited June 20, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

措施，並要求英國政府以日落條款模式說明是否會在疫情結束後銷毀資料。此外，還存在數位落差問題，英國有近 700 萬人使用過網路，但只有非常基本的技能，可能不知道如何使用應用程式。此外，關於互操作性，歐盟執委會強調採用單一模式開發應用程式的重要性，以確保未來疫情趨緩後歐盟境內開放，各國使用者不同接觸者追蹤應用程仍能有效應用[36]。

該 APP 隱私聲明[37]提到應遵循英國一般資料保護條例（UK General Data Protection Regulation, UK GDPR）[38]與 2018 年資料保護法（Data Protection Act 2018, DPA 2018）[39]規定之目的進行資料處理：

(一)UK GDPR 第 6(1)(e)條：資料處理為履行其在提供和管理醫療服務的公共利益而執行的任務所必需。

(二)UK GDPR 第 9(2)(g)條：基於 DPA 2018 附表 1 第 2 部分（第 6 段法定和政府目的）規定的重大公共利益，必須進行資料的處理。

(三)UK GDPR 第 9(2)(h)條：醫療診斷、提供治療以及管理健康和社會保健系統需要進行資料的處理。

(四)UK GDPR 第 9(2)(i)條：基於公共衛生領域的公共利益原因，必須進行資料的處理。

(五)DPA 2018 附表 1 第 1 部分第 2 節(2)(f)：醫療保健系統或服務的管理。

(六)DPA 2018 附表 1 第 1 部分第 3 節：公共衛生目的。

根據 UK GDPR 第 22 條，該 APP 並未使用自動化決策（automated decision-making, ADM），但已遵守自動決策制定的法律和政策框架，並依據 UK GDPR 規範關於資料留存與當事人權利。

---

[36] *Supra* note 34, at 16.

[37] NHS COVID-19 APP: privacy notice, Department of Health & Social Care, https://www.gov.uk/government/publications/nhs-covid-19-APP-privacy-information/nhs-covid-19-APP-privacy-notice (last visited June 20, 2021).

[38] The UK GDPR, ICO, https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/ (last visited June 20, 2021).

[39] Data Protection Act 2018, https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (last visited June 20, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

二、 政府因應 COVID-19 疫情於電信行動位置資料之分析

除了開發前述應用程式外，英國政府和衛生機關也透過分析電信公司提供的大量行動位置資料，了解 COVID-19 大流行期間人們移動和行為模式，以預測病毒可能傳播模式以及公共衛生措施的有效性，如社交距離，以分配檢驗與醫療量能。至於政府因公共利益向電信公司要求提供資料，可能涉及隱私保護議題需要探討，儘管電信公司會強調其所提供的任何資料都是去識別化、群集資料（aggregate data），並非即時且不涉及個人[40]，亦即無法識別個人的群集、去識別化之位置資料並非個人資料，因此不適用歐盟一般資料保護規範（General Data Protection Regulation, GDPR）。

然而歐洲資料保護監督機關（European Data Protection Supervisorm, EDPS）認為雖然去識別化資料不屬於資料保護範圍，但有效的去識別化不僅僅是刪除電話號碼等個資，必須是與第三方共享的任何資料都需要完全匿名，以確保無法追溯到個人而重新識別。若透過第三方分析匿名資料，必須確保該第三方符合嚴格資訊安全要求和保密義務，得近用該類資料應僅限於流行病學、資料保護和資料科學領域專家[41]。至於英國如何應用位置資料來追蹤社交距離措施執行情況，以倫敦為例，兩家主要電信公司 O2 和 EE 向政府提供群集位置資料，政府最初使用這些資料觀察疫情封鎖期間公眾活動的趨勢，評估是否需要提供額外服務或必要執法。而兩家公司皆強調他們提供的任何資料都是匿名群集資料，不會提供任何可識別當事人之個人資料[42]。

英國政府還表示支持使用其他形式的大數據，如 Google 關於疫情移動報告（COVID-19 mobility report）。透過與科技公司合作，尋找創新方法來阻止冠狀病毒的傳播。此外，2020 年 3 月 NHS 與 NHSX 合作建立 Covid-19 資料儲存（NHS COVID-19 Data Store）[43]，讓政府

[40] *Supra* note 34, at 20-21.
[41] *Supra* note 34, at 22-23.
[42] *Supra* note 34, at 26-27.
[43] NHS COVID-19 Data Store, NHS, https://www.england.nhs.uk/contact-us/privacy-notice/how-we-use-your-information/covid-19-response/nhs-covid-19-data-store/ (last visited July 29, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

得以應用資料在疫情下提供確保公眾安全之因應措施，如查詢醫院的床位容量，或特定區域可用的呼吸器數量等。然而該 Data Store 的資料來源包含大量與個人相關的資料，如 COVID-19 檢測結果、民眾撥打 NHS 健康諮詢熱線的內容，以及重症監護患者的臨床資訊等，但在上傳前都會經驗證並去識別化。雖然這些敏感特種個資已去識別化，但集中儲存於政府資料庫，初期仍引起隱私專家的質疑[44]。因此，2021 年衛生和社會保健大臣（Secretary of State for Health and Social Care）依據 2002 年健康服務（與病患資料管理）法（The Health Service (Control of Patient Information) Regulations, COPI）第 3 條(4)向 NHS England & Improvement 發布通知[45]，要求其應依規定方式處理病患機密資訊，並用於 COPI 第 3 條(1)規定之目的，並與當前的 COVID-19 疫情相關，並應完成資料保護影響評估[46]。該通知從 2021 年 9 月 30 日延長至 2022 年 3 月 31 日。

從 COVID-19 疫情爆發至今，政府應用科技數位措施，如開發接觸者追蹤應用程式和大數據分析評估流動模式。然而面對疫情衝擊帶來更多的挑戰，在立法和政策面不僅需要具有彈性，面對人民所關注之隱私和資料安全問題亦不容忽視。透過接觸者追蹤應用程式，為了能夠達成阻斷傳播鏈之目的，充分發揮應用程式效力，需要得到公眾接受和信任，因此資料儲存和使用應完全透明，以及歐盟重視後續疫情舒緩進而開放跨境移動時，應用程式間的互操作性更是關鍵。

至於政府使用電信公司提供之群集匿名位置資料來評估資源分配，以及社交距離措施，理論上由於資料集是匿名群集，而對於資料隱私威脅並不大。然而仍有重新識別個人風險存在，並且當前的去識別化技術，尚不足以個人提供完全隱私保護，且數位落差也可能造成

---

44 *Supra* note 34, at 27.

45 Coronavirus (COVID-19): notice under regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002 – NHSE, NHSI, https://www.gov.uk/government/publications/coronavirus-covid-19-notification-of-data-controllers-to-share-information/coronavirus-covid-19-notice-under-regulation-34-of-the-health-service-control-of-patient-information-regulations-2002-nhse-nhsi (last visited Nov. 12, 2021).
新通知將從 2021 年 9 月 30 日延長至 2022 年 3 月 31 日。

46 Data Protection Impact Assessment: NHS COVID-19 Data Store, NHS, https://www.england.nhs.uk/publication/data-protection-impact-assessment-nhs-covid-19-data-store/ (last visited July 29, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

沒有智慧手機的人被邊緣化，進而影響公共政策準確性。數位技術發展不僅加快政府應對 COVID-19 的能力，在運用這些解決方案時，也需要面對並突破技術帶來重大的倫理和技術挑戰。

三、 CMA、ICO、Ofcom、FCA 成立 DRCF

英國競爭及市場管理局（Competition and Markets Authority, CMA）、英國資訊專員辦公室（Information Commissioner's Office，ICO）和 Ofcom 於 2020 年 7 月共同成立英國數位監管合作論壇（Digital Regulation Cooperation Forum, DRCF），英國金融行為監理局（Financial Conduct Authority, FCA）則是於 2021 年 4 月加入（先前為觀察員）[47]。該論壇旨在確保線上監管事項各主管機關之橫向溝通與協調合作，並於 2021 年 3 月發布 2021/2022 年度工作計畫（Digital Regulation Cooperation Forum workplan 2021/22）[48]，包含三大重點工作：因應產業和技術發展啟動聯合專案、發展資料保護與競爭等議題之聯合監管方法、跨部會的監管制度，以及共享技能和專業知識，透過成立跨監理機構的專家團隊，與數位市場其他監理機構密切合作。

DRCF 於 2021 年 5 月 4 日回應英國文化媒體暨體育部（Department for Culture, Media and Sport, DCMS）關於數位監管格局的未來以及如何實現監管一致性的方法（Digital Regulation Cooperation Forum: Embedding coherence and cooperation in the fabric of digital regulators）[49]。DRCF 認為為了持續有效推動監管一致性，建議政府支持數位監管機關在以下領域合作，包含適當的資訊共享；在數位服務的法制框架中規範關於一致性與合作，如促進消費者、資料主體和公民的利益、諮詢職責與合作義務等；以及透明度和問責制。

此外，2021 年 5 月 19 日 CMA 與 ICO 共同發布關於競爭和資料

[47] The Digital Regulation Cooperation Forum, Competition and Markets Authority, https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum (last visited Nov. 8, 2021).

[48] Digital Regulation Cooperation Forum workplan 2021/22, Competition and Markets Authority, https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122 (last visited Nov. 8, 2021).

[49] Digital Regulation Cooperation Forum: embedding coherence and cooperation in the fabric of digital regulators, Competition and Markets Authority, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/982898/DRCF_response_to_DCMS__PDF.pdf (last visited Nov. 8, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

保護法的聯合聲明（Competition and data protection in digital markets: a joint statement between the CMA and the ICO）[50]，闡述 CMA 與 ICO 對競爭目標和資料保護之間關係的共識，聲明提到資料在數位經濟中發揮的重要作用，亦即更具競爭性的市場將提供消費者更好的服務，其中也包含增強隱私技術和更好地控制個人資料。而競爭目標和資料保護之間是相輔相成的，透過嚴謹法規和標準可以保護個人隱私，並使個人控制其個資，同時能促進積極的競爭結果。反之，透過適當和具針對性的監管，可以利用競爭壓力激勵保護和支持負責任創新（responsible innovation）。因此，營造公平的競爭環境是促進有效競爭蓬勃發展的基礎，而資料保護法則是確保各方對個資處理是公平合法並維護個人權利，同時有助於在資料近用方面實現公平競爭。CMA 與 ICO 期望透過合作一致和適當地適用競爭和資料保護法，以克服競爭和資料保護之間的緊張關係。而該聲明也提到此議題具有全球意義，因此也將持續與國際相關主管機關與組織接觸建立共識，並促進全球監管的一致性和協作。

第四節 日本

根據日本的「科學技術基本法」（科学技術・イノベーション基本法），政府應制定以五年為一期之「振興科學技術與創新創造之基本計畫」（簡稱為科學技術基本計畫），明確訂定日本振興科學技術推動之長期目標[51]。而 2016 年制定之第五期科學技術基本計畫[52]（2016 年至 2020 年）提出「超智慧社會」（Society 5.0），係指透過高度融合網路虛擬空間及實體空間，同步解決經濟發展與社會議題，以建立「以人為中心」之社會[53]。而 5G 係為實現 Society 5.0 不可或缺之下一世

[50] CMA-ICO joint statement on competition and data protection law, Competition and Markets Authority, https://www.gov.uk/government/publications/cma-ico-joint-statement-on-competition-and-data-protection-law (last visited Nov. 8, 2021).

51〈科学技術・イノベーション基本法・科学技術・イノベーション創出の活性化に関する法律〉，內閣府，https://www8.cao.go.jp/cstp/cst/kihonhou/mokuji.html（最後瀏覽日：2021/08/11）。

[52]〈第 5 期科学技術・イノベーション基本計画（2016）〉，內閣府，https://www8.cao.go.jp/cstp/kihonkeikaku/index5.html（最後瀏覽日：2021/08/11）。

[53] 〈Society 5.0〉，內閣府，https://www8.cao.go.jp/cstp/society5_0/（最後瀏覽日：2021/08/11）。

本報告之智慧財產權屬於國家通訊傳播委員會

代通訊技術，政府除了推動普及 5G 服務，亦將支援通訊業者設置 5G 基地台，並與通訊業者之 5G 服務同時並進，推動 5G 區域專網[54]。

2021 年制定之第六期科學技術基本計畫（2021 年至 2025 年）[55]，則探討了因 COVID-19 疫情擴大而加速國內外情勢變化，並檢討過去科學創新政策，延續推動實現 Society 5.0 之科學技術與創新政策。透過融合網路虛擬空間及實體空間創造新價值，推動 5G 普及並研發 Beyond 5G[56]。此外，2021 年 6 月日本資料專案小組（データ戦略タスクフォース）發布「總體資料戰略」（包括的データ戦略）[57]，以及日本總務省 2021 年發布「資訊通訊白皮書」（情報通信白書），與第六期科學技術基本計畫方向一致，持續以 Society 5.0 為目標，完善數位社會支柱之 5G 基礎建設，與整備促進資料活用之環境[58]。

一、 應用案例

以下介紹日本電信業者透過資料加值、維護國家安全或公共利益之相關應用案例。

(一) 新冠肺炎密切接觸者應用程式（COCOA）與感染者資料管理系統（HER-SYS）

2020 年 COVID-19 於全球大流行，為了控制疫情減少病毒擴散，應使人民掌握與確診者間之接觸狀況，因此不少國家皆推出密切接觸者查詢之應用程式。日本厚生勞動省 2020 年 6 月推出「新冠肺炎密切接觸者應用程式」（新型コロナウイルス接触確認アプリ，簡稱 COCOA）（COVID-19

[54]〈【第 6 回】「Society 5.0」実現に必要不可欠な次世代通信技術「5G」のここがすごい！〉，株式会社日立システムズ，https://www.hitachi-systems.com/report/specialist/society5/06/index.html（最後瀏覽日：2021/08/11）。

[55]〈第 6 期科学技術・イノベーション基本計画〉，內閣府，https://www8.cao.go.jp/cstp/kihonkeikaku/index6.html（最後瀏覽日：2021/08/11）。

[56]〈第 6 期科学技術・イノベーション基本計画〉，內閣府，頁 22-23，https://www8.cao.go.jp/cstp/kihonkeikaku/6honbun.pdf（最後瀏覽日：2021/08/11）。

[57] 〈包括的データ戦略〉，高度情報通信ネットワーク社会推進戦略本部，2021/06/18，頁 6，https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20210618/siryou3.pdf（最後瀏覽日：2021/08/11）。

[58]〈令和 3 年版情報通信白書〉，総務省，2020/03，頁 121，https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf（最後瀏覽日：2021/08/11）。

本報告之智慧財產權屬於國家通訊傳播委員會

COntact COnfirming application），該 APP 藉由藍芽無線通訊技術，記錄用戶間的接觸狀況，若曾與 COVID-19 確診者相距 1 公尺的距離內密切接觸超過 15 分鐘即會收到通知，以利被通知者得及早就醫或自我隔離。該 APP 為了保護使用者隱私，並不會蒐集任何可識別資料，如使用者姓名、出身年月日、地址、電話等，對於使用者之接觸訊息加密處理，而被通知者也不會獲得任何有關確診者之身分資訊，所有紀錄亦僅會保留 14 天[59]（參圖 6）。



資料來源：本計畫編譯自 COCOA

圖6 COCOA 使用說明

當確診者要在 COCOA 進行確診登錄時，係由「新冠肺炎感染者資料管理系統」(新型コロナウイルス感染者等情

[59]〈新型コロナウイルス接触確認アプリ（COCOA) COVID-19 Contact-Confirming APPlication），厚生労働省，https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/cocoa_00138.html（最後瀏覽日：2021/08/11）。

本報告之智慧財產權屬於國家通訊傳播委員會

報把握・管理支援システム，簡稱 HER-SYS）[60]，發送登錄時需要使用到的「確診處理號碼」。而確診者需要輸入發病日或檢查日，並向 COCOA 發送約前後兩日（可能的感染期間內）所生成的每日更換密鑰[61]，以通知在感染可能期間內與確診者接觸之 APP 使用者[62]。

而厚生勞動省制定「接觸者應用程式使用規則」（接触確認アプリケーション利用規約）[63]，該規則列出禁止事項[64]與應遵守事項[65]。此外，由於藍芽技術上的限制，厚生勞動省對於接觸距離和時間均不保證其正確性[66]。使用者可隨時刪除與停止使用該 APP，且若刪除則所有記錄資料也將全部刪除無法復原[67]。此外，厚生勞動省亦制定「接觸確認應用程式隱私保護方針」（接触確認アプリケーションプライ

[60]〈新型コロナウイルス感染者等情報把握・管理支援システム(HER-SYS)〉，厚生労働省，https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000121431_00129.html#oldjimren（最後瀏覽日：2021/08/11）。

[61] 係指與該終端具有一對一之對應關係，在已安裝應用程式之終端中以 24 小時為單位變更的識別碼。

[62]〈接触確認アプリケーションプライバシーポリシー〉，厚生労働省，2020 年 12 月 15 日　プライバシーポリシー改定のお知らせ，https://www.mhlw.go.jp/cocoa/privacypolicy_japanese.html（最後瀏覽日：2021/08/12）。

[63]〈接触確認アプリケーション利用規約〉，厚生労働省，https://www.mhlw.go.jp/cocoa/kiyaku_japanese.html（最後瀏覽日：2021/08/11）。

[64] 接触確認アプリケーション利用規約第 8 条第 1 項與第 2 項：「使用者於使用該應用程式時，應不得為以下行為：(1)將該應用程式應用於原本目的之外之其他目的；(2)違法訪問行為、對該應用程式服務器與網絡系統造成危害之行為、不正當操作的行為，有意鑽漏洞之行為；(3)反覆提問行為，對服務提供方提出不正當要求的行為、對於服務提供方合理管理和營運該應用程式以及第三方正常使用該應用程式造成妨害或構成阻礙的其他行為；(4)故意對該應用程式傳輸感染病毒、惡意軟體等行為；(5)違反或可能違反法律法規和公序良俗的行為、為反社會勢力輸送利益等協助行為、偽裝成服務提供方或第三方的行為、故意散布虛假資料的行為；(6)不正當蒐集、開示或提供第三方的個人資料、使用資料等行為；(7)其他厚生勞動省判斷對該應用程式合理營運造成或可能造成阻礙之行為。若使用者進行或有可能進行禁止行為，厚生勞動省可以不經事先通知，直接停止使用者對該應用程式之使用權。」

[65] 接触確認アプリケーション利用規約第 8 条第 1 項與第 3 項：「使用者在使用該應用程式之過程中，應遵守以下事項：(1)盡量只將該應用程式安裝在最常用的一部手機中；(2)不將已安裝應用程式之終端交給第三方進行管理；(3)在應用程式有更新版本，並且使用者可下載時，應下載最新版本；(4)如將已安裝應用程式的終端轉讓、借出、因發生繼承將終端給予第三方，或丟棄該終端，均應提前刪除本該應用程式。」

[66] 接触確認アプリケーション利用規約第 10 条第 2 項：「因該應用程式之終端間之距離測定會受藍芽信號強度的影響，設計時並未考慮到藍芽信號是否會穿過障礙物，測定值也會因安裝應用程式之終端性能、手持方向等條件和狀態的影響而產生偏差，因此該應用程式所測量到的接觸距離和時間均不保證其正確性。」

[67] 接触確認アプリケーション利用規約第 11 条。

本報告之智慧財產權屬於國家通訊傳播委員會

バシーポリシー）[68]，說明厚生勞動省藉由該 APP 會蒐集[69]與不會蒐集[70]的資料。而就該 APP 使用之相關同意，可以藉由刪除該 APP 而撤回同意。若撤回同意，則該 APP 相關資料也會刪除無法復原。此外，APP 不會透過程式外之系統去確認國家或地方自治團體所管理之可識別特定個人之訊息，並識別 APP 使用者之身分，亦不會向第三方提供資訊。

(二) KDDI 人口動態分析預測系統

日本大型電信公司 KDDI 與其綜合研究所於 2018 年 4 月開發了「人口動態分析預測系統」（人口動態分析/予測システム），該系統透過活用位置資料之大數據，作為移動方式與推斷路徑等行動分析之基礎，得即時預測出任意選定區域之人口分布、移動人數、停留人數、鐵路與道路之移動人數等詳細資料[71]（參圖 7）。

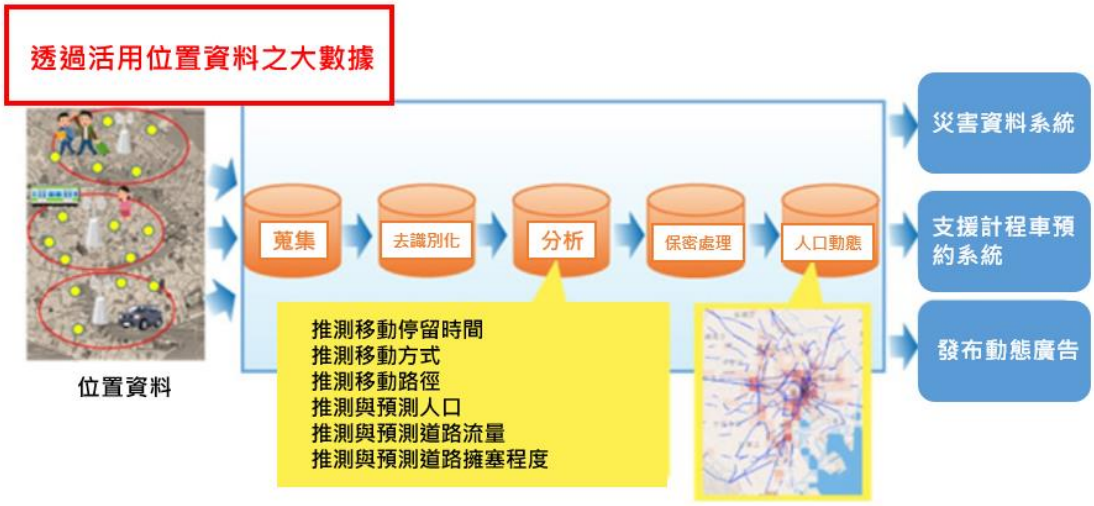
[68] 同前註 62。

[69] 厚生勞動省會蒐集之訊息：「厚生勞動省僅會透過該應用程式獲取感染者之確診處理號碼、每日更換密鑰、為改善該應用程式所需之程式運作資料（包含該應用程式所處理之內容、處理時間、處理是否成功、處理過程中所參考之資料、處理結果之輸出資料、處理狀態）以及該應用程式運作環境之資料（包含該應用程式的版本、何種作業系統、作業系統的版本、設備型號機種等）。」

[70] 厚生勞動省不會蒐集之訊息：「厚生勞動省不會透過本應用程式蒐集使用者之姓名、出生年月日、性別、住址、電話號碼、郵箱地址、終端位置資料等可識別應用程式使用者個人身分之資料，與可識別安裝應用程式之個別終端資訊。」

[71]〈人の流れを予測し可視化する「人口動態分析/予測」技術を開発〉，KDDI 株式会社，2018/04/24，https://news.kddi.com/kddi/corporate/newsrelease/2018/04/24/3095.html（最後瀏覽日：2021/08/14）。

本報告之智慧財產權屬於國家通訊傳播委員會



資料來源：本計畫編譯自 KDDI 人口動態分析預測系統

圖7 KDDI 人口動態分析預測系統

KDDI 公司為保護個人資料制定「個人資料隱私政策」（プライバシーポリシー）以遵循相關法律[72]與指引[73]。依該個人資料隱私政策規範之具體事項包含：

1. 以適當且公正之方式處理所獲得之資料[74]
2. 在遵守使用範圍前提下[75]，KDDI 公司與其關係公司，得相互使用所持有之資料
3. 若已達到利用目的，或未達利用目的但該目的業務終止，即應刪除所保留之個人資料，惟 KDDI 公司於契約終止後，仍得於利用目的範圍內利用個人資料

[72] 係指電信通訊事業法（電気通信事業法）、個人資料保護法（個人情報の保護に関する法律）、My number 法（行政手続における特定の個人を識別するための番号の利用等に関する法律）等，與其他該社業務進行相關之法律。

[73] 係指個人資料保護法指引（通則篇、確認紀錄義務篇、向外國第三方提供篇、匿名加工資料處理篇）、(電信通訊事業個人資料保護指引等，與其他該社業務相關之指引。

[74] 具體包含：(1)由客戶所提供之書面、Web，與口頭資料；(2)客戶在使用服務過程中所產生之 Cookie、Web beacon，與廣告用之識別碼等資料；(3)自公共機關獲得之資料；(4)由電話簿、官報，與各種已公布之資料中所獲得之資料；(5)自日本信用資訊機構（如 JICC）；(6)其他因客戶介紹等，自第三方合法獲得之資料。

[75] 因以下原因獲得之資料：(1)客戶同意(2)依法令(3)為保護本人生命、身體或財產之情形，而取得本人同意有困難之時(4)為提升公共利益或維護兒童身心健全發展，而取得當事人同意有困難時(5)協助國家機關或地方公共團體或受其委託者執行法令所規定之事務，基於取得本人同意有可能對執行該事務造成阻礙的之虞時。以及在各事業領域，為達成其服務與業務之使用目的必要範圍內所利用資料，係屬得在 KDDI 公司與其關係公司間相互使用之資料。

本報告之智慧財產權屬於國家通訊傳播委員會

4. KDDI 公司於變更前之目的具關聯、合理性之情況下得變更利用目的，惟需將變更目的通知本人並公布
5. 匿名加工資料必須採取無法識別出特定個人，以及無法復原個人資料之必要措施
6. 向外國第三方提供資料時應遵循法令，並取得同意等必要措施
7. 對個人資料管理應實施適當安全管理措施[76]
8. 提供不希望收到廣告訊息之用戶，取消收受訊息之申請管道
9. 在客戶本人與其代理人之要求揭露、更正，或要求利用目的之通知下，須即時做出應對措施
10. 對個人資料之相關諮詢，須適當且迅速地做出應對措施[77]

(三) KDDI 支援國家與自治團體對於災害因應之資料系統

2018 年 4 月 KDDI 公司、應用地質公司（応用地質株式会社）與豐田汽車公司（トヨタ自動車株式会社），以 IoT 與大數據分析之最新技術對「支援國家與自治團體災害因應之資料系統」（国・自治体向け災害対策情報支援システム）進行檢討，並於 2019 年將該系統商業化[78]。

此系統整合 KDDI 公司之人口動態資料[79]、應用地質公司之各種災害監測感應資料[80]，以及豐田汽車公司透過互聯汽車（Connected cars）獲得之浮動車輛資料（Floating car

[76] 遵循相關法令、指引以及訊安全管理制度（ISMS）實施適當之技術保護措施，與組織保護措施。

[77]〈プライバシーポリシー〉，KDDI 株式会社，https://www.kddi.com/corporate/kddi/public/privacy/（最後瀏覽日：2021/08/15）。

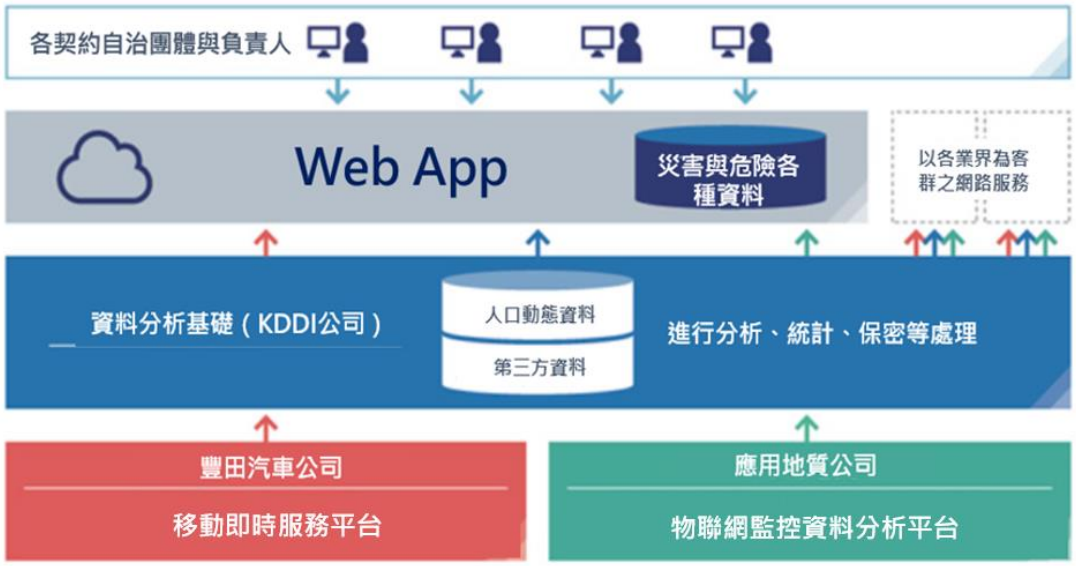
[78]〈KDDI、応用地質、トヨタ、IoT で防災・減災を実現するデータ協業に合意〉，KDDI 株式会社，2018/04/24，https://news.kddi.com/kddi/corporate/newsrelease/2018/04/24/3094.html（最後瀏覽日：2021/08/14）。

[79] KDDI 公司將使用手機位置資料之大數據，與人口動態分析預測系統之技術，對人口動態與各種 IoT 感測資料進行綜合分析。此資料得運用於災害發生時對避難場所之人口分布等進行分析，與向避難場所進行物資運送等。

[80] 應用地質公司將活用過去參與國家、自治團體與各種研究機關之防災減災諮詢實績與經驗，設置對自然災害等得隨時進行監視之各種感測器，已向本系統提供監測資料。

本報告之智慧財產權屬於國家通訊傳播委員會

data）[81]、氣象資料等開放資料，以產生各種防災資訊。藉由此系統讓地方自治團體掌握可通行之道路、即時網羅災害資訊，與整備日常基礎設施之監測體制，提高避難通知與通行管制等警戒避難措施之精準度與速度，確保當地居民安全生活[82]（參圖 8）。



資料來源：本計畫編譯自 KDDI

圖8 KDDI 支援國家與自治團體對於災害因應之資料系統

KDDI 公司在個人資料保護方面，遵循相關法律[83]與指引[84]，以及透過制定個人資料隱私政策[85]，詳參前述關於人口動態分析預測系統應用案例之相關說明。

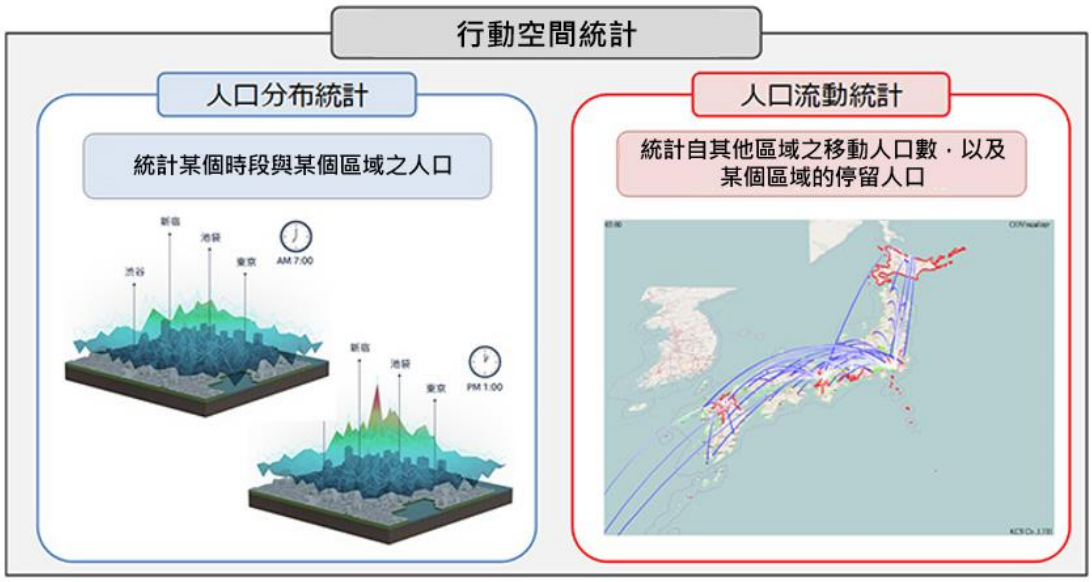
(四) NTT Docomo 人口流動統計服務

2018 年 6 月日本電信業者 NTT Docomo 公司（株式会社 NTT ドコモ）、國土交通省國土技術政策總合研究所（国土交通省国土技術政策総合研究所），與東京大學空間資訊科學研究中心（東京大学空間情報科学研究センター），共

[81] 豐田汽車公司會將自「行動運輸服務平台」（モビリティサービス・プラットフォーム）獲得之交通探測資訊、外部氣溫等統計資訊，提供給本系統。
[82] 同前註 78。
[83] 同前註 72。
[84] 同前註 73。
[85] 同前註 77。

本報告之智慧財產權屬於國家通訊傳播委員會

同研究開發「人口流動統計服務」(人口流動統計)。此服務係以 NTT Docomo 公司之行動電話網路資料為基礎，進行人口分布統計，具體應用「行動空間統計」(モバイル空間統計)[86]，以支援防災、觀光等領域，與進行社會與產業調查之分析。此外，為了調查人流與移動方式，則運用通訊技術與大數據統計處理，開發交通大數據，並藉由在服務範圍內切換基地台之行動電話統計數據分析，對日本全國用戶的移動路線、距離、速度、移動方式等資料做出推測。此統計服務所獲得之資料，可貢獻運用於新都市交通計畫、交通網網絡形成，與增設商業設施與人氣景點規劃等[87](參圖 9)。



資料來源：本計畫編譯自 NTT Docomo 人口流動統計服務網站資

圖9 行動空間統計說明

NTT Docomo 公司在個人資料保護方面，訂定「個人資料憲章」(パーソナルデータ憲章)，以宣示促進資料流通及創造創新同時為客戶提供最適當之隱私保護[88]。該憲章之具

[86] 人口流動統計服務與行動空間統計，係藉 NTT Docomo 公司對客戶於提供行動電話服務過程中，所蒐集之位置資料、特徵資料、運行資料（Operation data）等必要資料，進行統計處理，所獲得之人口推算數值，是一種不會特定客戶個人身分之統計資料。

[87] 〈(お知らせ) 国内最大規模の交通ビッグデータ「人口流動統計」を開発-ドコモ、国総研、東京大学による産官学共同開発-〉，株式会社 NTT ドコモ，2018/06/04，https://www.nttdocomo.co.jp/info/news_release/2018/06/04_00.html（最後瀏覽日：2021/08/14）。

[88] 〈NTT ドコモ パーソナルデータ憲章 -イノベーション創出に向けた行動原則-〉，株式会社

本報告之智慧財產權屬於國家通訊傳播委員會

體行動原則包含：

1. 確保個人資料處理之透明性
2. 思考顧客本身的利益與對社會的回饋
3. 尊重每位客戶意願
4. 與合作夥伴配合時也需考慮顧客的隱私權
5. 採取適切的資訊安全對策保護顧客個人資料
6. 整頓並運用保護顧客隱私權的體制[89]

NTT Docomo 公司依據上開憲章內容，制定「個人資料隱私政策」(プライバシーポリシー)，明定對個人資料保護之處理將嚴守國內外之法律與指引，此外亦將建立必要適當之安全管理、監督體制及措施，並整備公司內規則、實施必要教育訓練。若須告知個人資料進行之共同利用與匿名加工，均會隨時揭露，讓客戶得安心享受服務[90]。

而此案例中所使用之行動空間統計，僅係對群體人數進行人口統計，並不會識別特定客戶之身分[91]。NTT Docomo 公司為保護客戶之隱私，特別制定行動空間統計指引，依此指引行動空間統計時使用之運行資料（Operation data）[92]需

NTT ドコモ，https://www.nttdocomo.co.jp/utility/personal_data/charter/?icid=CRP_UTI_privacy_to_CRP_UTI_personal_data_charter（最後瀏覽日：2021/08/15）。

[89]〈(お知らせ）ドコモのパーソナルデータの取り扱いについて-パーソナルデータ憲章の公表、およびプライバシーポリシーをよりわかりやすく再編-〉，株式会社 NTT ドコモ，2019/08/27，https://www.nttdocomo.co.jp/info/news_release/2019/08/27_00.html（最後瀏覽日：2021/08/15）。

[90]〈NTT ドコモ プライバシーポリシー〉，株式会社 NTT ドコモ，https://www.nttdocomo.co.jp/utility/privacy/?icid=CRP_common_footer_to_CRP_UTI_privacy（最後瀏覽日：2021/08/15）。

[91]〈モバイル空間統計に関する情報〉，株式会社 NTT ドコモ，https://www.nttdocomo.co.jp/corporate/disclosure/mobile_spatial_statistics/index.html（最後瀏覽日：2021/08/15）。

[92] 提供電信通訊服務之過程中會產生之資料總稱，包含標示行動電話位置之位置資料，客戶簽訂契約時所提供之特徵資料等。

本報告之智慧財產權屬於國家通訊傳播委員會

經過去識別化處理[93]，統計處理[94]，以及隱匿處理[95]等三個處理階段。而簽訂提供行動空間統計資料之契約時，須明定利用目的，若欲將資料公開或再提供須遵循契約要求。此外，NTT Docomo 公司適當監督行動空間統計業務之相關職員與受委託處理者，以及因應客戶申請停止利用運行資料之程序[96]。

二、 相關法規

隨著日本高度資通訊社會發展，個人資料被廣泛運用，日本於2003 年制定個人資料保護法（個人情報の保護に関する法律）[97]，明定適當使用個人資料之基本方針及保護個人資料之措施，明確國家與地方自治團體及業者應遵守之責任義務，以及通訊業者使用個人資料皆受到個人資料保護法之規範。

而日本個人資料保護主管機關為個人資料保護委員會（個人情報保護委員会），作為內閣府外局，係具備高度獨立性之行政委員會組織，將負責制定保護個人資料之基本政策，並對運用資料之各行政機關、地方公共團體與民間業者進行監督。而日本之電信通訊事業係由總務省（総務省）進行推動，總務省促進電信通訊事業服務多元化發展之際，亦須維護電信通訊消費者權益。此外，日本於 2021 年 9 月正式成立數位廳（デジタル庁）推動數位發展，數位廳作為資料主管機關，將活用資料創造新價值，個人資料保護委員亦將對數位廳是否適當運用資料進行監督。

而為了使業者得適當處理個人資料，日本個人資料保護委員會制

---

[93] 行動空間統計在蒐集行動電話提供服務所必要之資料時，並不會使用到如電話號碼等可以識別個人之資料。此外，會對生年月日等進行年齡層的轉換，以進行資料的歸納，此種處理方式係屬去識別化處理。

[94] 依行動電話使用者之性別、年齡等不同特徵，計算行動電話之數量，再將 NTT Docomo 公司行動手機之普及率一起列入考量，推算出包含 NTT Docomo 公司客戶以外之人口，此種處理方式為統計處理。

[95] 去除人數極端少數之區域數值，此種處理方式為隱匿處理，以防止統計上之少數，被推測出個人身分。

[96]〈モバイル空間統計ガイドライン〉，株式会社 NTT ドコモ，https://www.nttdocomo.co.jp/corporate/disclosure/mobile_spatial_statistics/guideline/（最後瀏覽日：2021/08/15）。

[97] 個人情報の保護に関する法律，法律第五十七號（平成十五年˙五˙三十）（2003 年）。

本報告之智慧財產權屬於國家通訊傳播委員會

定「個人資料保護法指引」（個人情報の保護に関する法律についてのガイドライン），總務省則制定「電信通訊事業個人資料保護指引」（電気通信事業における個人情報保護に関するガイドライン），以下將針對上開規範處理個人資料與保護隱私之規定為介紹。

(一) 個人資料保護法

作為國家、地方自治團體與企業須遵循之個人資料保護共通規範，個人資料保護法於第四章至第七章規範個人資料利用之民間業者，處理個人資料時應盡之義務與罰則。

1. 個人資料之使用目的

個人資料處理業者應盡可能明確個人資料之使用目的。在變更使用目的時，必須與變更前的利用目的有相關性，且不得超過合理的範圍[98]。

2. 個人資料之取得

個人資料處理業者不得透過欺騙或其他不正當手段獲取個人資料，就敏感性特種個人資料，除獲得本人同意，或有下列情形之一者，不在此限：(1)依法令；(2)為保護本人生命、身體或財產之情形，而取得本人同意有困難時；(3)為提升公共利益或維護兒童身心健全發展，而取得當事人同意有困難時；(4)協助國家機關或地方公共團體或受其委託者執行法令所規定之事務，基於取得本人同意有可能對執行該事務造成阻礙之虞時[99]。

3. 個人資料之提供

個人資料處理業者不得擅自將資料提供予第三人，除獲得本人同意，或有下列情形之一者，不在此限：(1)依法令；(2)為保護本人生命、身體或財產之情形，而取得本人同意有困難之時；(3)為提升公共利益或維護兒童身心健全發展，而取得當事人同意有困難時；(4)協助國家機

[98] 個人情報の保護に関する法律第 15 条。
[99] 個人情報の保護に関する法律第 17 条。

本報告之智慧財產權屬於國家通訊傳播委員會

關或地方公共團體或受其委託者執行法令所規定之事務，基於取得本人同意有可能對執行該事務造成阻礙的之虞時[100]。

而業者將資料提供予第三人時應作成相關紀錄[101]，於接受來自第三人之資料時亦應進行確認[102]。為因應跨境資料傳輸之趨勢，該法於第 24 條規範向外國[103]之第三方[104]提供資料之限制，亦即當個人資料處理業者向位於外國之第三方提供個人資料，應事先取得當事人同意，有下列情形之一者，不在此限：(1)依法令；(2)為保護本人生命、身體或財產之情形，而取得本人同意有困難之時；(3)為提升公共利益或維護兒童身心健全發展，而取得當事人同意有困難時；(4)協助國家機關或地方公共團體或受其委託者執行法令所規定之事務，基於取得本人同意有可能對執行該事務造成阻礙的之虞時[105]。

4. 個人資料之管理與監督

個人資料處理業者為避免個人資料洩漏、滅失、毀損，須訂定適當之安全管理措施[106]。並應對處理個人資料之從業人員進行必要且適當的監督[107]。

5. 匿名加工資料之處理

匿名加工資料係指加工刪除個人資訊之一部分，或刪除全部之個人識別符號，所獲得無法識別特定個人之個人資料[108]。

---

100 個人情報の保護に関する法律第 23 条。

101 個人情報の保護に関する法律第 25 条。

102 個人情報の保護に関する法律第 26 条。

103 係指日本境外之國家或地區。依個人資料保護委員會規則所規定，在保護個人權益上，被認為具有與日本相同水準之保護個人資料制度的外國除外。

104 關於個人資料之處理，根據本法第四章第一節個人資料處理業者義務之規定，為了持續性採取相當於個人資料處理業者應採取措施的措施，建立符合個人資料保護委員會規則所規定標準之必要體制者除外。

105 個人情報の保護に関する法律第 24 条。

106 個人情報の保護に関する法律第 20 条。

107 個人情報の保護に関する法律第 21 条。

108 個人情報の保護に関する法律第 2 条第 9 項。

本報告之智慧財產權屬於國家通訊傳播委員會

匿名加工資料處理業者，在向第三方提供匿名加工資料時，根據個人資料保護委員會規則[109]所規定的內容，必須事先公告關於提供第三方之匿名加工資料的項目及提供方法，並對第三方清楚表明該提供之相關資料為匿名加工資料[110]。

(二) 個人資料保護法指引

依個人資料保護法第 4 條、第 8 條與第 60 條，為了使業者實施適當有效措施處理個人資料，個人資料保護委員會於 2016 年制定「個人資料保護法相關指引」(個人情報の保護に関する法律についてのガイドライン)，提供民間業者適當處理個人資料之方針，該指引適用對象包含個人資料處理業者、匿名加工資料處理業者[111]。而個人資料保護委員會除了訂定指引通則，又依不同狀況分別訂定確認與紀錄義務篇、匿名加工資料篇等。

1. 通則篇

本指引係就個人資料保護法上所規定之事項，以淺顯易懂之具體事例說明，幫助業者理解與遵循個人資料保護規範。業者倘若不遵守指引中關於「必須」及「不得」之敘述事項，有可能被判定違反法律；若不遵守有關「必須努力」、「期望」等文字之敘述事項，雖然不能據此立即判斷為違法，惟依個人資料保護法第 3 條個人資料應基於尊重個人人格之理念下為謹慎適當之處理[112]，業者應依其規模與特性盡可能實施適當之措施[113]。

2. 確認紀錄義務篇

日本過去曾發生民間企業大規模洩漏個資事件，有鑑於

[109] 係指個人資料保護相關法律實施規則（個人情報の保護に関する法律施行規則）。
[110] 個人情報の保護に関する法律第 37 条。
[111]〈個人情報の保護に関する法律についてのガイドライン（通則編）(令和 3 年 1 月一部改正版本)〉，個人情報保護委員会，頁 1，https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf（最後瀏覽日：2021/08/12）。
[112] 個人情報の保護に関する法律第 3 条。
[113] 同前註 111。

本報告之智慧財產權屬於國家通訊傳播委員會

此，個人資料保護法新增確保個人資料正當提供予第三人之規範。就業者向第三人提供確認紀錄之相關義務為詳細說明。本指引對個人資料保護法第 23 條將資料提供予第三人、個人資料保護法第 25 條業者將資料提供予第三人時應作成相關紀錄，個人資料保護法第 26 條於接受來自第三人之資料時亦應進行確認等規範，舉出淺顯易懂之具體事例為說明，以幫助業者確實遵循個人資料保護法規範[114]。

3. 向外國第三方提供篇

隨著資通訊技術高度發展，與經濟社會活動逐漸全球化，個人資料跨境傳輸應用逐漸增加，因此有必要制定向外國移轉個人資料之規範，與整備個人資料保護之國際法規範，依個人資料保護法新增第 24 條關於個人資料處理業者向位於日本境外之國家或地區之第三方提供資料之限制規範，並以本篇詳細說明之[115]。

依個人資料保護法第 24 條均應事先獲得本人同意，除非有以下情形：(1)第三方之國家在保護個人權益上，被認為具有與日本相同水準之個人資料保護體制；(2)持續性採取相當於個人資料處理業者應採取措施的措施，建立與規則相符之必要體制者;(3)符合個人資料保護法 23 條第 1 項各款之情況。而依第 24 條提供資料狀況判斷適用第 23 條提供資料方式[116]。

4. 匿名加工資料處理篇

個人資料保護法第 2 條第 9 項所稱得識別特定個人之狀態，係指由單一資訊或將多種資訊相互結合，以社會通

[114]〈個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）〉個人情報保護委員会，頁 1-2，https://www.ppc.go.jp/files/pdf/guidelines03.pdf（最後瀏覽日：2021/08/12）。

[115]〈個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編（令和 3 年 1 月一部改正版本）〉，個人情報保護委員会，頁 1，https://www.ppc.go.jp/files/pdf/210101_guidlines02.pdf（最後瀏覽日：2021/08/12）。

[116] 同前註 115，頁 2-4。

本報告之智慧財產權屬於國家通訊傳播委員會

念上一般人判斷力或理解力，是否得認定具體人物與該資料具備同一性。而無法識別特定個人之要件，並非指必須達到將所有技術面之可能性完全排除，而係要求以一般人與一般經營業者之能力、手段等為標準，無法透過通常方法識別個人之狀態[117]。

(三) 電信通訊事業個人資料保護指引

總務省針對電信通訊業者制定「電信通訊事業個人資料保護指引」(電気通信事業における個人情報保護に関するガイドライン)，以提升電信通訊服務之便利性，與個人資料保護。因應個人資料保護法相關指引(通則篇)之修正，總務省於 2017 年 9 月修正電信通訊事業個人資料保護指引之內容，以確保內容之一致性[118]。

該指引分為四章，第一章總則說明目的、適用對象及定義，第二章為利用個人資料之共通原則，第三章分別針對不同個人資料利用狀況，制定更細緻之蒐集、處理與利用規範，第四章將因應社會狀況與技術發展，隨時做出檢討與修正[119]。

1. 使用個人資料之共通原則

該指引第 6 條規定電信通訊業者提供電信通訊服務有必要時，始得蒐集個人資料[120]。指引第 7 條則規定電信通訊業者不得透過欺騙或其他不正當手段獲取個人資料，就敏感性特種個人資料，除獲得本人同意，或有(1)依法令；(2)為保護本人生命、身體或財產之情形，而取得本

[117]〈個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）(平成 29 年 3 月一部改正版本)〉個人情報保護委員会，頁 3-4，https://www.ppc.go.jp/files/pdf/guidelines04.pdf（最後瀏覽日：2021/08/12）。

[118]〈電気通信事業における個人情報保護に関するガイドライン〉，総務省，2017/09/14，https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html（最後瀏覽日：2021/08/12）。

[119] 電気通信事業における個人情報保護に関するガイドライン，平成 29 年総務省告示第 297 号，平成 29 年 9 月 14 日，https://www.soumu.go.jp/main_content/000507466.pdf（最後瀏覽日：2021/08/12）。

[120] 電気通信事業における個人情報保護に関するガイドライン第 6 条。

本報告之智慧財產權屬於國家通訊傳播委員會

人同意有困難時;(3)為提升公共利益或維護兒童身心健全發展，而取得當事人同意有困難時;(4)協助國家機關或地方公共團體或受其委託者執行法令所規定之事務，取得本人同意有可能對執行該事務造成阻礙的之虞時;(5)經本人、國家機關、地方公共團體、個人資料保護法第 76 條第 1 項各款所揭示者、外國政府、外國的政府機關、外國的地方公共團體、國際機構、或在國外相當於個人資料保護法第 76 條第 1 項各款所揭示者，公開該敏感性特種個人資料之情形;(6)目視或拍攝到本人，因此獲得本人外形上明顯敏感性特種個人資料之場合;(7)依第 15 條第 10 項各款所揭示之情形，接收敏感性特種之個人資料的提供時，上開情況始得取得個人資料[121]。

2. 取得特別性質之個人資料之規範

該指引將個人資料再區分為通聯紀錄、使用明細、發話人資料、位置資料、滯納費用之用戶資料、發送垃圾郵件之契約用戶資料、電話號碼等七種資料類型分別適用不同要件：

(1) 通聯紀錄

係指電信通訊服務用戶利用該服務之日期時間，與除了通訊內容以外之相關通訊資料。電信業者得蒐集通訊紀錄之範圍，僅限於為計算資費、請求繳費、處理客訴、防止不當利用及其他執行業務上之必要情形者等，並須於最小必要限度內記錄通聯紀錄之行為，始為正當業務行為[122]。

(2) 使用明細

係指記載電信契約用戶利用之日期時間、各通訊方，以及依費率計算通訊費用及其他記載有關通訊

[121] 電気通信事業における個人情報保護に関するガイドライン第 7 条。
[122] 電気通信事業における個人情報保護に関するガイドライン第 32 条。

本報告之智慧財產權屬於國家通訊傳播委員會

契約用戶資料之書面資料[123]。電信業者蒐集客戶使用明細資料之範圍不得超過達成使用明細之目的之必要範圍[124]。

(3) 發話人資料

係指有關發話人電話號碼、發話人位置等與發話人相關之資訊。電信通訊業者提供顯示發話人資料服務須採取確保使用者權利必要措施[125]。

(4) 位置資料

係指顯示持有行動設備終端機器者的位置資料，而非發話人資料的內容。當電信通訊業者事先得用戶同意時，僅以提供電信服務之相關正當業務行為及其他阻卻違法事由的情形為限，始得提供位置資料[126]。

(5) 滯納費用之用戶資料

係指超過付款日期仍拒絕繳納電信服務相關費用者，包含行動語音通訊服務等契約名義人姓名、住址、滯納金額、電話號碼及其他足以辨識個人之資料。當電信通訊業者為防止拒繳電信服務費用或不正當使用行動語音通訊服務，在適當必要之情況下，得與其他電信業者間交換滯納費用者之資料。惟若交換該滯納費用者資料可能有不當侵害本人權益之疑慮時，即不得為之[127]。

(6) 發送垃圾郵件之契約用戶資料

電信通訊業者為防止濫發電子垃圾郵件情形，於適當必要之情況下，得與其他電信業者交換該濫發郵

[123] 由電信通訊事業業者明細的記載事項觀之，包含了顯示開始通訊日期、時間、通話時間、對方電話號碼、每次通訊的金額、國際通話時的目的地等，故使用明細幾乎等同於屬於秘密通訊的通聯紀錄，電信業者蒐集客戶使用明細之資料。有必要將通訊秘密及個人隱私納入考量。

[124] 電気通信事業における個人情報保護に関するガイドライン第 33 条。

[125] 電気通信事業における個人情報保護に関するガイドライン第 34 条。

[126] 電気通信事業における個人情報保護に関するガイドライン第 35 条。

[127] 電気通信事業における個人情報保護に関するガイドライン第 36 条。

本報告之智慧財產權屬於國家通訊傳播委員會

件之契約用戶包含姓名、住所等相關個人資料。惟若交換該資料，有不當侵害當事人權益之疑慮時，即不得為之[128]。

(7) 電話號碼

電信通訊業者將電話號碼資料使用於印製發行電話簿或提供電話號碼查詢服務時，應讓用戶選擇是否提供，若用戶拒絕時應立即將該用戶之資料排除於電話簿或電話號碼查詢業務對象之外。而刊載或提供電話號碼查詢業務時之限制，與達成業務目的間應有必要性，其範圍應以刊載姓名、住所、電話號碼或刪除部分住址之資料為限，惟若經用戶同意則不在此限。而電信業者發行電話簿或提供電話號碼查詢服務之形態，不得不當侵害本人之權益[129]。

日本於 2003 年制定之個人資料保護法，明定適當利用個人資料之基本方針及保護個人資料之措施，明確國家與地方自治團體及業者應遵守之責任義務，而後隨著 2016 年 Society 5.0 之概念提出，與資料加值之應用越來越廣泛，個人資料保護法規範亦更加細緻。而為了使業者得適當處理個人資料，日本個人資料保護委員會制定個人資料保護法指引，總務省則制定電信通訊事業個人資料保護指引，協助電信通訊業者在基於尊重個人人格之理念下，適當使用個人資料。

面對 COVID-19 疫情，日本厚生勞動省開發之 COCCA 為確保使用者之隱私，並不會獲取任何可識別使用者之資訊，並制定隱私保護方針與使用規則。此外，日本電信業者 KDDI 公司開發人口動態分析預測系統，與支援國家與自治團體災害因應資料系統，透過訂定個人資料隱私政策相關規範保護用戶個人資料。而 NTT Docomo 公司之人口流動統計服務與行動空間統計，不會識別特定客戶個人身分之統計資料，該公司在個人資料保護方面制定個人資料保護憲章、個人資料隱私政策，與行動空間統計指引，行動空間統計所使用之運行資料需

[128] 電気通信事業における個人情報保護に関するガイドライン第 37 条。
[129] 電気通信事業における個人情報保護に関するガイドライン第 38 条。

本報告之智慧財產權屬於國家通訊傳播委員會

經過去識別化、計算、保密等三階段處理，以確保隱私。

上開案例中蒐集應用個人資料之電信業者，均訂定個人資料隱私相關保護方針，明確說明資料蒐集與處理措施，並遵循日本個人資料保護相關法規、指引等，可見業者對於個人資料處理之謹慎態度。隨著日本資料流通環境逐漸完備，未來除了防範災害、人口統計分析應用，應可看到更多元之應用案例。

第五節 韓國

韓國政府在應用電信資料部分，早期常見於犯罪偵查階段，由電信業者提供使用者的通信資料、通話內容等，提供國情院、檢察機關進行調查所用，爾後由於 IT 產業的蓬勃發展，韓國政府開始積極與電信業者合作，擴大電信資料於公部門中的應用範圍。

一、 應用案例

(一) 智慧檢疫系統

2015 年中東呼吸症候群冠狀病毒感染症（Middle East respiratory syndrome coronavirus [MERS-CoV]，以下稱 MERS）在韓國爆發，由於當時必須取得使用者本人同意始能追蹤行動裝置位置，導致韓國政府在 MERS 感染初期無法及時控制確診者及密切接觸者的位置與動線，引發 2 次接觸及 3 次接觸以上之大感染。

藉此契機，韓國政府分別於 2015 年及 2018 年對「傳染病防治暨管理相關法律」[130]（簡稱「傳染病防治法」）進行修正，以法律明文要求電信業者應提供使用者位置資訊，即為防免傳染病擴散等公益目的，電信業者應配合政府提供使用者位置資訊，強化追蹤確診者及回溯感染源等防疫措施。

2019 年 10 月 29 日韓國疾病管理本部(질병관리본부,

[130] 原文為「감염병 예방 및 관리에 관한 법률」。

本報告之智慧財產權屬於國家通訊傳播委員會

以下稱疾管部）援引過去 MERS 的經驗，以電信業者提供之使用者的位置資訊，包含使用者自傳染病流行國直接進入韓國或曾到訪傳染病流行國等漫遊資料，建構智慧檢疫系統（스마트검역시스템）[131]，即由疾管部交叉比對電信業者使用者之境外漫遊數據及入境名單，用以集中觀察特定使用者入境時的健康狀態，以即時追蹤並掌握傳染病動向。

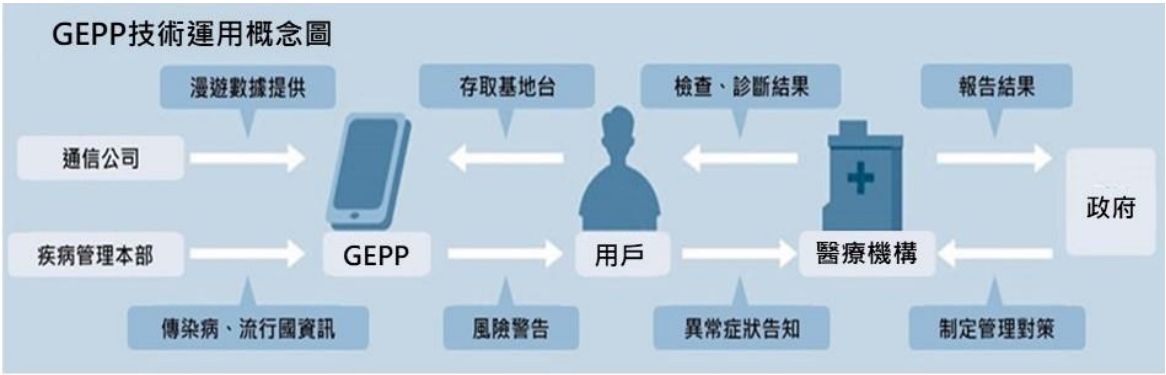
(二) GEPP

2020 年 COVID-19 在全球大流行，韓國的科學技術情報通信部、保健福祉部與電信業者 KT Corporation 合作，打造「全球傳染病擴散防止平台」（GLOBAL EPIDEMIC PREVENTION PLATFORM, GEPP），此平台以 2015 年 MERS 爆發後韓國政府所設置之智慧檢疫系統為基礎，由 KT 負責蒐集使用者（即 KT 用戶）的國際漫遊數據，並藉由 ICT 技術將使用者所在地區（境外）存在之流行性傳染病相關訊息以 SMS（簡訊服務）傳送給使用者，達到落實防疫觀念的宣傳；爾後，此平台更發展得對國內確診個案進行後續追蹤等技術，協助韓國政府透過蒐集行動通信商的漫遊資訊與基地台的位置資訊，落實防疫工作。

GEPP 技術運用可參考下方概念圖：

[131] 韓國疾病管理廳於 2019 年 10 月 31 日以「세계 최초!! 스마트검역정보시스템 실시로 해외 감염병 유입 사각지대 최소화」（譯：世界最初！！實施智慧檢疫系統減少海外傳染病流入之死角）發布新聞稿，介紹韓國打造的智慧檢疫系統，預期有效抑制海外入境的傳染病來源，資料來源：http://www.nih.go.kr/gallery.es?mid=a20503010000&bid=0002&b_list=9&act=view&list_no=144510&nPage=1&vlist_no_npage=2&keyField=&keyWord=&orderby=（最後瀏覽日：2021/08/10）。

本報告之智慧財產權屬於國家通訊傳播委員會



資料來源：本計畫編譯自코로나 꼼짝마! 글로벌 감염병 확산 방지 프로젝트 (GEPP)[132]

圖10　GEPP 技術運用概念圖

概念說明：

第一步：通信公司提供漫遊數據至 GEPP 平台；疾病管理本部提供傳染病、流行國資訊至 GEPP 平台。

第二步：使用者存取基地台的資訊會被傳送至 GEPP 平台；GEPP 平台判斷使用者所在地為傳染病流行國家時，對使用者(KT 用戶)發出風險警告。

第三步：使用者自認有異常症狀時向醫療機關告知；醫療機關將檢查或診斷結果通報使用者。

第四步：醫療機關將處理結果向政府報告；政府對醫療機關制定管理對策。

由於 GEPP 是政府利用 KT 的 ICT 技術，因此所蒐集包含用者之入出境日、訪問國、姓名及出生年月日等資訊以 KT 的使用者為主，透過平台向前往傳染病流行國的使用者傳遞預防傳染病消息，落實防疫宣導，使政府得掌握並管理可能暴露於感染源的入境使用者[133]，並持續追蹤至潛伏期結

[132] 코로나 꼼짝마! 글로벌 감염병 확산 방지 프로젝트 (GEPP), http://naver.me/G2UGJm9H（最後瀏覽日：2021/10/12）。

[133]法源為傳染病防治法第 76 條之 2 規定「疾病管理廳長、市・道知事或市長・郡守・區廳長，

本報告之智慧財產權屬於國家通訊傳播委員會

束，惟 GEPP 雖相較於早期智慧檢疫系統更多了預防傳染病傳播的宣導措施，但仍需要搭配使用者（用戶）察覺有異常症狀時的自行告知[134]，才能有效落實 GEPP 欲建立的防疫概念。

隨著 COVID-19 持續在全球流行，各種病毒變異株不斷的出現，因此 KT 以韓國政府為後盾，積極將 GEPP 技術推廣至其他國家，期望藉由多國合作以落實疫情控管，例如在肯尼亞、迦納、寮國等國家輸出 GEPP，並與盧安達、馬來西亞、阿拉伯聯合大公國及柬埔寨等國合作建置 GEPP，透過與全球各國電信業者的協力，可有效掌握使用者的位置資訊，而不再僅限於出入境紀錄或漫遊資訊等。

目前，KT 與東非最大電信業者 Safaricom PLC 合作，以加入 GEPP 獲取傳染病流行國家的資訊，東非各國亦可藉此對其國人進行防疫宣導，適度降低該國人至他國的感染風險，而 KT 更能藉此確實掌握韓國人在東非的位置資訊，供韓國政府防疫所用。

為預防傳染病及阻斷傳染散播而於必要時，得向『國家警察與自治警察之組織暨營運相關法律』所定之警察廳、市・道警察廳或警察署（以下於本條稱警察官署）之首長，要求傳染病確診者或疑似者之位置資訊。於此情形時，收到疾病管理廳長、市・道知事或市長・郡守・區廳長要求之警察官署，得向『位置情報之保護暨利用等相關法律』第 5 條第 7 項所定之個人位置情報事業者，及『電子通信事業法』第 2 條第 8 款規定之電子通信事業者，要求傳染病確診者或疑似者之位置資訊，無『位置情報之保護暨利用等相關法律』第 15 條及『通信秘密保護法』第 3 條之適用。而收到要求之個人位置情報事業者及電子通信事業者，若無正當事由，應依要求提供之。」；原文為「질병관리청장, 시·도지사 또는 시장·군수·구청장은 감염병 예방 및 감염 전파의 차단을 위하여 필요한 경우 감염병환자등 및 감염병의심자의 위치정보를 『국가경찰과 자치경찰의 조직 및 운영에 관한 법률』에 따른 경찰청, 시·도경찰청 및 경찰서(이하 이 조에서 "경찰관서"라 한다)의 장에게 요청할 수 있다. 이 경우 질병관리청장, 시·도지사 또는 시장·군수·구청장의 요청을 받은 경찰관서의 장은 『위치정보의 보호 및 이용 등에 관한 법률』 제 15 조 및 『통신비밀보호법』 제 3 조에도 불구하고 『위치정보의 보호 및 이용 등에 관한 법률』 제 5 조제 7 항에 따른 개인위치정보사업자, 『전기통신사업법』 제 2 조제 8 호에 따른 전기통신사업자에게 감염병환자등 및 감염병의심자의 위치정보를 요청할 수 있고, 요청을 받은 위치정보사업자와 전기통신사업자는 정당한 사유가 없으면 이에 따라야 한다.」。

[134] GEPP 發送風險警告訊息時會同時提供檢疫連結，當使用者發覺有異常症狀時得主動透過檢疫連結進行通報。

本報告之智慧財產權屬於國家通訊傳播委員會



資料來源：KT[135]

圖11　KT 與東非最大電信業者 Safaricom PLC 合作

(三) K-MyData

韓國政府為因應人工智慧（AI）技術的長期發展，於 2016 年 12 月推出 K-MyData 制度[136]，改變過去個人資料管理系統以服務提供者為中心的模式，而是由當事人處於主導的地位[137]，使各特定企業在取得當事人同意後可向其他企業提供該當事人之個人資訊，如整合電腦、金融、醫療等各產業間所保存之個人資訊，以運用於開發新的服務。

MyData 係指當事人享有對自己個人資料統治控制的權利，以此概念為基礎，應用個人資料及其應用範圍，並建立新的使用方式。而透過 K-MyData 制度的引進將使當事人變成管理個人資料的主體，當事人可決定是否將特定企業如電信業者、銀行、醫院等各領域所保存的個人資料集中，並

[135]알파에서 오메가까지 한눈에! KT GEPP 홍보 책자 발간，https://blog.kt.com/1525?category=705035（最後瀏覽日：2021/10/12）。

[136] 由韓國數據產業振興院（한국데이터산업진흥원）負責推廣。

[137] 개인정보보호 법제 하에서의 정보 활용성 향상 전략，KISDI Premium Report，2017/12/27， https://www.cisp.or.kr/archives/18706（最後瀏覽日：2021/10/12）。

本報告之智慧財產權屬於國家通訊傳播委員會

提供予他企業分析，以獲取新的服務[138]，例如提供銀行帳戶、歷年信用卡帳單及通信費帳單的繳費資訊等，供他企業進行個人的債務狀況評比。

2018 年開始，MyData 的應用逐漸在金融、通信等領域展現，韓國的科學技術部亦推出「本人認證 MyData 應用支援產業」，打造以資料主體為中心的個人數據管理及應用服務，極大化資料主體在提供及應用個人資料時的便利性及安全性，爾後 MyData 亦延伸至醫療[139]、能源[140]、物流、教育、文化、媒體等領域。

現在，在韓國的資料主體可透過 MyData[141]平台蒐集、儲存、管理與自己有關的數據資料。

(四) 智慧城市統合平台

韓國的「智慧城市統合平台」[142]於 2008 年 8 月間由國土交通部（국토교통부）、行政安全部（행정안전부）、知識經濟部(지식경제부)等共同委外設計，自 2009 年起至 2013 年，為研發「智慧城市統合平台」，韓國政府投入逾韓幣 100 億元（約為 2.35 億台幣），並於 2013 年至 2014 年起，以仁川青羅島及世宗市為示範地點；2015 年「智慧城市統合平台」連接 112 緊急救難中心及 119 消防中心，全力打造社會安全網，強化國家災難救助及管理系統。

2016 年「智慧城市統合平台」與電信業者 SK Telecom Co., Ltd.簽約，協力發展保護弱者（幼童、失智老人）系統，即「幼童與失智老人保護服務」，其服務宗旨為當幼童與失智老人有緊急情況發生時，智慧城市統合平台可以自電信

138 심연숙, “마이데이터(MyData) 활용의 국내외 현황 및 활성화 방안”, The Journal of the Convergence on Culture Technology (JCCT), Vol. 6, No. 4, 2020/11/30，553-558。

139 例如下載特定法院的 App 後，可以直接連線就診紀錄並提供給第三方企業分析，以推薦符合資料主體的運動商品、保健食品等。

140 指用水量、電力、瓦斯等與能源有關之產業，例如依家庭人口別分析平均能源使用量，確認是否需進行節約教育，目前韓國的世宗市實施中。

141 Kdata, https://www.kdata.or.kr/（最後瀏覽日：2021/08/10）。

142 原文為「스마트시티통합플랫품」。

本報告之智慧財產權屬於國家通訊傳播委員會

業者處取得使用者之位置資訊，以迅速提供緊急救援，確保黃金時間[143]。

爾後，「智慧城市統合平台」陸續於 2017 年、2018 年、2019 年透過利用雲端，及民間保全業者的投入，建構女性安全支援服務、電子腳鐐違反者迅速監督服務等智慧都市安全網，亦與法務部合作於首爾市、光州市、大田市等都市打造位置追蹤中心，與警察廳合作於首爾市、光州市、江原道、恩平區、瑞草區等打造通緝車輛檢索系統等，欲藉由利用電信資料得掌握犯罪者的動向，改善打擊犯罪的權能。

二、 相關法規

(一) 電子通信事業法

韓國的「電子通信事業法」(전기통신사업법) 第 83 條第 3 項規定電信業者得於法院、檢察機關或搜查機關（包含國稅廳長或地方政府國稅廳長），因裁判、搜查或國家安全保障之必要而請求提供或閱覽包含使用者姓名、住民登錄號碼、住所、電話號碼、ID（指透過電腦系統或在網路上使用可供識別之符號）、加入日期及解除日期等電信資料時，提供之[144]；同條第 4 項規定前揭請求應以書面記載必要資料之範圍向電子通信業者提出申請（若遇緊急狀況而無法事先提供書面時，得先為要求待緊急事由不存在後，即應補提

[143] 韓國國土交通部於 2020 年 5 月發表「스마트시티통합플랫품기반구축」（譯：智慧城市統合平台基本建設）之說明資料。資料來源：https://smartcity.go.kr/wp-content/uploads/2019/08/200603-%EC%8A%A4%EB%A7%88%ED%8A%B8%EC%8B%9C%ED%8B%B0%ED%86%B5%ED%95%A9%ED%94%8C%EB%9E%AB%ED%8F%BC%EA%B8%B0%EB%B0%98%EA%B5%AC%EC%B6%95.pdf（最後瀏覽日：2021/08/10）。

[144] 原文為「전기통신사업자는 법원, 검사 또는 수사관서의 장(군 수사기관의 장, 국세청장 및 지방국세청장을 포함한다. 이하 같다), 정보수사기관의 장이 재판, 수사(「조세범처벌법」 제 10 조제 1 항・제 3 항・제 4 항의 범죄 중 전화, 인터넷 등을 이용한 범칙사건의 조사를 포함한다), 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 다음 각 호의 자료의 열람이나 제출(이하 “통신자료제공”이라 한다)을 요청하면 그 요청에 따를 수 있다.」。

本報告之智慧財產權屬於國家通訊傳播委員會

書面）[145]。是韓國為了裁判、搜查、國家安全保障等，透過法律明文規定法院、檢察及搜查機關等於必要時得向電信業者提出提供或閱覽電信資料之請求，惟該法律明文非義務性規定，電信業者收到請求後得自行決定是否提供電信資料。

(二) 位置情報法

隨著移動通信技術的進步，利用位置資訊而生之物流、保全、商業交易等服務日趨蓬勃，對於個人位置資訊所衍生的洩漏、濫用等憂慮意識增高，韓國於 2005 年 7 月 28 日制定「位置情報之保護暨利用等相關法律」（위치정보의보호및이용등에관한법률，簡稱位置情報法），以監督使用位置資訊之相關產業，包含許可蒐集位置資訊業務、提供位置資訊基礎服務業務申請等，對蒐集及提供位置資訊之相關程序以明文規定，避免位置資訊之洩漏及濫用等侵害產生[146]。

然而，自「位置情報法」施行以來，電信業者遇到警察、海巡及消防等機關（以下簡稱緊急救援機關）有緊急救助或必要時，實務操作均面臨「應」提供，而非「得」提供之情況，使「位置情報法」制定的目的不達；國會議員鄭必模

[145] 原文為「제 3 항에 따른 통신자료제공 요청은 요청사유, 해당 이용자와의 연관성, 필요한 자료의 범위를 기재한 서면(이하 “자료제공요청서”라 한다)으로 하여야 한다. 다만, 서면으로 요청할 수 없는 긴급한 사유가 있을 때에는 서면에 의하지 아니하는 방법으로 요청할 수 있으며, 그 사유가 없어지면 지체 없이 전기통신사업자에게 자료제공요청서를 제출하여야 한다.」。

[146]詳參「位置情報之保護暨利用等相關法律」2005 年 7 月 28 日施行之立法理由「이동통신기술의 급속한 발달로 물류, 보안, 상거래 등에 위치정보를 이용하는 다양한 서비스가 등장하면서 개인위치정보가 유출, 남용되는 등 개인의 사생활이 침해될 우려가 커지고 있는 바, 위치정보를 수집하는 사업에 대하여 허가제도, 위치정보기반서비스를 제공하는 사업에 대하여 신고제도를 도입하고, 위치정보의 수집·제공 등에 관한 절차를 정함으로써 위치정보의 유출로 인한 사생활 침해의 방지를 도모하는 한편, 위치정보와 관련된 기술개발, 표준화 등을 지원함으로써 위치정보의 이용을 활성화하고 국민생활의 향상과 공공복리의 증진에 이바지하려는 것임.」。

本報告之智慧財產權屬於國家通訊傳播委員會

（정필모）於 2020 年 9 月 10 日，對現行電信業者及緊急救助機關之作為提出批判，認為根據「位置情報法」規定，為了保護有急迫危險之人生命及身體，如本人或其配偶提出緊急救助請求時，緊急救援機關即可向電信業者請求提供被救者之移動通訊位置（通常指手機位置），並在該地點展開救援行動，然而，緊急救援機關往往濫用此項規定，將請求之位置資訊用於監控一般民眾；且緊急救援機關及電信業者長期未依「位置情報法」規定，定期每 6 個月據實向國會報告其所提供或所請求之位置資訊相關數據，以隸屬國會之科學技術情報放送通信委員會（과학기술정보방송통신위원회）自 2017 年至 2019 年間的統計資料顯示，電信業者向國會報告提供給緊急救援機關位置資訊總計有 50,521,118 件，然而緊急救援機關向國會提交之報告數據卻是 64,286,813 件，顯見兩者向國會提交的數據差距懸殊，此即是國會未能確實扮演監督的角色，要求緊急救援機關及電信業者定期報告所致；此外鄭議員更表示現行「位置情報法」規定，國會對於位置資訊的管制，僅有要求提供報告的義務，缺乏對於報告數據的分析驗證等規定，實際上的監督機制略顯不足[147]。

2021 年 10 月 19 日韓國通過「位置情報法」部分修正案，並定於翌年 4 月 20 日施行，為降低處理個人位置資訊之事業者濫用位置資訊的問題，修法後要求韓國通訊傳播委員會必須對欲進入處理個人位置資訊之業者進行嚴格審查，且韓國通訊傳播委員會得對違反「位置情報法」之業者，命其中止違反行為等改正措施，及科處罰鍰等強制性手段，強化韓國通訊傳播委員會在蒐集、利用或提供個人位置資訊之監管權限。

147 정필모, 정부 통신사 아무도 지키지 않는 [위치정보법], 2020/10/11，https://www.theminjoo.kr/board/view/inspection/338137?st=wrote_post&keyword=%EC%A0%95%ED%95%84%EB%AA%A8&page=2（最後瀏覽日：2021/08/10）。

本報告之智慧財產權屬於國家通訊傳播委員會

(三) 傳染病防治法

韓國於 1994 年 6 月 28 日開始施行通訊秘密保護法（통신비밀보호법），以作為保護人民自由交談及通訊秘密的法律依據，對於電子監聽、監看等必要，亦制定嚴格的法定程序，致力於確保人民的隱私受到保護。

然而，2015 年 MERS 在韓國爆發，韓國政府為了有效掌握確診者動線以抑止疫情在韓國境內擴散，遂於 2015 年 7 月 6 日於傳染病防治法（감염병예방법）新設立第 34 條之 2，明定保健福祉部應即時公開確診者的移動路線、交通工具及醫療機構等資訊，使大眾得以輕易知悉是否為接觸者，此次新法修訂使防疫當局在公開確診者移動路線等相關資訊時，不會受到通訊秘密保護法的拘束，並符合韓國個人資料保護法第 58 條第 1 項第 3 款規定「為確保公眾衛生等公共之安全與秩序，因緊急必要而臨時性處理之個人情報」。

2020 年 3 月 4 日，韓國政府為因應 COVID-19 的爆發，修正第 34 條之 2 的規定，將可公開確診者足跡的權限及義務不再僅限於保健福祉部長，進而擴張至廣域市長、道知事長、地方郡守、區廳長等，並於法律明文限制性別、年齡等與防疫無關之資料不予公開，另包含確診者的移動路線、交通工具、診療機關及接觸地現況等應公開之資訊則必須第一時間透過網路或新聞資料對外發布，使國民得有效知悉傳染病最新資訊，期望達到抑止傳染病擴散的效果；而除了對公開足跡範圍作必要限制外，賦與人民對公開內容有爭議時，如公開資訊之事實有誤、對公開內容有意見等可依法向發布資訊之機關提出異議，並由發布機關對該異議進行調查；此次修法除以法律授權強化行政機關在防疫上的主導地位外，對於人民的權利保障亦併行。

2020 年 5 月初的梨泰院夜店群聚感染事件，韓國的中

本報告之智慧財產權屬於國家通訊傳播委員會

央防疫對策本部（중앙방역대책본부）即依「通信秘密保護法」及「傳染病防治法」等規定，向電信業者要求使用者特定區段時點資訊，以該區段時點之使用者資訊，即時掌握 1 萬名與確診者密切接觸之人。

然而，日常生活動向持續被電信業者暗地蒐集實已有侵害隱私之虞，除韓國隱私保護相關團體率先對韓國政府因「梨泰院夜店」事件而請求曾到訪梨泰院的 1 萬名個人資料之行為，以過度的隱私蒐集是對人民基本權的侵害提起違憲訴訟[148]外，韓國政府如何避免電信業者高舉維護公益目的大旗，卻暗地蒐集隱私販售營利[149]，乃韓國政府未來制度規畫上所需面對的課題。

第六節 小結

維護國家安全、公共利益為不確定法律概念，衡酌人民對於其資料利用目的，仍應有透明信賴基礎為前提，如透過充分告完整告知同意、事前完整影響評估機制等，如愛沙尼亞推動電子化政府，針對資料敏感性等重要議題，在保持技術中立性，逐步檢視調修法律可能對電子治理發展造成障礙，進行風險分析，避免過度監管或是造成監管障礙。而英國政府則為取得公眾信賴，資料儲存和使用完全透明，並進行資料風險評估，且考量去識別化技術、數位落差問題。日本為協助業者適當使用資料，制定個人資料保護法指引並依不同狀況再細分，如就去識別化技術則有匿名加工資料篇，而針對電信通訊業者亦

[148] 由律師團、數位資訊委員會、社團法人資訊人權研究所、進步網路中心、相關公會等分別對保健福祉部長、疾病管理本部長、首爾特別市長、首爾地方警察廳長（總稱為防疫當局）等，以防疫當局違法蒐集 2020 年 5 月 18 日到訪梨泰院約 1 萬人次行動電話基地台存取資訊等，提起憲法訴願，韓國憲法裁判所於 2020 年 7 月 29 日正式受理，現在該訴願進行中。資料來源：이대희，이태원 기지국 접속자 정보 수집, 헌재에서 다룬다，2020/07/30，http://www.pressian.com/pages/articles/2020073017151595841（最後瀏覽日：2021/09/08）。

[149] 電信業者未經過使用者事前同意即私下蒐集行動電話基地台存取資訊，原意係用於提供緊急救援機關進行急難救助，然而電信業者卻擅自將該資訊用於發展各自的大數據資料庫，而被視為以公益之名行營利之實。資料來源：김재섭，[단독] 이통 3 사, 따로 DB 만들어 '위치정보' 몰래 모았다，2020/09/02，https://www.hani.co.kr/arti/economy/it/960279.html（最後瀏覽日：2021/09/08）。

本報告之智慧財產權屬於國家通訊傳播委員會

制定電信通訊事業個人資料保護指引，以兼顧通訊便利性與個資保護。而韓國電信資料應用也延伸至保健衛生議題，透過傳染病防治法修法，直接依法授權相關機關取得電信資料，並藉此與電信業者合作落實防疫。相較於前述國家，美國雖無統一適用的個人資料保護專法，而依照各領域制定相關個資保護規範，但因應疫情美國政府重新思考使用電信資料評估作為後續政策規範考量。

觀察本研究整理電信業者因公共利益而配合提供電信資料應用，以當事人位置資訊應用最為廣泛，除了傳統用於配合檢警機關進行犯罪搜查等目的外，如愛沙尼亞行動定位資料（MPD）、美國位置資料追蹤應用、英國因應疫情於電信行動位置資料分析、日本為了防災進行人口動態分析，韓國逐漸發展出用於對於失智老人、走失幼童的緊急救援及對嚴重傳染病流行區加強巡邏等，有效提升國家安全機制，可預見若能有效運用電信業者所持有之位置資訊，對於國家安全公共利益的維護有加乘效果。由於目前針對位置資訊應用大多仍是以匿名資料為主，如日本就有針對假名加工資料有明文規定與相關指引，提供業者遵循依據。因此本研究後短期建議就當事人同意與透明度改善，如於隱私權政策有更詳盡告知說明，甚至預先進行資料保護影響評估，讓當事人對於公共利益而應用其個資能夠理解解除其疑慮；中長期建議我國得針對位置資訊與去識別化更詳細規範，以提供我國電信業者作為應用上的法源依據。

本報告之智慧財產權屬於國家通訊傳播委員會

表 1 資通訊技術傳輸資料維護國家安全公共利益應用案例與相關法規配套之整理

國家	應用案例	相關法規與配套
愛沙尼亞	• 接觸者追蹤：公私合作開發COVID-19應用程式 HOIA（此APP 單純以藍芽傳輸交換用戶ID，未涉及電信資料） • 位置資訊應用於人口分析：公私合作開發 MPD 系統，即時追蹤行動電話位置來統計移動定位資料	• 歐盟第223/2009號規則 • 電子通訊法 • 衛生資料系統法 • 醫療保健服務組織法 • 資料交換層法
美國	• 位置資訊濫用：FCC 裁罰 AT&T、Sprint、Verizon 和 T-Mobile 向第三方業者出售用戶即時位置資料案例	• 資訊自由法 • 隱私法 • 通訊法 • 電信法 • 健康保險可攜與責任法 • 聯邦貿易委員會法 • 無線通訊及公共安全法 • 行動定位服務開發部署指南
英國	• 接觸者追蹤：公私合作開發 NHS COVID-19 APP	• 一般資料保護條例 • 資料保護法 • 健康服務（與病患資料管理）法
日本	• 接觸者追蹤：新冠肺炎密切接觸者應用程式（COCOA）與感染者資料管理系統（HER-SYS） • 位置資訊應用於人口分析：KDDI 開發人口動態分析預測系統 • 位置資訊整合應用於防災：KDDI 公司、應用地質公與豐田汽車公司合作，整合人口動態資料、應用地質公司之各種災害監測感應資料，以及浮動車輛資	• 電信通訊事業法 • 個人資料保護法 • My number 法 • 個人資料保護法指引（通則篇、確認紀錄義務篇、向外國第三方提供篇、匿名加工資料處理篇） • 電信通訊事業個人資料保護指引

本報告之智慧財產權屬於國家通訊傳播委員會

國家	應用案例	相關法規與配套
	料、氣象資料等開放資料產生各種防災資訊 • 位置資訊整合應用於防災：NTT Docomo 與學研合作共同研究開發人口流動統計服務，進行社會與產業調查之分析	
韓國	• 位置資訊應用於防疫：公私合作打造全球傳染病擴散防止平台（GEPP），蒐集電信業者漫遊資訊與基地台的位置資訊落實防疫 • 資料自主：韓國政府 K-MyData，由當事人決定是否將特定企業如電信業者所保存的個人資料集提供予他企業分析，打造以資料主體為中心的個人數據管理及應用服務，極大化資料主體在提供及應用個人資料時的便利性及安全性 • 位置資訊應用於救援：公私合作建立智慧城市統合平台，打造社會安全網，強化國家災難救助及管理系統，協力發展保護弱者（幼童、失智老人）系統，即有緊急情況發生時，智慧城市統合平台得自電信業者取得使用者位置資訊，以迅速提供緊急救援	• 傳染病防治法 • 電子通信事業法 • 位置情報法
我國	• 接觸者追蹤：社交距離 APP 及簡訊實聯制實施 • 位置資訊應用於人潮警示：各縣市政府與電信業者合作建置旅遊人潮警示燈號系統，運用「去識別化之電信大數據技術」統計景區的人流數據	• 個人資料保護法 • 傳染病防治法 • 統計法

資料來源：本計畫製作

本報告之智慧財產權屬於國家通訊傳播委員會

第三章 電信服務業創新應用現況實際應用案例與政策法制研析

數位經濟趨勢下，資料加值應用之社會與經濟潛力相當巨大，除有助於創新技術、開發新產品和服務之外，對於提高生產效率與增進公共利益亦頗有成效。然而，方便且精準的服務代價可能是消費者大量個人資訊，且資料越完整則分析準確性越高，意即一旦資料外洩，對個人隱私影響甚深。近年來，國際社會對於隱私保護與資料合理利用日趨重視。因此，如何在促進產業資料流通利用的同時，衡平個人資料與隱私保護，為目前各國積極面臨之挑戰。以下將參考數位發展優勢國家進行國際趨勢研究，針對電信服務業者對其電信服務所產生之資料，在創新應用方面之產業發展，進行實際應用案例研析，以及探討其資料政策之發展與相關法制現況。

第一節 愛沙尼亞

北歐電信公司 Telia 和愛立信（Ericsson）2020 年 10 月宣布一項合作計畫，預計到 2025 年將在瑞典和愛沙尼亞的一萬個基地站部署完成下一代 5G 網路[150]。而電信網路作為關鍵的國家基礎設施，5G 是推動各種國家數位經濟發展的催化劑。在推行數位化應用的過程中，任何數位預測結果皆需建立於可信任資料，因此，在使用及分析電信資料的過程中，確保資料的透明性及可信賴性，以及使用者之隱私安全至關重要。

一、 應用案例

(一) Telia 智慧停車系統（M-Praking）

交通建設作為智慧城市最基本之服務，愛沙尼亞自 2000 年開始透過電信業者 Telia 共同推出利用手機支付停車費的智慧停車系統 M-Praking，目的在於管理人口密集的城市交通，並建立現代化的低成本停車基礎設施，目前已有

[150] Telia and Ericsson switch on Estonia's first commercial 5G network, Ericsson (Nov. 10, 2020), https://www.ericsson.com/en/news/2020/11/estonia-switches-on-5g (last visited Aug. 28, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

超過 90%的停車費透過此系統支付。M-Praking 的運作方式僅需停車的過程使用手機應用程式 Pargi.ee 或傳送一則包含停車區代碼（Parking Zone Code）的簡訊給系統，使用者就可以透過 Pargi.ee 查看有關停車區域的相關詳細資訊，例如停車場位置、服務提供業者、計費方式等（參圖 12），以及設置停車提醒。在啟用 Pargi.ee 之前會對使用者進行身分識別，透過加入車牌號碼及銀行信用卡等方式，以便利繳費程序，而警察只要到資料庫中查詢車牌號碼，即可知道該車輛是否已付停車費。另外，若是手機設定開啟定位，此系統還會顯示距離最近的停車場，並可以查看過去六個月的停車紀錄[151]。



資料來源：本計畫編譯自 Telia.ee

圖12　Pargi.ee 使用介面

根據 Pargi.ee 服務條款，使用者透過 Pargi.ee 執行的交易紀錄會顯示車牌號碼、停車時間、停車地點以及費用，並透過手機號碼進行身分識別，並不會連結到個人 Mobile-ID，若使用者同意亦可以透過手機帳單來支付停車費。Pargi.ee

[151] E-Estonia, mobility services, https://e-estonia.com/solutions/location-based-services/mobile-parking/ (last visited June 20, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

會將使用者資料傳輸給停車場業者、銀行或其他其他相關第三方業者，並自使用期間或交易日起三年內保留使用者在 Pargi.ee 輸入的資料，而使用者在不違反使用協議或法律規定的情況下，有權向 Telia 提交申請要求刪除儲存在 Pargi.ee 內的資料[152]。

愛沙尼亞電信業者蒐集、處理及利用個人資料應符合歐盟一般資料保護規則（General Data Protection Regulation, GDPR）及電子通訊法之各項規定。根據 Telia 資料使用原則，Telia 蒐集個人基本資料，包括個人身分、通訊、與產品訂購相關以及付款能力債務評估等資料。通訊資料包括與通訊傳輸相關的電子通訊服務詳細資料，亦即使用服務時所產生的行動資料；位置資料則是指使用服務過程中終端設備的地理位置或提供服務的位置資料。資料保存期限則是根據電子通訊法第 111 條各項資料所需保留的法律要求期限內保留。

(二) Telia 人口流動分析（Telia Crowd Insights）

為了解人口流動趨勢及預測交通狀況、商業稠密區或是旅遊熱點等人群聚集地，Telia 透過蒐集北歐地區的 1600 萬名客戶的手機移動訊號，透過每人每天所產生的 400 多個訊號，以提供每天數十億個真實且準確的資料，並運用於以下面向：

1. 城市規劃：透過測量各地人口數，即可以分析哪些區域活動人口更多，而需要更多公共服務或是做出更適合之城市發展規劃，例如了解旅客從何而來、消費地點及購物喜好等，即可針對旅遊行銷方向提供更契合市場之方案，規劃出更適宜之活動企劃，以增添經濟效益[153]。
2. 公共交通：透過蒐集人民移動方式係透過搭乘大眾交通

[152] Contracts and Terms, Telia, https://www.telia.ee/en/lepingud-ja-tingimused#teenusetingimused (last visited Aug. 3, 2021).
[153] Crowd Insights for Municipalities, Telia, https://business.teliacompany.com/crowd-insights/Crowd-Insights-for-Cities (last visited Aug. 28, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

工具亦或其他移動模式，了解當地交通運輸概況，以分析出當發生不可預測之緊急情況時，應採取何種應變措施[154]。

3. 零售業者：透過蒐集客戶停留時間、客戶性別及年齡比例，即可以分析出潛在之客戶群，以在未來進行更好之商業決策[155]。
4. 活動及旅遊：透過分析旅客所欲前往之目的地以及旅遊目的、停留時間、地點、淡旺季趨勢、競爭產業表現情形等，即可以在未來進行最佳之投資及行銷方向，以提升競爭力[156]。

本項資料蒐集是透過 Telia 所建立之蜂窩網路資料，配合匿名 Wi-Fi 資料進行補充（參圖 13），資料蒐集之相關隱私設計皆符合 GDPR 對於資料蒐集、儲存與匿名化之相關規定。

[154] Crowd Insights for Transport, Telia, https://business.teliacompany.com/crowd-insights/Crowd-Insights-for-Public-Transport (last visited Aug. 28, 2021).
[155] Crowd Insights for Retail, Telia, https://business.teliacompany.com/crowd-insights/Crowd-Insights-for-Retail (last visited Aug. 28, 2021).
[156] Events & Tourism, Telia, https://business.teliacompany.com/crowd-insights/Crowd-Insights-for-Events-and-Tourism (last visited Aug. 28, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會



資料來源：本計畫編譯自 Telia

圖13　Telia 人口流動分析

二、　愛沙尼亞使用電信資料之個人資料保護

為促進電子通訊網路和電信服務的發展，確保技術中立及保障電子通訊用戶的利益，愛沙尼亞於 2005 年頒布電子通訊法取代原先之電信法（Telecommunications Act）[157]。電子通訊法第 111 條規定，電信和網路服務業者應該將通訊資料(包含元資料 Metadata)保留一年，以便識別來源、目的地、時間、持續時間和通訊的位置，並規定電信和網路服務業者所需保留的資料類型。另外，電子通訊法第 102 條要求電信和網路服務業者提供服務的過程中應對所取得之所有資料保密，若發生與通訊服務業務相關之個人資料外洩之情形時，應盡早通知資料保護監察機關[158]。

[157] The Right to Privacy in Estonia, Human Rights Committee (Mar. 2016), at 2-3.
[158] Electronic Communications Act, Riigi Teataja, https://www.riigiteataja.ee/en/eli/501042015003/consolide (last visited June 20, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

第二節 德國

德國電信產業自 1970 年代開始由壟斷走向競爭，逐步開放私人申請經營，進而轉向市場化及民營化。1988 年時德國政府決定配合歐盟於 1986 年所提出的電信自由化政策，政府由經營者蛻變為僅提供制度保障之監管者。2017 年德國推出 5G 戰略（5G Strategy）支持網路擴展計畫，以及 5G 應用開發。2019 年啟動行動通訊戰略（Mobile Communications Strategy），目標在於確保全國皆可接受行動語音及數據服務。德國聯邦經濟事務暨能源部（Federal Ministry for Economic Affairs and Energy）亦發布 2025 年數位戰略（Digitale Strategie 2025）希望加速刺激不同行業的寬頻普及與創新應用[159]。

一、 Deutsche Telekom AG 智慧家園求救系統

德國電信（Deutsche Telekom AG）作為德國最主要電信業者之一，其擁有約 2.42 億用戶、2700 萬條固定網路線路，以及 2200 萬條寬頻線路，並提供包括固網/寬頻、行動通訊、網路和網路協定電視（Internet Protocol Television, IPTV）產品和服務等，而為持續保持市占率，德國電信也從傳統電信業者轉型提供不同領域之全新服務。例如透過 GreenMagenta 計畫，將電信網路及旗下產品皆調整為綠色產品或服務，希望能提高能源使用效率並對環境友好，以符合氣候與資源保護及數位社會永續發展的目標。另外，也結合智慧家園（SmartHome）計畫，透過智慧家電或智慧服務協助使用者減少能源消耗以節約資源[160]。

SmartHome 計畫除了符合綠色標準之外，主要目標仍在打造智慧家居，將家居產品連接網路除了提升日常生活的便利性之外，更可以在家庭安全防護上做出貢獻。德國電信開發智慧家園求救系統（SmartHome Schutzbrief），與消防隊、警務單位以及安顧（ERGO）

[159] Country information – Germany, European Commission, https://ec.europa.eu/digital-single-market/en/country-information-germany (last visited July 20, 2021).
[160] #GreenMagenta - the name says it all, Deutsche Telekom AG, https://www.telekom.com/en/corporate-responsibility/corporate-responsibility/greenmagenta-the-name-says-it-all-624448 (last visited July 20, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

集團合作，當 SmartHome 產品自動識別家中出現的任何危險，例如煙霧偵測、漏水感測或是不明人士闖入等，當家中設備感測異常時，會透過智慧型手機向家庭成員發出警告，若無法聯繫到使用者時，則會向 ERGO 的緊急服務系統發出通知，以安排必要的行動[161]。

SmartHome 之產品包括電燈、煙霧感測器、攝影機等，在使用過程中雖不會直接蒐集個人資料，但為提供個人化服務，其仍會蒐集個人使用習慣相關資料，以持續改善平台服務並保證服務品質。然而，其所蒐集之資料僅為匿名資料，且德國電信僅在 SmartHome 使用者同意時方能近用所蒐集之資料，以進行必要之故障排除。當該服務涉及第三方時，德國電信會透過發送電子郵件取得使用者明確同意後，以設備序號資料等方式，有限地將資料傳送給第三方合作廠商，以進行必要之維護作業。

二、 相關標準及法規

德國於 2021 年 5 月通過新的電信現代化法（Telekommunikationsmodernisierungsgesetz, TKMoG）[162]，大幅度修正原先之電信法（Telekommunikationsgesetz, TKG）。電信現代化法調整歐盟現有之電子通訊法律框架，並針對電信監管框架進行全面性修正，目的在於促進超大容量網路（Very High Capacity Networks, VHCN）擴展，同時設計有利於投資的管制獎勵措施，希望在保持網路和服務的可近用性和安全性之餘，能夠提高共同合作及投資的意願，並增加終端使用者的利益。修法重點在於：

1. 將適用範圍擴展到其他服務提供商：電信現代化法將應用範圍擴展到人際電信服務（interpersonal telecommunications services）。因此，過去不屬於電信業者定義的 OTT 服務（Over-the-top media services, OTT services）服務提供商，亦將納入監管範圍，包括電子

[161] More partners, more devices, more security – Deutsche Telekom spices up Magenta SmartHome, Deutsche Telekom AG, https://www.telekom.com/en/media/media-information/consumer-products/-deutsche-telekom-spices-up-magenta-smarthome-501526 ; SmartHome Schutzbrief, Deutsche Telekom AG, https://www.smarthome.de/ideen/smarthome-schutzbrief (last visited July 20, 2021).

[162] Fedral Ministry for Econmic Affairs and Energy, Telekommunikationsmodernisierungsgesetz (Feb. 24, 2021), https://www.bmwi.de/Redaktion/DE/Artikel/Service/Gesetzesvorhaben/telekommunikationsmodernisierungsgesetz.html (last visited Aug. 6, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

郵件服務、可穿戴式設備，以及其他 OTT 應用程式，例如音頻、影片和其他透過網路傳輸的串流媒體內容。

2. 超大容量網路（VHCN）獎勵措施：該法加速 VHCN 擴展的核准程序以及新的監管原則，目的在於推動對 VHCN 的投資，確保在快速和廣泛部署網路時有適合的寬頻網路。
3. 加強消費者的權利：該法將有關消費者保護的適用範圍擴展到 OTT 服務，新增透明度義務和有關契約修改的規則。
4. 對高風險場域的 ICT 安全要求增加（尤其針對新電信技術，例如 5G）：包括加入「關鍵電信零件」（critical telecommunications components）的概念，意即針對零組件建立官方認可或認證機構測試和認證的可信賴聲明。德國聯邦網路局（Bundesnetzagentur, BNetzA）提出安全要求框架（Catalog of Safety Requirements），包括確定電信服務提供者潛在風險的標準，使用適當的入侵偵測（intrusion detection systems, IDS）及攻擊偵測（attack detection systems, ADS）系統。

德國聯邦參議院於 2021 年 5 月 28 日通過電信與電子媒體資料與隱私保護法（Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien, TTDSG），目的在於保護數位世界中的資料隱私，並平衡數位服務使用者利益與公司經濟利益，解決因電信法、電信媒體法（Telemediengesetz, TMG）與 GDPR 同時並行，使消費者、電信服務提供者以及監管機關不確定如何適用上開法律之情況。電信與電子媒體資料與隱私保護法第 3 條至第 8 條規定電信內容的保密義務及須遵守保密義務之對象，並禁止電信系統濫用。關於交通位置資料之使用範圍，則規定於該法第 9 條至第 13 條，並應符合 GDPR 第 6、7 條之要求。該法第 25 條規定保障對終端使用者設備的隱私保護，原則上第三方只能在終端使用者同意的情況下，在終端設備上存儲 cookies 等資料[163]。

[163] DEUTSCHER BUNDESTAG, Datenschutz und Schutz der Privatsphäre in der Telekommunikation (Mar. 25, 2021), https://www.bundestag.de/dokumente/textarchiv/2021/kw12-de-datenschutz-telekommunikation-826510; BUNDESMINISTERIUM FÜR WIRTSCHAFTS UND ENERGIE [BMWi], Gesetz zum Schutz der Privatsphäre in der digitalen Welt beschlossen (May 28, 2021), https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2021/05/20210528-gesetz-zum-schutz-der-

本報告之智慧財產權屬於國家通訊傳播委員會

第三節 美國

一、 應用案例

(一) T-Mobile 個人化廣告行銷

T-Mobile 自 2021 年 4 月起推出個人化廣告推播，透過業者的蜂巢網路即可知道使用者網路瀏覽紀錄及應用程式使用紀錄，以及撥打的電話。除非使用者自行退出，否則都將進行個人化廣告推播。T-Mobile 直接透過使用者 T-Mobile 帳號自動蒐集使用其產品或服務之相關網路資料，亦蒐集來自其他合作第三方（例如金融或信貸機構），透過使用或組合資料分析出個人偏好，以進行個人化精準行銷。

T-Mobile 所蒐集資料包括使用者所提供之聯絡資料及帳號資料（例如姓名、使用者名稱、密碼、地址、電話號碼、電子郵件及家庭成員）、身分認證及安全資料（例如身分證、社會安全碼及簽名）、人口統計資料（例如年齡、性別、退伍軍人身分及生日）、付款資訊（例如信用卡及銀行帳號）、個人偏好資料（包括行銷、廣告、通訊或其他參與 T-mobile 計劃的偏好），以及其他調查資料（例如參與之問卷調查或促銷活動）；自動蒐集的個人資料包括透過語音服務生成的使用者專用網路資料（customer proprietary network information, CPNI）、透過追蹤技術所蒐集之唯一識別碼（unique identifiers）（例如 cookie、設備 ID、IP 位址等）、設備及服務性能診斷資料、備份資料、商業資料（例如產品購買紀錄）、地理位置資料、生物特徵資料、影像及聲音資料。共享資料方面，T-Mobile 會透過書面、線上或取得使用者之同意才向第三方提供資料，包括 T-Mobile 品牌與公司之間、提供福利之第三方、其他身分驗證或詐騙預防單位、

privatsphaere-in-der-digitalen-welt-beschlossen.html (last visited Aug. 13, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

來電顯示服務提供商、公司業務所需之交易或轉讓方。並會遵守法律、法規或其他合法要求以保障 T-Mobile 使用者之權益及財產安全[164]。

T-Mobile 聲明並非直接識別個人資料，而是將大量匿名使用者資料聚集後將個人分配唯一識別碼，並根據資料分析出使用者興趣或人口統計資料，將其資料提供給第三方廣告商，意即第三方業者並不會取得個人真實資料。由於 T-Mobile 蒐集之資料具體程度，導致可能很容易透過分析比對重新識別個人身分。因此，電子資訊隱私中心（Electronic Privacy Information Center, EPIC）總裁警告 T-Mobile 此次計畫仍被認為比以往電信業者之資料蒐集更具侵略性，FCC 應重新定義寬頻服務提供業者在共享資料之相關規範，後續發展仍值得持續關注[165]。

(二) ATIS 與 US Ignite 提出智慧城市資料治理政策白皮書

美國電信產業解決方案聯盟（Alliance for Telecommunications Industry Solutions, ATIS）與 US Ignite 非營利組織於 2021 年 5 月發布「智慧城市資料治理政策：建立與城市合作夥伴的資料共享基礎」（Smart City Data Governance Policies: Creating a Foundation for Data Sharing with City Partners）白皮書，藉由深入了解城市的主要資料政策及挑戰後，建立有效的資料管理共享規則與程序來解決，並從 COVID-19 大流行的經驗中學到關於城市資料處理的經驗，包括資料完整性、透明度、隱私和同意的可擴展資料策略等，以幫助未來城市在尋求優化資料資產管理和共享時，能夠做出更好的決策[166]。

---

[164] T-Mobile Privacy Notice, T-Mobile Privacy (May 5, 2021), https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (last visited Aug. 13, 2021).

[165] Sara Morrison, How your mobile carrier makes money off some of your most sensitive data, Vox (Mar. 13, 2021), https://www.vox.com/recode/22325420/t-mobile-verizon-att-ad-targeting-data (last visited Aug. 20, 2021).

[166] ATIS – US Ignite Smart City Data Governance Policies Create a Foundation for Data Sharing with City Partners, ATIS (May.27, 2021), https://www.atis.org/press-releases/atis-us-ignite-smart-city-data-governance-policies-create-a-foundation-for-data-sharing-with-city-partners/ (last visited June 20,

本報告之智慧財產權屬於國家通訊傳播委員會

根據本白皮書的調查，目前在推動智慧城市資料治理政策所面臨的主要挑戰在於[167]：

1. 執行政策的主導單位和問責制度
2. 跨機構/轄區資料共享協議
3. 資料共享政策之實際執行
4. 多種資料來源彙整與公開
5. 資料管理者、資料科學家和其他必要的人員參與制定資料政策，以滿足未來應用需求
6. 根據 COVID-19 疫情調整工作和預算需求，確立資料應用規劃與優先順序

因此，本白皮書建議資料政策必須從開放的資料共享發展轉為與第三方合作提供一個有效的平台。資料的快速增長將需要新的資料治理方法，應透過隱私、保密、同意和其他資料分析和學習技術，在城市和社區之間建立可信賴的應用，確保針對單一資料集和從多個來源聚合的資料集能夠符合隱私要求。透過資料終端使用者反饋從中評估資料的價值及可用性，以在未來做更有效的資源分配[168]。

二、 美國電信網路應用規範

美國針對電信業者使用消費者個人資料及隱私保護主要規定於電信法（Telecommunications Act of 1996），目的在於促進競爭並鼓勵科技發展，採取較彈性之監管方式。依據電信法第 222 條規定，電信業者有義務保護消費者資訊隱私。在資料蒐集方面，除非符合法律規定或取得客戶同意，否則僅能在提供電信服務的範圍內使用客戶專線資訊。但是如果移除客戶識別資訊，則例外可以在電信服務為目的以外利用。根據電信法第 702 條規定，電信服務業者應依使用者要求方能向第三方業者提供其個人專有資料，但電信業者有責任保護其他營

2021).

[167] Smart City Data Governance Policies: Creating a Foundation for Data Sharing with City Partners, ATIS – US Ignite, May 27, 2021, at 6.

[168] *Id*. at 9.

本報告之智慧財產權屬於國家通訊傳播委員會

運商、設備製造商和使用者的專有資料及個人資料之機密性[169]。

第四節 英國

2020 年 9 月英國透過「國家資料戰略」（National Data Strategy）期能釋放資料潛力，推動更好、更安全、更具創新性的資料應用，改善社會公共服務，使英國成為資料驅動創新的領導者。同時考量脫離歐盟後的國際定位，持續發會對於全球資料共享和應用之影響力。而值得關注的是戰略中關於資料共享應用的具體行動，即為「智慧資料」（Smart Data）計畫，獲得企業或消費者同意，讓受信任的第三方協助進行資料近用，不僅改善消費者體驗，也能減少企業進入特定市場壁壘，以促進創新與公平競爭。

Smart Data 計畫先導案例為金融產業之「開放銀行」（Open Banking），從 2020 年至今已超過 300 萬消費者和中小企業，透過開放銀行應用來節省時間成本，消費者也願意使用開放銀行來獲得債務建議與其他多元服務。英國政府現階段亦正在著手評估立法，擴大政府部門參與 Smart Data 權限，使得其他產業之消費者和中小企業得以享有資料共享之益處，並思考衡平隱私保護與資料價值提升。

除了前述開放銀行，2020 年 8 至 11 月英國通訊傳播管理局（The Office of Communications, Ofcom）針對「開放通訊：使人們能夠透過創新服務共享資料」（Open Communications: Enabling people to share data with innovative services）進行公開意見徵詢，使消費者能簡單安全共享通訊資料給獲授權第三方，同時消費者應有控制權利。以下蒐整關於英國電信業者資料在創新應用之產業發展之應用案例，與英國政府資料應用政策趨勢研析。

一、 應用案例

(一) Ofcom 開放通訊第三方服務提供案例

Ofcom 開放通訊諮詢報告中，關於第三方服務提供案

[169] S.652 - Telecommunications Act of 1996.

本報告之智慧財產權屬於國家通訊傳播委員會

例，提出以下四項服務提供類型，雖然目前尚未實行，但對於電信業者後續因應開放通訊應用從消費者角度出發，所推出之服務亦得參考：

1. 產品服務之比較推薦：消費者直接與其他業者共享其資料，接收適合其需求的產品服務建議。
2. 帳戶整合：整合消費者在不同業者間所擁有的帳戶和產品的資料，甚至是公用事業繳費資料等；幫助消費者管理和掌握其通訊服務相關帳戶，開放銀行也有類似服務模式，且應獲其同意與第三方持續共享資料。
3. 帳戶管理：協助消費者在接近服務契約終止或價格上漲時，提醒消費者，並結合產品服務之比較推薦，提供消費者後續選擇；應獲消費者同意與第三方持續共享其資料。
4. 協助財務困難的消費者：若有財務困難消費者選擇透過如慈善機構、資產管理等第三方尋求幫忙，並與第三方共享其資料。

而該諮詢於 2020 年 11 月結束後， Ofcom 於 2021 年年 7 月 7 日發布聲明表示[170]，受訪者對開放通訊的看法分歧，支持建立開放通訊利用資料進行創新，而消費者團體一致認為，這將有助於消費者找到更適合他們需求的服務；但也有部分意見並不支持監管干預。受訪者普遍支持諮詢中提出的原則，但對於需要哪些通訊服務業者讓客戶能夠共享有關其服務的資料，亦存在不同的看法。許多提供意見之消費者團體和數位比較工具業者都同意 Ofcom 在諮詢中概述的潛在好處。然而，大多數服務提供者不同意，或認為這些好處可能並不顯著，且有風險存在與成本問題，並認為是否可以提供準確服務還為時過早。至於開放通訊後續規劃，目前英國政府考慮朝向立法模式進行，以利於在不同領域

[170] Statement: Open Communications – Enabling people to share data with innovative services, Ofcom, https://www.ofcom.org.uk/consultations-and-statements/category-1/open-communications (last visited July 29, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

能夠推動 Smart Data 計畫。因此 Ofcom 將待相關立法，始推動後續措施。若立法賦予 Ofcom 實施資料移動性的具體權力，此諮詢回應意見將作為 Ofcom 在電信和付費電視市場資料移動性後續推動依據。Ofcom 也是政府 Smart Data 工作小組的成員，將持續評估借鏡其他部會的資料移動計畫。

(二) EE 電信推出之數位身分平台（Digital Identity platform）

2020 年英國 EE（Everything Everywhere）電信公司推出之數位身分平台（Digital Identity platform）提供身分認證[171]，以防止欺詐並促進客戶交易安全。數位身分為其母公司英國電信集團 BT（British Telecom, BT）創新計畫之重點。平台協助英國銀行避免 SIM 卡偷換（SIM Swap）之詐騙攻擊，亦即帳戶接管詐欺[172]，詐騙手法是透過 SMS 或撥打電話方式進行，利用電信營運商將受害人的電話號碼移植到另一張 SIM 卡，常發生在客戶手機被偷的情況。

為因應身分詐欺，EE 數位身分平台之 SIM Swap checker 使企業能夠了解客戶 SIM 卡上次更換之時間，判斷是否可能有潛在欺詐風險。對於銀行而言，此類資訊將得以用於停止金融交易，直到完成身分確認。此外平台之來電轉接（Call Divert）功能，得確認是否設置轉接，避免轉接到欺詐電話。

銀行相當重視 KYC（Know your customer），亦即確認客戶之身分，常用於合規與反洗錢的方面，該平台也有設計此項功能，防止欺詐帳戶註冊，銀行可以將新客戶資料與 EE 資料庫中進行比對，確認手機是否已報失或被盜，進而確認客戶的身分真實性。

---

171 EE, EE Launches Identity Checker to Help Business Protect Customers Against Fraud, https://newsroom.ee.co.uk/ee-launches-identity-checker-to-help-businesses-protect-customers-against-fraud/ (last visited June 25, 2021).

172 Federal Trade Commission, SIM Swap Scams: How to Protect Yourself, https://www.consumer.ftc.gov/blog/2019/10/sim-swap-scams-how-protect-yourself；Federal Communications Commission, Cell Phone Fraud, https://www.fcc.gov/consumers/guides/cell-phone-fraud (last visited June 25, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

BT 與 EE 將持續致力以創新幫助保護客戶免受欺詐，並且已與銀行、電子商務和遊戲多個產業密切合作，以保護交易安全，讓英國消費者可以安心進行線上交易。

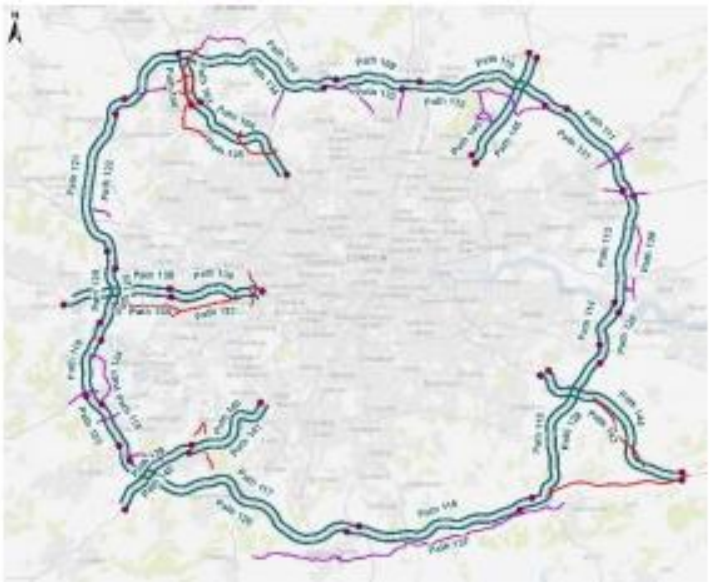
(三) EE 電信與 Atkins 於 M25 公路之電信與交通大數據應用

2014 年 EE 電信與 Atkins 工程公司合作監控 M25 高速公路上交通流量，該路段經過機場、工業區，且是民眾通勤要道等，亦即從地理空間的角度將英國最繁忙的高速公路路段與行動網路同步，優化英國道路使用者駕駛體驗[173]。EE 將電信資料經過匿名處理，以保護用戶隱私，並將其轉化為可分析資料。Atkins 也可以應用分析資有效地規劃道路工程的時間安排，以保持高速公路的暢通。

透過逐步改善使資料輸出與驗證資料集間正相關性提出解決方案。最初是在 M25 高速公路（M25 motorway，或稱倫敦外環高速公路 London Orbital motorway）上使用自動車牌辨識（Automatic number-plate recognition, ANPR）攝影機來計算行程時間，但此方式不僅耗費成本，也會增加道路基礎設施，同時可能造成安全問題，如人員路邊進行安裝的安全性和持續維護成本，因此最終並未採用此方式。為了提供更具成本效益和安全性的行程時間計算解決方案，Atkins 和 EE 合作使用 EE 資料並將其與 Atkins 的地理空間、運輸資料分析結合，以提供旅程時間（參圖 14）。

[173] The Telegraph, The Atkins-EE partnership: using big data to solve infrastructure problems, https://www.telegraph.co.uk/education/stem-awards/design/atkins-ee-big-data-partnership/ (last visited June 26, 2021); Atkins, M25 MOBILE PHONE DATA JOURNEY TIMES, https://datainsights.atkinsglobal.com/assets/pdf/Case_Study_M25_V03.pdf (last visited June 26, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會



資料來源：本計畫編譯自 M25 mobile phone data journey times

圖14　M25 電信與交通大數據應用

該服務提供超過 3 年每天 16 小時的旅程時間資料，獲得英國公路局（Highways England）認可，未來將持續協助改善 M25 公路交通。

二、　資料經濟政策趨勢：國家資料戰略與智慧資料計畫

國家資料戰略從去年發布至今，配合公眾意見諮詢滾動調整，整體架構維持由下而上（參圖 15），透過 4 大支柱，包含資料基礎（Data foundations），亦即資料在完備基礎上，始能真正發揮其價值，如標準格式、能因應未來發展的機制，且容易查找、可近用性、具互操作性，並得再利用；資料技能（Data skills）則是確保人民具備應用資料相當技能，所學具持續發展性；資料可用性（Data availability），確保資料得適當近用、移動和再利用，並鼓勵公私部門與第三方間共享資料，以及國際資料流通的適當保護；負責任的資料（Responsible data）確保以合法、安全、公平、倫理、可持續和負責任利用資料，並支持創新與科學研究。

戰略架構中層則是五項優先行動任務，包含釋放整體經濟中資料的價值、確保促進持續增長與可信賴的資料機制、改變政府資料利用以提高效率和改善公共服務、確保資料基礎架構的安全性和韌性，以

本報告之智慧財產權屬於國家通訊傳播委員會

及促進國際資料流通，期能掌握創新的機會，包含促進生產力和貿易、支持創新和相關工作機會、提高科學研究效率和範圍、推動更好政策和公共服務，以及為所有人創造更加公平的社會。



資料來源：本計畫編譯自英國國家資料戰略

圖15　英國國家資料戰略整體架構

從上述可知英國對於資料應用策略框架，而戰略中資料可用性為促進公私部門、第三方間適當資料近用、移動和再利用。英國政府針對消費者利益在特定領域資料共享，如在開放銀行與 Smart Data 計畫於電信、能源等應用。Smart Data 計畫使消費者能與獲授權的第三方簡單、安全地共享資料，從而使第三方服務提供者（third party service provider, TPPs）能提供創新服務。前述提到之先導案例即為「開放銀行」（Open Banking），透過具互操作性格式和資料流通，使創新服務得以發展並促進競爭。Ofcom 於 2020 年開放通訊意見徵詢，開放通訊將使消費者能將通訊資料與獲授權第三方簡單安全地共享。消費者能控制其所共享之資料，並得要求業者共享更多有關產品或服務的相關資料，確保任何經認可第三方都得依消費者的要求近用資料。

本報告之智慧財產權屬於國家通訊傳播委員會

Ofcom 下一步將持續與利益相關者溝通，也將思考訂定相關規範，以及確保資料移動安全性與消費者控制權限，並期能循序漸進開放資料，如風險低但對消費者有較高利益的資料。此外，英國資料保護法參照 GDPR 資料可攜權規定，而 Smart Data 亦可謂對資料可攜權擴展，提供共享消費者資料框架。戰略考量未來將進行立法，作為所有 Smart Data 計畫法律依據。

2021 年 6 月智慧資料工作組提出之春季報告(Smart Data Working Group: Spring 2021 Report）[174]。首先，更新關於 Smart Data 在銀行、金融、通信和能源領域的潛在優勢與案例，並探討 Smart Data 使用者所面臨挑戰。針對開放通訊部分，Ofcom 將在 2021 年夏季更新，就開放通訊實施最終決定前進行進一步磋商。其次，提出跨部門協作建議，將有助於為未來政策制定。其中關於跨部門協作原則，包含部門合作、開發 Smart Data 生態系統、實現互操作性、Smart Data 框架的持續發展，確定具體的協調領域，目前 Smart Data 計畫是不同領域獨立發展，由英國商業、能源暨工業策略部（Department for Business, Energy and Industrial Strategy, BEIS）負責 Smart Data 政策協調，報告也提出了三種不同的組織調整之選項，以協調層級的形式發展當前的跨部門工作組安排，為跨部門協調創造更多機會，包含沿用現有 Smart Data 跨部門工作組規劃，主要是政府和監管機構間就跨部門問題討論；其二，建立跨部門 Smart Data 委員會，具有廣泛跨部門成員自願性參與，提供跨行業、消費者利益和技術專家參與；其三，成立董事會來領導 Smart Data 委員會，就跨部門問題向政府提供意見和建議，但這也是最耗費資源，但得以實現更好的溝通協調。工作組目前仍在尋求對上述建議以及該跨部門安排之意見，而利益相關者的初步意見傾向設置 Smart Data 委員會，但尚未定案，工作組期能 2021 年 7 月底能蒐集更廣泛意見。至於 Smart Data 下一步規劃，將持續致力於 Smart Data 之相關立法，並將於年底發布更新報告。

綜上，英國國家資料戰略作為整體推動方向，Smart Data 計畫作

[174] Department for Business, Energy & Industrial Strategy, Smart Data Working Group: Spring 2021 report, https://www.gov.uk/government/publications/smart-data-working-group-spring-2021-report (last visited June 20, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

為英國共享消費者資料框架，透過資料賦權使消費者應對未來更多元跨域資料應用情況下，都能掌握自己的資料也能從中獲益，同時第三方業者亦得開展出不同的資料商業模式與服務。除了 Smart Data 計畫，英國政府也考量資料對於數位市場競爭，還有政府開放資料對於民間影響，並發展從公私資料中獲取價值的共享模型。

第五節 日本

2016 年日本第五期科學技術基本計畫提出超智慧社會（Society 5.0）之概念[175]，同時為促進公私部門間資料開放與流通，推動官民資料活用推進基本法施行。2021 年第六期科學技術基本計畫亦持續的建立資料治理規則與整備資料流通環境[176]。鑑於公私部門間資料開放逐漸活躍，於促進資料流通背景下，以下就日本電信服務業者透過資料加值進行之創新應用案例說明。

一、 應用案例

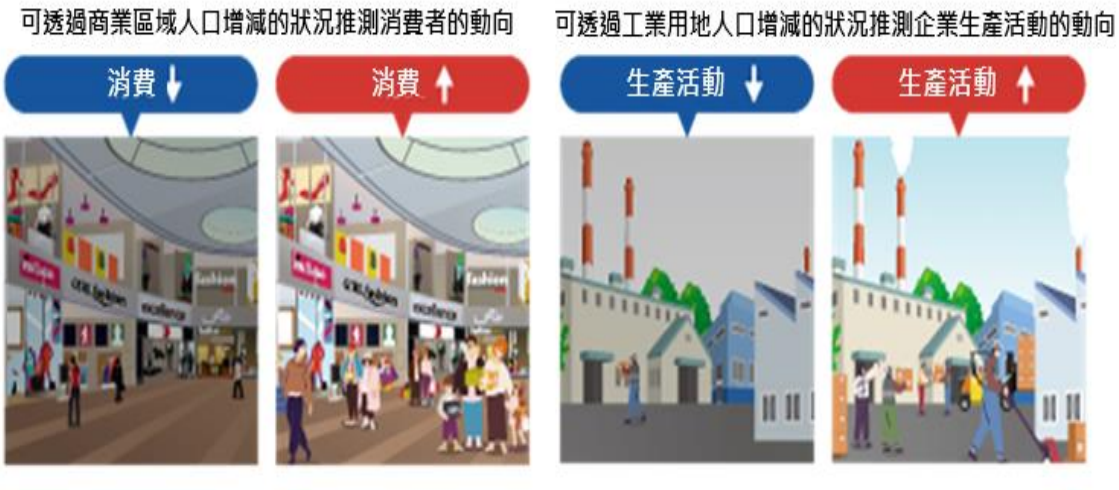
(一) NTT Docomo 行動空間統計應用於人流與消費預測

NTT Docomo 公司與三井住友資產管理公司（三井住友 DS アセットマネジメント株式会社），於 2020 年 11 月簽訂將 NTT Docomo 公司所持有之統計資料，運用於投資信託之商業聯盟契約。由 NTT Docomo 公司提供替代資料（Alternative data）[177]予三井住友資產管理公司，以提高投資信託之效能。行動空間統計[178]即利用 NTT Docomo 行動電話網路之使用資料，來掌握每個區域之人口分布和年齡組成等，亦可使用商業設施區域之人口增減資料來預測個人消費動向。目前行動空間統計已應用在三井住友資產管理公司之公募型投資信託「資料戰略分散基金」（データ戦

[175] 同前註 53。
[176] 同前註 55。
[177] 係指應用於投資判斷之資料一般傳統可公開資料以外之資料。
[178] 為保護隱私，使用的資料將會經過非識別化處理、群集資料（Aggregate data）、保密處理。行動空間統計僅係對群體人數進行人口統計，並不會特定客戶之身分。

本報告之智慧財產權屬於國家通訊傳播委員會

略分散ファンド）[179]。未來 NTT Docomo 公司將會持續推動為客戶提供高附加價值服務[180]（參圖 16）。



資料來源：本計畫編譯自 NTT Docomo

圖16　行動空間統計運用意象圖

(二) NTT Docomo 高鐵車廂內動態戶外廣告

NTT Docomo 公司、埼玉高速鐵道公司（埼玉高速鉄道株式会社）、BiZright Technology 公司（株式会社ビズライト・テクノロジー）與 LIVE BOARD 公司（株式会社 LIVE BOARD），於 2019 年 11 月運用車廂內之數位動態車輛螢幕（Dynamic Vehicle Screen），共同推動因應環境變化而即時變動廣告內容的動態戶外廣告（Digital Out Of Home, DOOH）[181]（參圖 17）。

此案例中 BiZright Technology 公司會在車廂內數位螢幕上設置相機與 IoT 感測設備，蒐集溫度、濕度等車廂內狀

[179] 係以日本美國公司、債券等作為投資對象之分散型投資信託。
[180]〈（お知らせ）ドコモが三井住友 DS アセットマネジメントとドコモ統計データの投資信託への活用に関する業務提携に合意-取組み第一弾として「モバイル空間統計」を投資信託の運用に活用-〉，株式会社 NTT ドコモ，2020/12/01，https://www.nttdocomo.co.jp/info/news_release/2020/12/01_01.html（最後瀏覽日：2021/08/12）。
[181]〈（お知らせ）NTT ドコモ、埼玉高速鉄道、ビズライト・テクノロジー、LIVE BOARD 世界初、鉄道車両内でのダイナミック DOOH 事業を共同で推進〉，株式会社 NTT ドコモ，https://www.nttdocomo.co.jp/info/news_release/2019/11/11_00.html（最後瀏覽日：2021/08/12）。

本報告之智慧財產權屬於國家通訊傳播委員會

況資料，還有擁擠狀況、性別、年齡等與乘客相關之資料，藉著邊緣人工智慧（Edge AI）解析，因應環境變化在車廂內播放廣告。NTT Docomo 公司之長期演進技術（Long Term Evolution, LTE）電路可蒐集車輛外之天氣與災害等資料，並即時在數位動態車輛螢幕播放即時資料。此外，LIVE BOARD 公司將運用 NTT Docomo 公司行動電話網路之運行資料所獲得之人口統計、行動空間統計[182]等資料，依廣告觀看數量計算廣告費用、播放時段。2020 年 4 月埼玉高速鐵道全部的車廂已設置數位動態螢幕[183]。



資料來源：NTT Docomo

圖17　車廂內之數位動態車輛螢幕

[182] 同前註 178。
[183] 同前註 181。

本報告之智慧財產權屬於國家通訊傳播委員會

(三) NTT Docomo 行動空間統計應用於提升購物便利性之區域循環巴士

NTT Docomo 公司、伊藤洋華堂公司(株式会社イトーヨーカ堂)與 YOU'S 公司（ユーズ株式会社），於 2020 年 9 月共同對伊藤洋華堂公司所營業之購物中心 Ario 葛西（アリオ葛西）與其周邊區域，結合免費循環巴士進行實驗（參圖 18）。此服務係藉由提供人口分布之行動空間統計[184]，找到大眾運輸需求較高之區域，如高齡者或育兒家長等，並在該區域免費行駛，並提升購物便利性，協助店舖招攬客人[185]。



資料來源：NTT Docomo

圖18　行動空間統計應用於提升購物便利性區域循環巴士

[184] 同前註 178。

[185] 〈買い物の利便性を向上させる地域循環バスの実証実験を開始～「モバイル空間統計」を活用し、高齢者や子育て世代のバス利用の需要を発見～〉，株式会社 NTT ドコモ，2020/08/24，https://www.nttdocomo.co.jp/binary/pdf/info/news_release/topics_200804_01.pdf（最後瀏覽日：2021/08/12）。

本報告之智慧財產權屬於國家通訊傳播委員會

前述關於 NTT Docomo 公司應用案例，在個人資料保護方面，制定個人資料保護憲章[186]，與個人資料隱私政策[187]；以及行動空間統計之資料製作步驟[188]，以及行動空間統計指引[189]，已於前述關於人口流動統計服務[190]應用案例說明。

二、 相關法規

2021 年日本政府因應數位社會形成基本法之制定（デジタル社会形成基本法）修正個人資料保護法，使全國、地方政府與民間適用統一之個人資料保護規範。以下分別說明關於 2020 年與 2021 年個人資料保護法之重要修正。

(一) 2020 年（令和二年）個人資料保護法修正

日本國會於 2020 年 6 月通過「個人資料保護法修正案[191]」（個人情報の保護に関する法律等の一部を改正する法律），將於 2022 年 4 月施行。本次修法旨在強化當事人對個人資料保護之意識、衡平資料創新應用與個資保護，以及因應跨境資料流通伴隨的新型風險[192]相關措施。以下說明本次主要修法重點內容：

1. 強化當事人對個人資料之權利

本次修法大幅強化當事人對個人資料之權利。除了擴大個人資料停止利用與刪除請求權之範圍，亦放寬當事人在個人權利或正當利益受侵害之虞時，得行使個人資料停止利用與刪除請求權。資料揭露方法也由原先以書面交付為原則，修正為得依當事人指定之方式揭露，並可要求以電磁紀錄方式為之。當事人得請求業者揭露將個

186 同前註 88。
187 同前註 90。
188 同前註 91。
189 同前註 96。
190 同前註 87。
191 個人情報の保護に関する法律等の一部を改正する法律案，法律第四十四號（令和二年˙六˙十二）（2020）。
192〈個人情報の保護に関する法律等の一部を改正する法律〉，個人情報保護委員会，頁 4-5，https://www.ppc.go.jp/files/pdf/200612_houritsu.pdf（最後瀏覽日：2021/08/15）。

本報告之智慧財產權屬於國家通訊傳播委員會

人資料提供予第三方之紀錄。而於 6 個月內刪除之短期持有個人資料，經修正後亦係屬第 2 條第 7 項所定義之「持有個人資料」範疇，當事人得請求揭露與請求刪除[193]。另外也強化對「選擇退出」(opt out)[194]規定之限制，就業者因不當方法取得個人資料，以及基於 opt out 相關規定得提供個人資料之例外情形，進行調整[195]。

2. 加重業者責任義務

本次修法新增業者發生個人資料洩漏時，對當事人個人權利造成危害之虞時，應向個人資料保護委員會報告並向通知當事人。並新增本法 16 條之 2 將「業者不得以助長違法或具不當行為疑慮之不當方法，利用個人資料」明文化[196]。

3. 鼓勵業者自主取得個人資料保護制度認證

原先團體制度認證，僅能使業者以全體部門進行認證，本次修正使業者亦能以特定部門進行團體制度認證[197]。

4. 新增假名化加工資料規範促進資料利用

「假名化加工資料」係為確保個人資料一定之安全性與功能，較匿名加工資料更為簡單之加工方式，得以確保

---

[193] 依修法前個人情報の保護に関する法律第 2 条第 7 項：「在本法律中，所謂『持有個人資料』係指個人資料處理業者具有可以執行公開、修訂內容，追加或刪除、停止使用、消除及停止提供第三方之權限的個人資料，政令所規定之表明其存在與否時會有損公益及其他利益之內容或一年以內之政令所規定的期間以內必須消除之內容以外的內容。」再依修法前個人情報の保護に関する法律施行令第 5 条：「個人資料保護法第 2 條第 7 項所規定之政令期間為 6 個月。」故修法前對「持有個人資料」之定義，並不包含 6 個月內刪除之短期持有個人資料。惟 6 個月內刪除之短期持有個人資料，若遭到洩漏，仍會對當事人造成無可回復之損害，故此次修法刪除個人情報の保護に関する法律第 2 条第 7 項之「一年以內之政令所規定的期間以內必須消除之內容」文字，使 6 個月內刪除之短期持有個人資料，亦包含在「持有個人資料」之定義下，當事人得請求揭露與刪除。

[194] 是指個人資料處理業者向第三方提供個人資料，因應當事人的要求，停止向第三方提供可識別當事人之個人資料的情形。若根據個人資料保護委員會所規定的規則，事先通知當事人或置於當事人容易得知的狀態，同時向個人資料保護委員會申報時，則例外可向第三方提供該個人資料。

[195]〈個人情報の保護に関する法律等の一部を改正する法律について〉，個人情報保護委員会，2021/04/27，頁 8，https://www.soumu.go.jp/main_content/000747671.pdf（最後瀏覽日：2021/08/15）。

[196] 同前註 195，頁 9-10。

[197] 同前註 195，頁 11。

本報告之智慧財產權屬於國家通訊傳播委員會

資料之活用與資料創新運用之需求。此次修正新增將姓名等刪除之假名化加工相關規定。僅限於內部分析使用等條件下，得緩和個人資料保護上揭露與停止利用請求等相關義務[198]。

5. 加重刑事之處罰

本次修正提高違反個人資料保護委員會命令之法定刑為 1 年以下有期徒刑或 100 萬日圓以下罰金，亦提高對委員會提出虛假報告之法定刑為 50 萬日圓以下罰金，並考量法人與個人間之資力差距，提高資料庫不當提供罪與違反委員會命令之罰金，大幅提高法人之罰金最高上限金額為 1 億日圓[199]。

6. 域外效力與跨境傳輸相關規範

本次修法亦使外國處理日本國內相關個人資料等業者，成為本法規範對象，並要求資料傳輸業者向外國第三方提供個人資料時，就個人資料處理之相關資訊，應告知本人資料轉移之國家以及該國對個人資料保護相關制度等資訊[200]。

(二) 2021 年（令和三年）個人資料保護法修正

日本國會於 2021 年 5 月通過「數位社會相關法律整備法」（デジタル社会の形成を図るための関係法律の整備に関する法律）[201]，需整備數位社會形成之相關法律，而個人資料保護法修正亦屬重點範疇，以下介紹此次促進資料流通之主要修法內容。

1. 統合並修正個人資料保護法相關法律

此次修法將「個人資料保護法」（個人情報保護法）、「行政機關個人資料保護法」（行政機関個人情報保護法）、

198 同前註 195，頁 13-15。
199 同前註 195，頁 19。
200 同前註 195，頁 21。
201 デジタル社会の形成を図るための関係法律の整備に関する法律，法律第三十七號（令和三年˙五˙十九）（2021）。

本報告之智慧財產權屬於國家通訊傳播委員會

「獨立行政法人個人資料保護法」（独立行政法人等個人情報保護法）三部法律統合為一部新個人資料保護法。同時整備地方政府個人資料保護制度，建立合於新法規定之全國共通性標準。隨著國家統一標準之建立，將由個人資料保護委員會進行統一監督國家、地方自治團體與民間對個人資料之利用[202]。

2. 統一個人資料定義並明確匿名加工資料規範

統一全國、地方政府與民間對個人資料定義[203]，使全國適用統一標準，便利資料流通。

隨著第五期科學技術基本計畫 Society 5.0 概念之提出，與第六期科學技術基本計畫延續打造 Society 5.0 之理想，2020 年日本對個人資料保護法修正，使資料創新應用與個人資料保護間得以取得平衡，並對跨境資料傳輸伴隨之新型風險做出應對措施。2021 年個人資料保護法修正則整合全國適用統一之個人資料保護規範，以促進資料流通環境逐漸完備。而前述關於 NTT Docomo 公司將行動空間統計多元創新應用於投資信託、戶外廣告與區域循環巴士上，未來隨著 5G 基礎建設之普及，與日本促進資料流通之環境逐漸完備，將發展出更多元應用。

第六節 韓國

一、 應用案例

(一) 巨量資料服務平台：Geovision、BigSight、U Cube

2020 年韓國國會通過包含「個人情報保護法」、「情報通信網法」、「信用情報法」等數據 3 法的修正案，於本次修

[202] 〈デジタル改革関連法案について〉，内閣官房 IT 総合戦略室，2021/03/03，頁 9，https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/dejigaba/dai14/siryou1.pdf（最後瀏覽日：2021/08/15）。

[203] 同前註 202，頁 13-14。

本報告之智慧財產權屬於國家通訊傳播委員會

法特別引進「假名情報」的概念，使個人情報處理者在兼顧資料運用與維護個人資料安全前提下，允許其得利用個人資料進行統計編製、科學研究或保存公益紀錄等，使個人資料的保護得以更加落實；而韓國的三大電信業者因應該次修法分別推出「巨量資料服務平台」，各電信業者以其所擁有之使用者電信資料為基礎，針對多方產業而提供相應之服務。

1. Geovision

   SK 電信（SK Telecom, SKT）與成立 Geovision（지오비젼）平台，連結基地台蒐集 SKT 用戶位置，據此分析各商圈的人口組成及流動，提供數據資料給異業進行包含不動產規劃等商業用途。

   2020 年 8 月 31 日，SKT 在由 Big Data UN Global Working Group 舉辦之「第六屆大數據國際會議」公布韓國政府利用 Geovision 促進 COVID-19 防疫的成果，主要內容為 SKT 無償提供慶北警察廳利用 Geovision 的流動人口分析服務，警察廳透過 Geovision 篩選出人口密度高的地區進行「定點巡邏」（핀 포인트 순찰），藉此降低人民外出活動並抑制 COVID-19 的擴散。

2. BigSight

   韓國電信（Korea Telecom, KT）設立 BigSight（빅사이트）平台，將蒐集的電信資料分別以觀光、商圈、生活人口及行銷等 4 大領域進行分析，並將分析成果商品化對外銷售；以觀光分析為例，觀光人口的報告顯示項目為訪問性別、年齡層、並分別以每月、每週，觀光客滯留時間、訪問率等統計資料，再以大數據分析位於濟州島數個著名觀光景點，並藉由觀光年齡層以推測旅遊傾向，透過大數據比較 COVID-19 發生前後，到濟州島觀光的年齡層及人次有顯著不同，進而篩選出人氣景點、新興觀光點等內容，提供在濟州從事商業行為者使用。KT 更

本報告之智慧財產權屬於國家通訊傳播委員會

以 BigSight 的分析成果為根基，成立 AI 專門公司（AI Company）將巨量資料集中於商業應用。

2020 年 6 月間，為因應 COVID-19 對經濟帶來的衝擊，BigSight 以 COVID-19 爆發前後一年之通信數據為基礎，對全韓國各地區的觀光及商圈進行分析，並將分析結果低價銷售予被視為嚴重受到 COVID-19 影響的教育機構、風險投資公司及一般中小企業，使這些產業得用這些數據資料投入開發新的服務及事業，適度緩解產業因疫情所受到的衝擊。

3. U Cube

LG U+[204]則選擇以自家的企業資源規劃系統 U Cube（유큐브）為基礎，與 LG CNS Co., Ltd. （隸屬於 LG 集團的子公司）、韓國金融保安院（금융보안원）合作，開發使用巨量資料的企業對企業（B2B）（business-to-business）服務，整合用戶的網路數據使用量及金融消費情報等設計適合各別客戶的產品，例如推出每月只要韓幣 7700 元（約為 181 台幣）即可享有智慧居家服務等[205]。

(二) SKT 之 T-map 道路導航系統及位置資訊服務

T-map（티맵）是 SKT 整合道路導航系統及位置資訊服務於 2007 年 7 月所推出，並於 2010 年開始提供行動裝置使用 T-map 服務。2021 年 1 月 1 日 SKT 將集團的行動事業部改組，另外成立 TMAP MOBILITY CO., LTD，負責推廣 T-map 業務；目前 T-amp 所提供的服務，除了一般的道路導航系統外，亦包含大眾交通運輸工具的時間資訊、事故易發生路段警示、測速照相機設置場所、叫車及代駕等服務。

T-map 為韓國最主要的導航服務系統，每月有效使用人

[204] LG U+（LG 유플러스）電信公司，為韓國樂金集團（LG）之子公司。

[205] 如「U+스마트홈」的多種消費方案可供 LG U+的用戶選擇適合的智慧居家服務。

本報告之智慧財產權屬於國家通訊傳播委員會

約有 1288 萬名，使用人只要透過手機下載 T-map 的 App，即可隨時隨地使用 T-map 所提供的服務；此外 T-map 會記錄每位使用人的行車習慣，透過分析行車習慣進行評分，使用人得透過評分了解自己的行車習慣。

T-map 除了提供使用人便捷的交通路線與方式外，使用人亦可透過網路連線隨時更新路況資訊，且 TMAP MOBILITY CO., LTD 進一步與保險公司合作，將其所有包含使用人的行車紀錄、習慣及評分等資料供保險公司進行分析及評估，以規劃出適合的汽車保險，並根據使用人的評分而給予保險費優惠，使用人只需要向保險公司投保時即可確認是否獲得優惠，亦可直接透過 T-map 的介面選擇最划算的汽車保險產品。

未來，T-map 規劃與仁川廣域市共同提出智慧停車的示範服務，使用人只要透過 T-map 即可確認停車位置、費率、自動結帳等服務，適度降低仁川廣域市管理公有停車場的人力。

(三) KT 與 BNK 合作推出貸款優惠

因應 COVID-19 對用戶所生之衝擊，KT 與韓國徵信中心（KCB）、BNK 釜山銀行及 BNK 資本等於 2020 年 4 月 22 日共同簽署合作意向書[206]，將由 BNK 集團旗下的銀行為 KT 的電信用戶提供優惠貸款服務，主要對象為主婦、學生、青年創業者等信用等級弱勢之族群。

由於 COVID-19 對經濟的影響，信用貸款需求增加，然而信用等級弱勢族群難以直接透過銀行申請貸款，因此 KT 將其用戶之通信費、商品內容、使用模式等電信資料以 AI 進行分析，進而整理出各用戶信用等級資訊，再由銀行與 KCB 合作，評估各用戶等級以規劃金融產品，使 KT 用戶

206 통신 정보 분석해 금융 혜택… KT, 부산은행 등과 MOU (2021/04/22)，https://biz.chosun.com/site/data/html_dir/2020/04/22/2020042201508.html（最後瀏覽日：2021/08/03）。

本報告之智慧財產權屬於國家通訊傳播委員會

中信用等級弱勢者得免去其他審核，輕易地獲得相應之優惠貸款服務。

二、 大數據個人資料保護準則

由於蒐集、利用電信用戶資料依法必須取得電信用戶之事前同意，而分析大量數據的從業者在取得事前同意較為困難，容易延伸對隱私權侵害的疑慮，因此，韓國放送通信委員會（방송통신위원회，以下稱 KCC）於 2014 年 12 月 23 日公布「大數據個人資料保護準則」（以下稱保護準則），作為處理大數據時兼顧個人資料保護與應用之具體性基準，以防範個人資料遭到誤用或濫用。

保護準則主要內容為以下五項：

(一) 自蒐集開始即應對可識別個人之資料進行徹底的去識別化措施

(二) 確保處理大數據之事實或目的等透明公開

(三) 個人資料經再識別後，應立即為廢棄或去識別化措施

(四) 禁止對敏感資料或通信秘密為蒐集、利用、分析等處理行為

(五) 對被蒐集的個人資料為保存或管理時，應實行技術性、管理性保護措施[207]

KCC 預期在保護準則施行後，可以有效掌握並監督利用大數據分析產業對個人資料保護的狀況，在兼顧保護個人資料的同時，有效提升大數據分析產業的發展性，期待大數據分析產業未來的活躍[208]。

第七節 小結

研究各國電信事業運用資料創新應用服務案例與其治理模式過程中，發現近年來電信業者積極投入發展大數據資料庫及 AI 領域，透過各種大數據分析成果，發展多元商業模式，如運用數據資料創新應用於交通運輸、人口流動分析、觀光旅遊、廣告行銷、身分認證、

[207] 例如設置阻斷侵入系統、防止存取紀錄被偽造及變造等措施。

[208] 정복덕，빅데이터, 수집 시부터 철저히 비식별화 조치해야，KCC，2014/12/23，https://www.kcc.go.kr/user.do?mode=view&page=A05030000&dc=K05030000&boardId=1113&cp=4&ctx=ALL&searchKey=ALL&searchVal=%EB%B9%85%EB%8D%B0%EC%9D%B4%ED%84%B0&boardSeq=40287（最後瀏覽日：2021/08/04）。

本報告之智慧財產權屬於國家通訊傳播委員會

金融服務如進行保險、貸款評估等領域。然而各國面臨不同挑戰需要解決，如愛沙尼亞國家資料庫中雖擁有大量個人資料，只要資料主體同意就有可能開放這些資料用於開發創新服務，但爭議在於無法得知此類服務是否將資料傳輸給第三方服務提供者。而德國則進行修法包含電信現代化法，希望保持服務可近用性和安全性，同時提高共同合作及投資的意願，並增加終端使用者的利益，還有針對電信與電子媒體資料與隱私保護法修法，解決電信法、電信媒體法與 GDPR 適用法律狀況。日本也有對個人資料保護法進行重大修正，使全國、地方政府與民間適用統一之個人資料保護規範。上開修正將有助於促進資料流通，有助於電信業者進行更多元之資料創新應用服務。而美國各州也有消費者隱私保護與逐步朝向聯邦個資法立法趨勢。英國以國家資料戰略推動，輔以 Smart Data 計畫促進英國共享消費者掌握自己的資料，其中電信也是英國推動重點領域，未來也將有相關立法因應跨域資料應用，並讓第三方業者得以近用電信資料開展出創新資料商業模式與服務。

前述異業資料應用結合，不僅對於消費者更加便利，對於大數據應用更是蓬勃發展，因此各國逐步推動關於個資法修法，甚至是政策立法趨勢朝向第三方近用資料，如英國 Smart Data 計畫、日本資料銀行，還有歐盟 2020 年提出之歐洲資料治理規則草案發展出資料中介機制亦相當值得參考，此外大數據資料之應用發展相對成熟，但相關立法仍待補足，如韓國放送通信委員會即透過訂定大數據個人資料庫保護準則，使電信業者在應用相關電信資料時亦能適度保護個人資料。因此短期建議如制定大數據創新應用相關指引準則，使電信業者有規範可循，以期減輕電信業者在處理大數據資料庫與個人資料保護時的矛盾，而中長期則應考量跨域資料應用之資料治理，甚至是第三方業者對於資料近用，亦得借鑒我國目前已進入第二階段開放銀行推動，另一思考面向是關於資料中介機制建構，以及促進當事人資料自主。

以下綜整各國電信事業運用數據資料創新應用案例，應用領域大致上得分為交通、人流分析、旅遊應用、廣告行銷、身分認證、金融

本報告之智慧財產權屬於國家通訊傳播委員會

服務，如保險評估、貸款等。

表 2 各國電信事業運用數據資料創新應用案例與相關法規配套整理

國家	應用案例	相關法規與配套
愛沙尼亞	• 交通應用：Telia 推出利用手機支付停車費的智慧停車系統 M-Praking • 城市規劃、交通、零售、旅遊應用：Telia 之人口流動分析（Telia Crowd Insights）	• 歐盟 GDPR • 電子通訊法
美國	• 廣告行銷：T-Mobile 推出個人化廣告推播	• 電信法
德國	• 智慧家庭：德國電信開發智慧家園求救系統識別家中危險發出警告	• 電信現代化法 • 電信與電子媒體資料與隱私保護法
英國	• 身分認證：EE 電信公司數位身分平台（Digital Identity platform），防止欺詐並促進客戶交易安全 • 交通應用：EE 電信與 Atkins 於 M25 公路之電信與交通大數據應用	• 國家資料戰略 • Smart Data 計畫 • 資料保護法
日本	• 人流與消費預測：NTT Docomo 異業合作，應用行動空間統計用於商業設施區域之人口增減資料來預測個人消費動向 • 廣告行銷：NTT Docomo 異業合作，應用人口分布行動空間統計，以及運用車廂數位動態螢幕推播因環境變化即時變動廣告內容 • 大眾運輸：NTT Docomo 跨界合作應用人口分布行動空間統計，解決大眾運輸需求	• 官民資料活用推進基本法 • 數位社會形成基本法 • 個人資料保護法
韓國	• 商圈人流分析：SKT 成立 Geovision 平台，提供數據資料供不動產規劃等商業用途 • 觀光、商圈、人口及行銷：KT 設立 BigSight 平台，將蒐集的電信資料分析，並將分析成果商品化銷售	• 個人情報保護法 • 情報通信網法 • 信用情報法 • 大數據個人資料保護準則

本報告之智慧財產權屬於國家通訊傳播委員會

國家	應用案例	相關法規與配套
	• 巨量資料分析：LG U+企業資源規劃系統 U Cube 異業合作，開發使用巨量資料的 B2B 服務，整合用戶的網路數據使用量及金融消費情報等設計適合各別客戶的產品 • 交通保險服務：SKT T-map 整合導航系統及位置資訊服務，T-map 透過記錄使用人行車習慣進行評分，與保險公司合作規劃出適合的汽車保險與保險費優惠 • 金融貸款服務：KT 與 BNK 集團合作推出貸款優惠	
我國	• 身分識別： TWID 身分識別中心和電信業者推動「Mobile ID 行動身分識別服務」，憑手機就能通過實名認證，完成銀行線上開戶、網路購物交易確認等 • 金融科技：國內首宗沙盒實驗成功案例由中華電信與凱基銀行合作，執行「實踐普惠金融首創電信行動身分認證」實驗計畫，身分認證流程優化，透過電信數據為未曾使用金融服務的人可以申請銀行服務 • 人流分析：人潮客群分析平台，掌握人流及統計型客戶輪廓資訊，景點遊客數量及活動人數統計	• 個人資料保護法 • 金融科技發展與創新實驗條例

資料來源：本計畫製作

本報告之智慧財產權屬於國家通訊傳播委員會

第四章 電信事業運用數據資料創新應用服務治理模式研析（網路公眾意見諮詢與 2 場實例分享座談會）

第一節 網路公眾意見諮詢

一、 工作內容

本工作項目為研擬並評估電信事業運用數據資料，提供創新應用服務治理模式之實際案例可能面臨之問題及建議解決方案，辦理一次諮詢期間為 14 天以上之網路公眾意見諮詢。

二、 工作項目

(一) 工作規劃

本團隊參考網路平台 vTaiwan、i-Voting 等彙整網路公眾意見之諮詢方式，架設問卷平台，蒐集公眾對於電信事業運用數據資料提供創新應用服務治理模式之意見，並透過本團隊（達文西個資暨高科技法律事務所、資策會科法所）官網及電子報、資策會官網及電子報、電腦稽核協會官網及電子報、臉書分享及 Line 群組轉傳等方式進行宣傳，廣邀對此議題有興趣民眾前往網站發表意見。

(二) 問卷內容

參考本研究國內外電信加值應用案例，讓網路公眾更加瞭解電信事業現行已運用或有意規劃之加值利用，及其資料運用、治理、保護與創新應用服務等實務情形，以問卷方式蒐集網路公眾對國內相關法令限制及挑戰、政府與企業責任、未來法規修正或決策流程等議題之相關意見。問卷內容請參考附錄 1：。

本報告之智慧財產權屬於國家通訊傳播委員會

(三) 諮詢期間及問卷數[209]

本次網路公眾意見諮詢於 110 年 7 月 19 日至 8 月 1 日間舉辦，共計 14 天，共有 1,333 人填寫問卷，誤差範圍 3%[210]。

(四) 網路公眾諮詢結果

本次網路公眾意見諮詢結果請參考附錄 2：，簡要說明如下：

1. 公共利益：

對於政府因應疫情，採取「簡訊實聯制」的方式進行防疫工作，有 40.2%民眾表示完全支持、55.9%民眾有條件支持，3.7%民眾完全不支持。有條件支持者最希望政府清楚說明的事項為「如何做好資安措施」；完全不支持的原因為「有可能被目的外利用」及「有資安疑慮」等。對於政府因應疫情，採用「電子圍籬智慧監控系統」進行防疫工作，有 38.4%民眾表示完全支持、54.9%民眾有條件支持，6.6%民眾完全不支持。有條件支持者最希望政府清楚說明的事項為「保存期限屆滿後刪除」；完全不支持的原因為「保存期限屆滿後可能不會刪除」及「有可能被目的外利用」等。

2. 身分識別：

對於電信業者利用電信資料提供「身分識別」相關的創新服務，有 23.4%民眾表示完全支持、57%民眾有條件支持，19.5%民眾完全不支持。有條件支持者最希望能達成的條件為「手機遺失時可立即停用身分識別功能」；完全不支持的原因為「擔心手機遺失時無法立即停止身分識別功能」等。

3. 金融科技：

[209] 樣本蒐集方法：1.財團法人資訊工業策進會官網、電子報、2.達文西個資暨高科技法律事務所官網、電子報、3.中華民國電腦稽核會官網、電子報、4.臉書分享及 Line 群組轉傳。

[210] 母體大小為 23,000,000 人，信心水準 95%，樣本大小為 1,333 人，套用「誤差範圍=標準分數×母體標準差÷$\sqrt{樣本大小}$」之公式，得出誤差範圍為 3%之結果。

本報告之智慧財產權屬於國家通訊傳播委員會

對於電信業者利用電信資料提供「金融科技」相關的創新服務，有 19.6%民眾表示完全支持、57.4%民眾有條件支持，22.8%民眾完全不支持。有條件支持者最希望能達成的條件為「不會被使用在行銷用途」；完全不支持的原因為「擔心電信資料被用在行銷用途等」等。

4. 商業應用：

對於電信業者利用電信資料提供「商業應用」相關的創新服務，有 18.6%民眾表示完全支持、55.9%民眾有條件支持，25.4%民眾完全不支持。有條件支持者最希望能達成的條件為「確保沒有個資外洩的風險」；完全不支持的原因為「可能被商家行銷訊息騷擾」及「不想讓電信業者無償將民眾個資分析後營利」等。

5. 交通運輸：

對於電信業者利用電信資料提供「交通運輸」相關的創新服務，有 31.8%民眾表示完全支持、57.2%民眾有條件支持，10.9%民眾完全不支持。有條件支持者最希望能達成的條件為「資料提供給第三方時不可辨識出民眾身分」；完全不支持的原因為「不想被電信業者或第三方追蹤民眾的位置資訊」等。

第二節 實例分享座談會

一、 工作內容

本團隊邀請國內電信事業、合作產業、相關產業、消保及人權團體及專家學者，舉辦 2 場實例分享及討論座談會，以瞭解電信事業已運用或有意規劃利用數據資料之模式；並對其資料運用、治理、保護與創新應用服務等情形，與產官學研各界專家學者探討國內相關法令限制及挑戰、政府與企業責任、未來法規修正或決策流程建議等議題。

本報告之智慧財產權屬於國家通訊傳播委員會

二、 工作規劃

本團隊於 110 年 8 月 2 日及 8 月 4 日以小型座談會方式討論電信事業現行已運用或有意規劃利用數據資料之模式，並邀請以下各領域專家（參表 3、表 4）：

表 3 110 年 8 月 2 日座談會專家名單

110 年 8 月 2 日		
主持人	達文西個資暨高科技法律事務所	葉奇鑫律師
	財團法人資訊工業策進會	宋佩珊主任
國內電信業者	中華電信股份有限公司 大數據處	闕仁斌總監
	遠傳電信股份有限公司	江奎徵律師
合作產業	走著瞧股份有限公司(Whoscall)	柯志強資深商務經理
學者專家	中央研究院法律學研究所資訊法中心	邱文聰主任
	世新大學法律學院	翁逸泓副教授
	東吳大學法律學系	余啟民教授
	輔仁大學法律學系	張陳弘教授
人權團體	中華民國消費者文教基金會	蘇錦霞律師
	台灣人權促進會	周冠汝專員
政府單位	金融監督管理委員會	蔡少懷組長

資料來源：本計畫製作

本報告之智慧財產權屬於國家通訊傳播委員會

表 4 110 年 8 月 4 日座談會專家名單

110 年 8 月 4 日		
主持人	達文西個資暨高科技法律事務所	葉奇鑫律師
	財團法人資訊工業策進會科技法律研究所	孫鈺婷專案經理
國內電信業者	台灣大哥大股份有限公司	與會代表人
	台灣之星電信股份有限公司	陳梅芬副理
	亞太電信股份有限公司	與會代表人
合作產業	域動行銷股份有限公司	與會代表人
	中華黃頁多媒體整合行銷股份有限公司	與會代表人
學者專家	中華電信股份有限公司	陳人傑主任
	東海大學法律學院	范姜真媺教授
	國立政治大學法學院	劉定基副教授
人權團體	開放文化基金會	李柏鋒董事長
政府單位	內政部統計處	賴威宇專員

資料來源：本計畫製作

與會者並針對電信事業資料運用、治理、保護與創新應用服務等實務情形，並發表對相關議題之網路公眾意見、國內相關法令限制及挑戰、政府與企業責任、未來法規修正或決策流程等議題之相關意見。

三、 工作成果

本團隊彙整國內外電信事業運用資料創新應用服務案例時，發現大致可區分為「公共利益」、「身分識別」、「金融科技」、「商業應用」、「交通運輸」等五大類別，簡要介紹如下：

(一) 公共利益

世界各國政府因應疫情，和電信事業合作利用電信資料進行防疫工作。英國 NHS COVID-19 App 曾面臨 App 開發人員承認即使 App 對用戶身分進行匿名處理，但理論上

本報告之智慧財產權屬於國家通訊傳播委員會

可能重新識別等關於資料安全的爭議。

英國民間團體則建議政府：

1. 提供強而有力的法律框架確保資料安全
2. 建立監督機制來監督資料的使用
3. 為確保資料安全採取資安措施
4. 援引類似於澳洲政府採取落日條款模式，說明是否會在疫情結束後銷毀資料。

英國民眾在 NHS App 開始使用時，對其資安或缺少法律框架管制上有所疑慮。而英國的 UK GDPR 及 DPA 規定在重大公共利益且必要時，例如預防或偵查不法行為時，可以目的外利用 NHS App 的資料（健康資料，在英國屬於特種資料）。

不過，NHS App 因應民眾的質疑，在其隱私權政策裡採用非常強硬的措辭，「就算有其他法律規定，也不能使用 NHS 的資料去識別使用者身分或追蹤使用者的位置」，且 NHS 也保證其所蒐集的都是匿名的資料。

因此，雖然英國法律規定可以將 NHS 使用者資料使用在犯罪偵查的用途上，但 NHS 只能提供去識別化的資料，實務上，警方就算拿到資料也無法識別及追蹤使用者。

在我國，因應 COVID-19 疫情，政府也和電信業者合作辦理我國社交距離 APP 及簡訊實聯制等，但民眾最有疑慮的是資料安全、屆期刪除、目的外利用等。尤其是日前曾有法官在媒體投書指出，有警察目的外利用簡訊實聯制資訊偵辦犯罪的爭議[211]。

(二) 身分識別

電信產業運用數據資料進行跨界合作已是世界趨勢，也有許多國外電信業者推動「身分識別」的創新服務，以愛

[211] 中央社，實聯制簡訊遭誤解用於辦案 法務部：研議修法保障個資，2021/06/24，https://www.cna.com.tw/news/asoc/202106240357.aspx（最後瀏覽日：2021/09/09）。

本報告之智慧財產權屬於國家通訊傳播委員會

沙尼亞 MobileID 為例，有 eID 的民眾得向電信公司申請加密 SIM 卡，並於手機安裝具驗證及簽署功能的 APP，就可以將手機當成 eID 使用。

愛沙尼亞推行 Mobile ID 曾遇到民眾對於資訊安全的相關質疑，而愛沙尼亞政府以「布建免費網路」、「公開透明政府」、「分散資安風險」、「完整法律架構」、「強化資訊教育」等方式，強化民眾對政府的信任。

在我國，TWID 身分識別中心和五大電信聯手推動「Mobile ID 行動身分識別服務」，讓個人使用的手機有類似網路身分證的功能，憑手機就能通過實名認證，完成銀行線上開戶、網路購物交易確認等，2021 年（今年）綜所稅報稅導入 Mobile ID 驗證[212]。

(三) 金融科技

有關國外電信業者推動「金融科技」的創新服務，韓國 KT 電信與徵信業者、BNK 釜山銀行及 BNK 資本等共同簽署合作意向書，為信用等級弱勢族群提供優惠貸款服務。

COVID-19 對經濟的影響也使信用貸款的需求增加，然而主婦、學生、自營業者等信用等級弱勢族群，難以直接透過銀行申請貸款，因此 KT 電信以 AI 分析用戶通信費、商品內容、使用模式等資料，得到用戶信用等級資訊，再由銀行與徵信業者合作，針對信用等級提供用戶金融服務上的優惠，使信用等級弱勢者亦可以獲得貸款服務。

在我國，金管會曾推動國內首宗沙盒實驗成功案例，便是由中華電信與凱基銀行合作，執行「實踐普惠金融首創電信行動身分認證」實驗計畫，除了身分認證流程優化，也透過電信數據（持有 6 個月行動門號且正常繳費者）為未曾使用金融服務的人（金融小白）加分，讓剛出社會的年輕人、

[212] 財政部 109 年度綜合所得稅行動電話認證，https://qa.twca.com.tw/taxmid/（最後瀏覽日：2021/09/09）。

本報告之智慧財產權屬於國家通訊傳播委員會

新創家、SOHO 族自由職業者也可以申請銀行服務[213]。

(四) 商業應用

有關國外電信業者推動「商業應用」的創新服務，韓國 KT 電信設立 BigSight 平台，透過基地台蒐集人流動向，判斷哪些人是常住人口或旅行人口，分析後向商家販售人口數據，分為商圈、觀光及生活類，並進一步提供商業規劃服務。

BigSight 平台也會分析電信用戶在網路上搜尋的關鍵字、消費特徵、訪問網站等，規劃廣告設計，進行精準行銷。而面對疫情影響經濟，商家收益均大幅降低，也更傾向利用大數據分析決定經營策略，BigSight 平台則推出折扣，吸引商家使用 BigSight 平台服務。

在我國，則有中華電信的人潮客群分析平台，其中人潮分析平台是掌握人流及統計型客戶輪廓資訊，可即時掌握景點遊客數量及活動人數統計，成為區域經營及展店選址利器；店內人潮分析則掌握室內人潮時段趨勢及人潮輪廓，讓商家藉此調整營業時段及商品組合[214]。

(五) 交通運輸

有關國外電信業者推動「交通運輸」的創新服務，英國 EE 電信和 Atkins 工程公司合作，監控倫敦外環高速公路 M25 的路況。一開始是用 ANPR 攝影機來計算行程時間，但效果不佳，既耗費成本也有人員維護的安全問題。後來 EE 電信將電信資料匿名處理後轉化為可分析的資料，Atkins 工程公司則應用電信資料規劃道路工程時間，維持高速公路交通順暢，並提供預估旅程時間服務。

[213] 陳蕙綾，金融監理沙盒成功首案誕生 信用小白電信借貸未來可望一體適用，鉅亨新聞，2019/08/15，https://news.cnyes.com/news/id/4367746（最後瀏覽日：2021/09/09）。

[214] MBA-人潮客群分析平台規格介紹，中華電信，https://www.cht.com.tw/home/enterprise/businessapplication/bigdata/684（最後瀏覽日：2021/09/09）。

本報告之智慧財產權屬於國家通訊傳播委員會

在我國，臺北、桃園、高雄等各縣市政府與電信業者合作建置旅遊人潮警示燈號系統，運用「去識別化之電信大數據技術」統計景區的人流數據，以簡單易懂的燈號呈現景區人流情形，讓民眾查詢，並藉由系統掌握開放式景點現場人流狀況，依防疫規定適時進行勸離及管制[215]。

(六) 會議記錄摘要

本研究 2 場座談會之完整會議紀錄請參考附錄 3：，摘要如表 5：

表 5 110 年度電信事業運用數據資料提供創新應用服務治理模式座談會討論摘要表

議題	討論重點
電信事業加值利用之障礙	業者就當事人同意及去識別化之困難及期待
	加值利用之風險
	我國推動加值利用之體制問題
公共利益	公共利益之目的外利用透明化
	防疫相關應用之技術及制度設計
身分識別	身分識別應用之風險考量
	民眾對身分識別應用之顧慮
	管理身分識別應用相關技術之制度設計
商業應用	業者推廣商業應用之困難
	未來推動商業應用可能之機制設計
交通運輸	交通運輸相關資料之可能用途
	業者對未來交通運輸應用之期待
	交通運輸應用之制度設計

[215] 孫家銘，掌握高雄七大熱門景點人潮 旅遊警示燈號測試版上線，新頭殼新聞，2021/07/27，https://newtalk.tw/news/view/2021-07-27/610975（最後瀏覽日：2021/09/09）。

本報告之智慧財產權屬於國家通訊傳播委員會

(七) 座談會照片





資料來源：本計畫拍攝

圖19　110 年 8 月 2 日座談會

本報告之智慧財產權屬於國家通訊傳播委員會





資料來源：本計畫拍攝

圖20　110 年 8 月 4 日座談會

本報告之智慧財產權屬於國家通訊傳播委員會

第三節 初步建議

一、 前言

(一) 多數民眾接受電信資料創新應用

依據前開網路公眾意見諮詢，民眾認為電信業者應優先發展的創新服務，最多人選擇身分識別類（1333 人中有 428 人，32%），交通運輸類次之（352 人，26%），第三為金融科技類（275 人，21%），第四為商業應用類（199 人，15%），亦有民眾認為均不應發展（64 人，5%），另有部分民眾認為應先發展環境、文化、醫療或犯罪偵查領域等創新應用（15 人，1%）。

而在電信業者推動創新服務的同時，民眾關於個資保護議題，最顧慮的事項分別為「若需要創新利用本人資料，有無事先經過本人同意？」、「電信資料是否會提供第三方」、「如何更便利地行使個人資料相關權利？」、「資料的安全性？」、「有無事先進行隱私風險評估？」等。

由此可知，1,333 份問卷中，只有約 5%的民眾認為電信業者均不應發展創新應用，換言之，多數（95%）民眾均能夠接受電信資料創新應用，但對個資保護仍有所疑慮。

(二) 現行個資法困境

大部分電信業者在座談會中均表示，目前我國現行個資法規定過於簡陋，利用電信資料創新應用時，常在發想階段因法規限制無法推行，且我國對於去識別化規範亦不甚清楚；座談會中亦有學者表示，我國的個資法跟不上科技時代，也沒有個資保護專責機關，若電信事業發展加值應用容易產生爭議。

準此，雖然個資法修法並非通傳會權責，惟座談會中眾與會者對個資法應盡速修法頗有共識，並提出許多修法建

本報告之智慧財產權屬於國家通訊傳播委員會

議，茲整理如下：

1. 訂定去識別化標準：我國個資法如修法，應訂定去識別化方法及基準，並針對將資料進行去識別化之業者，及接受去識別化資料之業者，課以不得再將該資料回復再識別之義務。
2. 強化當事人權利行使：以加州《消費者保護法》CCPA 為例，CCPA 不要求蒐集者取得當事人同意，而是強化當事人權利，讓當事人權利能更便利行使。
3. 設置個資保護專責機關：設置個資保護專責機關，加強個資保護之監理能量，尤其在跨行業個資蒐集、處理及利用上能統一規範，以免個別主管機關規範有所歧異而產生爭議；也讓民眾對政府更有信心，有助於電信事業發展創新應用。
4. 隱私衝擊評估：在英國 NHS APP 推出當下正值歐洲疫情大爆發，然 NHS APP 仍然進行完整之隱私衝擊評估後，始推出 APP 供英國民眾使用。隱私衝擊評估程序除了能事前找出可能發生之風險及可能補救措施外，也能建立民眾信賴度。
5. 建立透明化之要求：對於業者如何取得資料、取得哪些資料？利用目的為何？提供給誰？對民眾有哪些風險等資訊都應該公布於眾；除此之外，資料生命週期亦應該公開，讓民眾能瞭解提供出去之個資狀態為何。

本報告之智慧財產權屬於國家通訊傳播委員會

二、 建議

惟在我國個資法尚未修法的現狀下，本研究針對電信事業運用資料創新應用服務之治理模式，提出初步建議如下：

(一) 修訂《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》（短期建議）

本研究茲彙整座談會專家學者關於修訂《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》（下稱 NCC 安維辦法）之意見如下，未來通傳會於修訂相關辦法後，為求與個資法的一致性，亦可評估請國家發展委員會就修訂內容提供意見。

1. 動態取得同意及透明化要求

座談會中有電信業者提及在加值應用上取得當事人同意之困難，學者亦對此提出見解，認為電信業者除了擁有客戶即時之聯絡方式以外，每個月亦至少有一次與客戶聯繫之機會（如寄送帳單），相較於其他產業（如醫療產業）已較容易與當事人溝通，並有效取得特定目的外利用的動態同意。

除此之外，透明化亦為學者認為電信業者在加值應用時必須踐行之要求，即電信業者於利用電信資料進行加值應用時，須公開透明其創新應用處理電信資料之方式及目的，讓民眾清楚瞭解資料如何被利用。

因此，本研究針對電信業者如何動態取得當事人有效同意，並符合透明化要求，建議通傳會可參考歐盟個資保護委員會（The European Data Protection Board, EDPB）發布的同意指引、GDPR 透明性指引及韓國《大數據個人資料保護準則》等關於有效同意及透明化要求之規範內容，於 NCC 安維辦法增訂電信資料加值應用中關於有效同意及透明性之相關規定。

本報告之智慧財產權屬於國家通訊傳播委員會

2. 電信資料去識別化標準或指引

除了取得當事人同意之障礙外，電信業者於座談會再三強調我國個資法對於去識別化之標準不明確，造成即使電信業者希望透過去識別化之方式運用客戶個人資料，卻無法達到個資法之要求。

我國現行實務上，去識別化之標準會因涉及哪類個資、在什麼目的下蒐集處理、為何目的之利用而有所不同，現今尚無明確且統一之規範，因此，去識別化與否在實務運作認定相當困難，亦被學者認為是現行個資法的重大缺憾之一。

準此，縱使未來我國個資法進行修法，屆時主管機關可能將去識別化一事建立統一的基礎標準，但在現行個資法修法之前，電信業者加值應用發展已刻不容緩，因此本研究建議通傳會可參考日本「假名化加工資料」、韓國KCC《大數據個人資料保護準則》等關於去識別化措施，與電信業者及專家學者一同研商，於 NCC 安維辦法中訂定電信資料加值應用相關規範，如該等電信資料涉及個人資料，應先進行去識別化，且不得再重新識別之原則[216]。

3. 隱私衝擊評估

參與座談會之學者亦多次提及隱私衝擊評估（DPIA）之重要性，並指出此為歐盟 GDPR 規定之重要程序，惟我國個資法亦漏未規定。歐盟優良實務建議可以公開隱私衝擊評估之摘要及結論217，因此，若能再透過公開評估與執行的結果，或可強化民眾對主管機關及電信業者進行加值應用的信任度。

---

[216] 經濟部已制訂國家標準 CNS29100-2 及 CNS29191 二項去識別化認證制度及作業標準，若我國未來個資法修法後對於去識別化之標準較為明確之後，此二項標準亦可能因修法而有所變動，未來通傳會可視情形要求電信事業遵循之。

[217] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

本報告之智慧財產權屬於國家通訊傳播委員會

因此本研究建議通傳會可參考 GDPR 有關隱私衝擊評估之內容，於 NCC 安維辦法增訂之電信資料加值應用相關規範中納入隱私衝擊評估之規範，要求電信業者於加值應用涉及較高風險時，例如利用生物資料、大規模分析追蹤、資料庫比對、自動化決策等，應先進行隱私風險評估，並公布其評估結果。

4. 強化當事人權利

另有學者專家指出，如能提升資料當事人行使個資法權利之便利程度(如可向業者查閱個資應用情形)等作法，有助於降低民眾對電信業者進行創新應用之疑慮。

故本研究亦建議通傳會可於 NCC 安維辦法增訂之電信資料加值應用相關規範中，要求或鼓勵電信業者定期公布加值應用相關資訊，以強化當事人行使個資法的權利。

舉例而言，電信業者與政府機關合作時，可公布哪些公務機關調取多少筆個資；或是電信業者在不妨礙商業機密前提下，將目前進行創新應用的相關數據透明公開，有助於提升民眾對主管機關及電信業者進行加值應用的信任度。

5. NCC 安維辦法草案

本研究依據上述幾點建議，草擬《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》修正草案，請參見第七章第二節。

(二) 建立網路公眾意見諮詢平台（短期建議）

本團隊於本次研究中，為彙整公眾對研究主題之意見，參考既有之公眾參與網路平台如 vTaiwan、i-Voting 等，以網路問卷方式辦理公眾意見諮詢。前述平台運作方式略述如下：

1. vTaiwan 係由台灣公民科技社群「g0v 零時政府」建置、

本報告之智慧財產權屬於國家通訊傳播委員會

國發會法制協調中心及資策會科技法律研究所協力支援之專案，讓民眾透過留言、轉貼、協作等方式，針對各項提案討論相關法規應如何制定或修改，並由政府相關單位彙整後送交立法院議決。

2. i-Voting 則為台北市政府推出之網路投票機制，民眾可透過網路參與公共政策提案、討論、形成選項到投票之歷程，促進市民參與市政討論及推動。

本團隊進行網路公眾意見諮詢過程中，發現大部分民眾並不反對電信事業利用資料進行創新應用，但民眾對業者或主管機關沒有信心，而產生諸多疑慮。

為利通傳會未來訂定相關法規政策時，可即時、廣泛徵詢電信事業、一般大眾及其他利害關係人之意見，建議通傳會可參酌本次研究經驗，建立網路公眾意見諮詢平台[218]，以使政策制定過程透明化，並使相關法規政策更加符合實務需求，增進治理之效益。

此外，電信事業進行監理沙盒實驗時，亦可運用該平台使電信事業與網路公眾進行溝通對話，促進民眾對通傳會及電信事業之信任度。

(三) 訂定電信監理沙盒規範，鼓勵業者以監理沙盒模式進行創新試驗（中期建議）

目前電信業者已有金融科技之創新服務進入金管會監理沙盒中，其中二件關於身分認證之實驗案，一為凱基銀行與中華電信合作之數位身分認證；二為阿爾發投顧與永豐

[218] 網路公眾意見諮詢平台之運作流程建議如下：
1.設定主題。
2.依主題擬定研究問題。
3.依研究問題檢視既有文獻。
4.參酌文獻回顧結果設計問卷。
5.透過網路發布問卷，蒐集業者及民眾意見。
6.彙整、分析問卷結果。
7.依據問卷結果，針對研究問題提出結論及建議。

本報告之智慧財產權屬於國家通訊傳播委員會

金證券合作，讓客戶在開戶時可透過手機進行身分認證。

其中凱基銀行與中華電信之合作已取得正面成果，可知監理沙盒模式可提供電信事業在創新應用之良好環境，讓業者於風險可控之情形下測試其創新產品。

又依據前開網路公眾意見諮詢結果，可知較多民眾認為「身分識別」及「交通運輸」服務應優先發展創新服務，因此，本研究建議通傳會可參考金管會之《金融科技發展與創新實驗條例》，訂定《電信加值發展與創新實驗條例》，並鼓勵電信業者進入電信監理沙盒模式，就身分識別及交通運輸類等創新服務進行實驗[219]，協助電信業者與合作廠商辨識進行電信資料加值應用服務時可能遭遇到的具體障礙，並釐清現行法規可調整之方向或可行之輔導措施，而後更能進一步接軌法規落地。

(四) 建置資料銀行制度（長期建議）

座談會中有學者專家認為，在大數據發展的時代，民眾若要瞭解並決定自己的個資要提供給誰進行加值應用，是相對困難的，並提及日本資料銀行制度，即民眾可委託第三方公正機構進行個人資料管理。

日本之資料銀行制度係以信託方式[220]進行個人資料管理，由受託人（一般民眾或擁有大量個資的業者）通過信託行為，預先指定或設定條件將其資料信託予受託人（資料銀行），並由受託人按信託人設定信託之目的，為其管理個人資料，並應善盡管理個人資料之義務。如遇須將個人資料提供予第三人使用之情形，資料銀行亦得於必要時對資料作匿名化。

準此，本研究提出長期建議，為鼓勵電信業者進行創新

[219] 關於金融科技的電信資料創新服務則仍應適用《金融科技發展與創新實驗條例》。

[220] 日本資料銀行機制採用之資料信託，如欲轉化為適於我國現行法規者，或需考量資料本身性質並非財產權之範疇，無法作為信託契約標的情形，宜採行委任契約作法為妥。資料來源：蔡毓華，自資料流通機制建置擴大資料經濟市場，資策會科法所，2020/04，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8440（最後瀏覽日：2021/09/11）。

本報告之智慧財產權屬於國家通訊傳播委員會

加值應用，避免囿於法規而有所侷限，通傳會可評估參酌日本做法建置資料銀行制度，藉由可信任之第三方機構作為資料流通基礎，鼓勵並促進電信資料加值再利用。

此外，我國為邁向國家數位轉型並推動國家六大核心關鍵產業，目前正在推動行政院的組織改造，將成立專責的數位發展部[221]，整合「電信、資訊、資安、網路與傳播」五大領域，統籌基礎建設、環境整備及資源運用等工作，相關機關的資訊、資安、網路、通信和傳播等產業的輔導及發展業務可能全數移撥至數位發展部主管，以上建議，屆時可供相關承辦單位作為施政參考。

[221] 黃彥棻，【專訪行政院政務委員郭耀煌】落實總統政見，數位發展部最快 2022 第一季掛牌，iThome，2021/05/18， https://www.ithome.com.tw/news/144110（最後瀏覽日：2021/09/11）。

本報告之智慧財產權屬於國家通訊傳播委員會

第五章 電信事業運用數據資料提供創新應用服務治理模式研究建議（解決方案座談會）

第一節 解決方案座談會執行摘要

一、 座談會目的

本工作項目之執行目標，係與國內電信事業、合作產業、相關產業、消保及人權團體、專家學者等進行合作，透過舉辦座談會等方式，與產官學研各界專家學者，針對前揭公眾諮詢及座談會之建議意見進行實際議題深入探討，彙整相關數據資料蒐集種類、應用態樣及實際應用可能面臨之問題及解決方案，共同研商因應解決建議，並協助政府規劃推動政策。

二、 座談會規劃

時間：110 年 10 月 13 日 14 時 00 分至 17 時 10 分

地點：資策會科法所行遠講堂

（座談會簡報請參附錄 5：）

本報告之智慧財產權屬於國家通訊傳播委員會

表 6 110 年 10 月 13 日座談會專家名單

類別	服務單位	姓名
國內電信業者	遠傳電信股份有限公司	江奎徵 副理
	中華電信法律事務處	陳人傑 主任級管理師
合作產業	走著瞧股份有限公司（Whoscall）	柯志強 資深商務經理
	景翊科技股份有限公司	陳奕廷 總經理
學者專家	東吳大學法律學系	余啟民 副教授
	元智大學資訊傳播學系	葉志良 副教授
消保及人權團體	中華民國消費者文教基金會	蘇錦霞 名譽董事長
	開放文化基金會	李柏鋒 董事長
政府單位	交通部運輸研究所	吳東凌 組長
	內政部統計處	賴威宇 專員（書面意見）

資料來源：本計畫製作

表 7 110 年 10 月 13 日座談會議程

時間	議程內容	主持人/主講人
13：30~14：00	報到	
14：00~14：05	開場致詞	張乃文 副主任（資策會科法所）
14：05~14：25	引言簡報及議題說明	孫鈺婷 專案經理（資策會科法所）
14：25~17：00	與會學者專家綜合討論	張乃文 副主任（資策會科法所） 王慕民 律師（達文西個資暨高科技法律事務所）
17：00	賦歸	

資料來源：本計畫製作

本報告之智慧財產權屬於國家通訊傳播委員會

三、 座談會紀錄摘要

(一) 東吳大學法律學系余啟民教授

簡報第 14 頁中對解決方案建議研擬短、中、長期規劃，個人對中期規劃之「隱私衝擊評估」深表認同，惟國家通訊傳播委員會（以下簡稱 NCC）可能需要更具體的建議。因此關於中期規劃建議 NCC 作為電信監理機關，應建立相關指引，在不同利益（例如公共利益、資料利他或是資料共享）之間權衡。三項具體建議如下：

1. 建議得參考「電子商務消費者保護綱領」，具體名稱建議可以配合主題，命名為「電信數據資料創新應用隱私衝擊評估指引」。透過綱領的形式，在不衝擊目前各部會執掌且能兼顧監理，建立一個包含當事人同意與去識別化評估的原則，並於定型化契約或應記載事項中明確說明，在電信資料跨業應用時滾動調整，即可在跨部會間形成協調作用。
2. 建議區別風險層級，定期檢視並滾動式調整，以因應數位匯流情勢以及不同風險的等級與態樣。風險等級由高至低依序考量為國安、公共利益、醫療、金融、交通運輸，最後則是商用。同時考量造成風險等級的改變情事，例如未來可能推出虛擬健保卡，透過手機為載體，可能同時產生電信資料，此時，虛擬健保卡內資料之風險等級即需要調整。此外，當事人同意雖涉及跨機構處理問題，然已可逐漸透過科技方式去克服，且未來科技應用面將快於法規突破。
3. 涉及跨領域資料應用的去識別化，須注意消費者保護與告知事項（即消費者知的權利），應告知消費者資料將如何應用與去識別化範圍為何。

本報告之智慧財產權屬於國家通訊傳播委員會

(二) 中華電信法律事務處陳人傑主任級管理師

1. 關於電信數據資料於公共利益目的應用：
   (1) 法務部有函釋認為 1922 簡訊非通保法上通訊紀錄，故電信業者在配合檢調調取通訊資料的操作上皆依此函釋內容處理。
   (2) 目前法制上就資料公共目的加值應用規範在個人資料保護法第 16 條與 20 條，惟就增進公共利益與維護國家安全之描述不具體且容易產生爭議。故建議參考歐盟電子隱私條例（ePrivacy regulation）草案第 11 條規定，對於個人資料保護法的權利限制，應考量基本權利與自由等比例原則內涵。
   (3) 歐洲資料治理規則草案規定，目前觀察到的問題可能包含須克服資料標準化與格式化的問題，以及須確保資料之去識別化，未來才可能安全地進行資料共享，在我國實現資料利他主義與建立資料中介。
2. 關於電信數據資料於商業目的應用：
   (1) 商業加值利用資料可分為流量資料與位置資料兩類，除非符合公益考量或進行去識別化，否則就個人資料保護法第 20 條之規定，原則上進行資料加值應經過當事人同意。故電信業者雖有許多用戶的個人資料，但必須在符合合目的性之限制下利用。
   (2) 簡報第 13 頁所提到的電信數據應用型態，涉及電信業者與第三方業者之合作，電信業者僅提供電信網路與服務，而非掌握所有資料。目前實務上，電信業者是以合約方式，在獲得消費者同意之前提下進行資料利用，處理相關合作關係。
3. 當事人同意與退出的實務做法：同意是透過服務契約勾選是否同意加值應用，退出則可以由用戶進線到電信公司客服申請退出，或親自到門市辦理。關於通信紀錄查

本報告之智慧財產權屬於國家通訊傳播委員會

詢，依 NCC 頒佈的「電信事業用戶查詢通信紀錄及帳務紀錄作業辦法」之規定，通信紀錄與帳務紀錄皆須保存一年，在此期間內可提供用戶查詢，一年後原則上即會刪除資料。而通信紀錄所稱的位置資訊，為基地台的 Cell ID 位置，並非用戶的實際位置。

(三) 元智大學資訊傳播學系葉志良副教授

1. 關於電信數據資料於公共利益目的應用：
   (1) 首先應明確說明與定義何謂國家安全與公共利益，政府在資料應用串接與跨域利用上，也須向人民說明，並建立事前評估與事後查驗機制。針對資料運用是否涉及國家安全或公共利益時，公務部門在執行之前應先釐清是否有法源依據。
   (2) 針對事前評估與事後查驗機制，具體作法為公務需求端應提出需求計畫，審查是否涉及個資保護議題；事後查驗則是指在資料蒐集過程中，審查是否符合計畫送審之過程以及相關紀錄是否符合規定。癥結點在於是否需要成立獨立機關，雖在目前政府組織架構體制下不易達成，但期能儘快成立。
2. 關於電信數據資料於商業目的應用：
   (1) 電信事業在民眾申辦業務時，即已具雙證件查核申請民眾之身分，再透過 TWCA 第三方驗證的方式，在身分驗證上較無問題。目前電信業者透過身分驗證亦拓展許多個人化服務。
   (2) 惟資料應用共享的困境的管理面在於當事人同意，電信業者在應用上會受到主管機關箝制，另外，個資法上是有多個中央目的事業主管機關，在規範不夠明確的狀況下，即便獲得當事人同意亦受到諸多限制。技術面上，則是無法釐清何謂去識別化。因此，根本解決應從主管機關確立規範。

本報告之智慧財產權屬於國家通訊傳播委員會

3. 建議可參歐盟資料治理草案先建立嚴格保護規範後，逐漸鬆綁對資料應用之方向。參考美國並非透過單一法典處理資料保護，更利於資料仲介業者生存之相對寬鬆做法，來建立我國資料應用之脈絡與未來方向。
4. 就短、中、長期規劃，建議應先加強法制面對當事人權利行使，讓當事人知悉與調整對資料之同意應用。因此，在資料應用起步上方向應越簡單越好，讓消費者知悉資料會如何被使用，業者則須確實管理個人資料。

(四) 中華民國消費者文教基金會蘇錦霞名譽董事長

1. 目前消費者普遍可接受將資料應用在學術研究發展上之公益目的，而商業應用上則須回饋消費者並衡平風險與利益。大部分的消費者對資料應用有疑慮是因為不了解資料應用之實際狀況。
2. 建議從消費者八大權利[222]檢視，除滿足消費者基本需求外，尚須講求安全，以法律作為最低底線規範，由政府與業者共同營造安全環境。適當教育消費者，並提供正確資訊，例如讓消費者知悉業者如何使用資料，並給予消費者意見表達，以及選擇進入與退出之機會。亦應建立適當賠償機制，賦予消費者受到傷害後請求賠償的權利。
3. 若欲滿足消費者八大權利，須要確立明確的主管機關，以明確技術層面概念或建立相關指引，將資料利用過程透明化，讓消費者了解資料如何被利用以及產生何種價值。商業應用上則須提供消費者選擇退出，並使消費者確實了解風險。而共享平台上則須透過具相同規模與信念之平台業者合作，始得減少風險。
4. 希望由業者或政府來掌控與保護消費者資料，並強化資

[222] 消費者八大權利包含：基本需求、講求安全、正確資訊、決定選擇、表達意見、請求賠償、消費教育、健康環境。

本報告之智慧財產權屬於國家通訊傳播委員會

料應用之透明性，讓消費者能夠清楚地知悉資料利用與流通。若因消費者不了解而產生抗拒，可能阻礙資料之創新。在制度設計上也應確保消費者有選擇權，而不是被迫選擇。

(五) 遠傳電信股份有限公司江奎徵副理

1. 電信業者所擁有的資料優勢在於正確性與真實性。電信業者蒐集資料類型為民眾申辦電信服務時所提供之資料(包含基本資料及雙證件影本),與實際使用電信服務時所產生之資料(例如位置資訊、網路活動軌跡等)。電信業者以最初蒐集資料之目的，擁有資料與使用資料應無問題。
2. 關於電信數據資料於公共利益目的應用：建議應更重視法律保留。當電信業者收到檢警的公文要求配合調查時，即會檢視是否符合通訊保障監察法第 11 條之 1 與刑事訴訟法相關規定，惟協助防疫而提供資料的部分是否有法律保留則受到質疑。因此，在法律保留之前提下使用資料，方能讓業者放心並更符合公益。
3. 關於電信數據資料於商業目的應用:NCC 在審閱業者服務契約時，也會要求將個人資料保護法上告知事項之文字納入。針對當事人撤回同意是否與同意之便利性相同，認為撤回同意雖無法透過按鈕方式撤回，但透過客服基本資料核對後申請撤回，對當事人影響應不大。
4. 資料在使用上可能會有許多當初沒辦法考量到的蒐集目的與創新應用，雖再次取得同意是可行的方式之一，但成本可能過高，因此建議以去識別化方式提供是較可採行的方式。另外，因先前同意而產出之去識別化資料或是其他應用資料，是否會因為撤回同意而需要將資料從母數取出。若是,對業者而言可能產生風險與不便利；因此我個人意見是傾向當事人撤回同意時，不回溯發生

本報告之智慧財產權屬於國家通訊傳播委員會

效力。

(六) 交通部運輸研究所吳東凌組長

1. 資料應用上的難題在於創新與治理間的衡平，目前在資料應用上法規範尚不明確，會使業者對資料應用產生恐懼。因此認為應訂立隱私衝擊評估相關指引，並定期進行滾動式調整，才能使電信業者所擁有的資料發揮價值。
2. 在進行資料加值時，除了最低限度遵循法律維護消費者安全外，亦可由利他主義出發，來思考可給予消費者何種回饋與利益。第一步應該建立制度，針對何種資料能夠蒐集，提供指引依循，並設計事前申請及事後查核機制，例如建立公、私部門的資料保護委員會，定期檢視該計畫所使用的資料，以及比對該計畫是否有相關法理依據以及執行成效。第二步則透過利己，讓提供資料的民眾有感。

(七) 開放文化基金會李柏鋒董事長

1. 關於身分識別建議：雖然電信業者目前已提供身分識別機制，惟建議電信業者可考慮參考愛沙尼亞具 eID 電子簽章功能的 SIM 卡機制（即 mobile-ID），加強化身分驗證機制與管理。
2. 關於個人資料主管機關建議：我國目前缺乏獨立的個人資料主管機關，現行個人資料保護法規範是由中央各目的事業主管機關管轄。而電信業者之目的事業主管機關為 NCC，故建議其可訂定相關指引，並藉由國發會協調，使在數位發展部正式設立前電信事業資料應用得繼續發展。
3. 關於建立民眾信賴建議：須保障個人資料，民眾才會放心提供資料，故電信業者至少須遵守個人資料保護法第 5 條所規範蒐集、處理或利用個人資料時之四大原則。

本報告之智慧財產權屬於國家通訊傳播委員會

參考愛沙尼亞國家資訊系統管理局（State Information Authority）之個人資料使用監測系統（Personal Data Usage Monitor），國民可清楚檢視政府調取資料軌跡，並經過長久發展建立國民對政府的高度信賴性。建議從賦予國民刪除資料的權利開始，逐步提高民眾信任度。雖然目前確實可以申請撤回同意或刪除資料，且電信事業有最基本之相關權利保護措施，但資料是否完全刪除仍有疑慮，要滿足消基會或個人要求仍有一段距離。另外關於當事人權利最需要強化的部分為資料可攜權（data portability），在強調個資保護的同時不只是保護個人，也也能促進商業目的資料加值應用的活絡。

(八) 景翊科技股份有限公司陳奕廷總經理

1. 資料創新已為目前的顯學，但我國目前仍處於較保守的階段。參英國、日本與韓國，皆訂定上位的戰略建立資料運用準則，並鼓勵資料創新應用。我國電信業者目前對資料應用的狀況較接近日本與韓國，但缺少上位戰略，若要直接訂定指引，可能沒有法律可依循，故建議先訂定高位階上位戰略。
2. 由於電信數據無論是在觀光、交通運輸還是其他大數據領域，都是非常寶貴且有價值之資料。惟電信數據難以取得，且取得成本過高，目前民間業者可能透過標準化的商業合作模式取得相關數據。因此，若是未來電信資料能夠透過沙盒的方式，在政府監管之下有更多創新應用，相信新創業者都非常樂見其成。建議可將資料沙盒模式移至中期規劃，未來數位發展部將正式設立，目前也有盤點資料創新領域，交通與開放銀行（Open banking）將會是兩大重點領域。

(九) 走著瞧股份有限公司(Whoscall)柯志強資深商務經理

1. 以過去推動開放銀行金融業者配合的經驗對照：首先，

本報告之智慧財產權屬於國家通訊傳播委員會

金融業者對於推動開放創新服務並無動力，故須提供業者更多執行的動力與誘因。第二，推動新創產業常有成本大於利益的問題，故須訂定適當配套措施鼓勵業者。第三，推動新創產業時對消費者保護常要求至盡善盡美，將不利新創產業發展，故建議對個人資料分級，提升對風險的容忍度。最後亦應考量政策的延續性，始能持續推展。

2. 針對監理沙盒的設計，業者的態度是期待且支持，但問題在於進入沙盒對於新創業者而言成本太高，因此希望此機制，搭配相關配套措施，能夠對中小企業得更加友善。

(十) 內政部統計處賴威宇專員（書面意見）

1. 基於國家安全與公共利益下，在我國具有推動優勢的電信數據資料類型為何？透過何種機制比較容易推行？
   (1) 在維護公眾利益、促進國家發展範疇下使用電信數據資料，為目前較不具爭議的使用情境，例如交通、防疫或住宅政策。但外界仍有少數侵犯個人隱私或淪為政治工具之聲量。為確保政府機關使用電信資料的正當性，如何使用？什麼情況下使用？使用的範圍為何？建議有明確的規範及透明的審核監管組織或系統，透過公開、透明的執行過程，作為建立民眾與政府在隱私資訊運用的互信關係。
   (2) 電信數據的類型與細緻程度，基於國家安全與公共利益下應取得最大開放，但仍應與執行目的需求做最大限縮。例如今天你想解決通勤時交通阻塞的問題，那資料的密度（資料的間隔）及細緻度（路口或巷弄）是必要考量，但取得資料的性別比、年齡層，與解決交通阻塞問題沒有直接關連，而標準的認定，仍須有個專責的審核監管組織進行。

本報告之智慧財產權屬於國家通訊傳播委員會

2. 在商業資料創新應用領域，具有推動優勢的電信數據資料類型為何？透過何種機制比較容易推行？

   在商業模式下難有利他行為出現，而在現今的商業環境，掌握數據者掌握優勢，若自由的將電信數據商業使用，容易有大者恆大，排擠小規模業者的生存空間，建議在商業創新過程，提取部分收益，建立低價或免付費的公眾資訊，除弭平資訊落差，亦達到公眾資訊（電信使用者）公眾享用的目標。

3. 解決方案建議：基於民眾需求推動電信資料應用，政府機關間可行的分責合作模式為何？

   對於民眾在電信數據的需求，內政部也在住宅及人口政策的計畫下，衍生產製一套不涉及個資及隱私的「電信信令人口統計資料」，就是想嘗試了解，民眾對電信資訊的具體需求，目前，礙於成本考量，較細緻的付費單元目前尚未有人申請，但較粗略的統計結果，已有許多金融業、大型賣場、不動產業及學術單位下載利用。未來其實也可以參考這樣的模式，由公部門主導處理及整合，消弭民眾在隱私或公平上的疑慮。

本報告之智慧財產權屬於國家通訊傳播委員會

四、 座談會照片紀錄





資料來源：本計畫拍攝

圖21　110 年 10 月 13 日座談會-1

本報告之智慧財產權屬於國家通訊傳播委員會





資料來源：本計畫拍攝

圖22　110 年 10 月 13 日座談會-2

本報告之智慧財產權屬於國家通訊傳播委員會

第二節 座談會議題討論與解決方案建議

一、 數據資料應用種類與態樣

對應本次座談會討論議題第一與第二大題，分別針對前述研析兩大面向，其一是基於國家安全與公共利益，以及其二是於商業資料創新應用，擬定兩題分別為「基於國家安全與公共利益下，在我國具有推動優勢的電信數據資料類型為何？透過何種機制比較容易推行？」，以及「在商業資料創新應用領域，具有推動優勢的電信數據資料類型為何？透過何種機制比較容易推行？」。團隊先將期中研析成果整理提供專家參考，就公共利益多以預防災害、疫情控制等目的提供電信資料，而資料類型主要為位置資料，且強調對於資料皆有進行去識別化，或是提供群集資料，而無法識別特定當事人。其中，有特別以法律明文規定的國家為韓國，透過修正傳染病防治暨管理相關法律，明文規定電信業者為防止疫情傳染並擴散，應提供使用者位置資訊。

表 8 各國電信事業配合維護國家安全、公共利益提供電信資料案例整理

國家	電信事業配合維護國家安全、公共利益提供電信資料案例
愛沙尼亞	以行動定位資料（MPD）即時追蹤行動定位資料，評估各區域風險，並妥適地進行資源規劃。
英國	以電信行動位置資料分析，且為去識別化之群集資料，了解疫情期間人們移動和行為模式。
美國	電信法及無線通訊及公共安全法規範電信業者公開用戶位置資訊須經同意，並有 LBS 開發部署指南。
日本	KDDI 人口動態分析，支援國家對災害因應；NTT Docomo 人口流動統計服務，亦是支援防災與社會產業調查。

本報告之智慧財產權屬於國家通訊傳播委員會

國家	電信事業配合維護國家安全、公共利益提供電信資料案例
韓國	修正傳染病防治暨管理相關法律，明文要求電信業者為防止疫情傳染並擴散，應提供使用者位置資訊。

資料來源：本計畫整理

座談會簡報也有整理關於歐盟執委會因應資料戰略，並加強歐盟資料共享機制，強化大眾對資料中介者（data intermediary）之信賴，並促進資料的可用性，於 2020 年 11 月提出「歐洲資料治理規則草案」（Proposal for a Regulation of the European Parliament and of the Council on European Data Governance, Data Governance Act, DGA）。其中該法第四章規定關於資料利他主義（data altruism），亦即促進個人或公司出於公共利益自願提供資料，資料利他組織需註冊為「歐盟認可的資料利他組織」（data altruism organisation recognised in the Union），以增進社會對該等組織營運的信賴。同時，為促進基於資料利他主義的資料蒐集，該法也有規範關於「共通歐洲資料利他同意書」（common European data altruism consent form），以降低中介者取得當事人同意成本，促進資料可攜性。

延續第三章第四節關於 2020 年英國 Ofcom 公開意見徵詢中也有提到關於消費者可以獲授權第三方共享通訊資料，範疇包含市話（landline）、固網、行網與付費電視（pay TV services）的獨立和套餐（standalone and bundled）服務等的兩大類資料：

(一) 消費者資料（customer data）：如消費者姓名、地址、資費、服務合約相關資訊、使用經驗等。

(二) 產品資料（product data）：產品詳細資訊（合約內容、費用、加值服務）、速度、服務品質（覆蓋率、可用性等）以及消費者的總體客戶體驗詳細資料等。

而公眾對開放共享資料類型之意見，認為仍應就資料類型訂定標準，以確定開放何種資料，並建議共享的資料應與客戶決策相關、不同提供者資料應具有相容性（comparable），且業者提供資料前需要考量提供成本或難度。然而現階段尚未達成共識，因此後續也將待資料

本報告之智慧財產權屬於國家通訊傳播委員會

應用之立法，以利於作為資料類型開放共享依據，值得持續觀察。

關於電信業者所蒐集資料類型，專家提到包含民眾申辦電信服務時所提供之資料（包含基本資料及雙證件影本），以及實際使用電信服務時所產生之資料（如位置資訊、網路活動軌跡等）為提供服務蒐集、處理、利用資料之目的。此外，也應注意電信事業對於資料保存期限法律規定，並非消費者要求即應刪除，依 NCC 頒佈的「電信事業用戶查詢通信紀錄及帳務紀錄作業辦法」第 4 條[223]之規定，通信紀錄與帳務紀錄皆須保存一年，在此期間內可提供用戶查詢，一年後即會刪除資料。而通信紀錄所稱的位置資訊，專家也提到是基地台的 Cell ID 位置，並非用戶的實際位置。

而本次座談會中，專家針對此議題也從不同角度切入探討。依據個資法第 16 條與 20 條就資料公共目的加值應用，在增進公共利益與維護國家安全之描述並不具體且易產生爭議，因此仍需要有相關函釋來說明，如 1922 之簡訊並非通保法上通訊紀錄，故電信業者在配合檢調調取通訊資料則依據函釋操作。此外，也有專家從風險角度切入為全面性思考，建議區別資料的風險層級，並應定期檢視調整，風險等級由高至低依序考量為國安、公共利益、醫療、金融、交通運輸，最後則是商用，並考量改變風險等級的情事，並呼籲透過科技方式克服，且避免法規尚未規範到情況。此外，除了法律面，專家也提醒也需要一併考量技術面，亦即解決資料標準化與格式化問題，並應確保資料去識別化，才能安全共享資料。

在維護公眾利益、促進國家發展範疇下使用電信數據資料，專家提到較不具爭議的使用情境，如交通、防疫或住宅政策等。但為確保政府機關使用電信資料的正當性，包含目的、範圍、方式、電信數據類型與細緻程度等，建議應有明確的規範，及透明的審核監管組織或系統，透過公開透明過程，建立民眾與政府在隱私資訊運用的互信基礎。

---

[223] 電信事業用戶查詢通信紀錄及帳務紀錄作業辦法第 4 條
1. 電信事業應將其保有之通信紀錄及帳務紀錄提供用戶查詢。
2. 前項通信紀錄及帳務紀錄之保存期間自紀錄發生時起算至少一年。
3. 第一項通信紀錄之查詢，須以完成通信者為限。

本報告之智慧財產權屬於國家通訊傳播委員會

至於電信數據資料於商業加值利用資料，專家也有提到可分為流量資料與位置資料，依據個資法第 20 條規定，除非符合公益考量，或進行去識別化，原則上進行資料加值應經過當事人同意。因此即使電信業者保有大量用戶的個資，但仍必須在符合目的限制下利用。而電信數據應用型態繁多，若涉及電信業者與第三方業者之合作，電信業者僅提供電信網路與服務，並非掌握所有資料，且雙方以契約約定關於資料利用，因此實務上仍應取得消費者同意，才能進行資料利用。

二、 電信業者應用時面臨資料應用問題

關於電信業者目前所面臨資料應用問題，對應本次座談會討論議題第三大題，對應報告第四章關於網路公眾意見諮詢與 2 場實例分享座談會，蒐整民眾與專家對於資料創新包含於公共利益、身分識別、金融科技、商業應用、交通運輸等領域之資料應用態度與建議。本次座談會希望綜整前述意見，並再次確認是否還有其他未考慮到的問題或風險，以擬定解決方案。因此擬定議題「業者應用時面臨問題整理如下，是否還有其他問題或風險需要考量，以促進電信數據資料應用？」

團隊先將期中所辦理之 2 場實例分享座談會意見整理，並對應英國資料倫理與創新中心（Centre for Data Ethics and Innovation, CDEI）2021 年 7 月提出關於「釋放資料的價值：探索資料中介的作用」之研究報告（Unlocking the value of data: Exploring the role of data intermediaries）[224]，該報告中表 3 整理關於「可能阻礙最佳資料共享之議題」（Table 3: Issues that may prevent optimal data sharing）對應先前座談會討論所提出問題可知，與該報告盤點問題皆能對應（參下表），「資料中介機制」可能亦得作為解決方案參考方向。

表 9 可能阻礙資料共享議題對應座談會討論整理

[224] Centre for Data Ethics and Innovation, Independent report Unlocking the value of data: Exploring the role of data intermediaries, https://www.gov.uk/government/publications/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries#fn:17 (last visited Oct. 31, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

議題	說明	資料中介潛在作用	座談會討論摘要對應
缺乏共享動力	資料提供者沒有足夠動力共享或提供資料	付費模式（pay to play），如組織近用資料集的前提是該組織也貢獻資料	• 業者推廣商業應用之困難 • 民眾對身分識別應用之顧慮
對於資料缺乏了解	資料提供者可能對其資料潛在用途缺乏了解，而資料使用者則不了解哪些資料可用與如何用	容易找到特定資料集，使資料提供者能發揮資料價值，資料使用者可以促進潛在應用	• 交通運輸相關資料之可能用途 • 未來推動商業應用可能之機制設計
商業、道德和聲譽風險	失去競爭優勢風險、破壞他人信任的資料使用而遭受聲譽損害，或允許在道德上有問題的資料使用	向資料主體和持有人保證，資料只能由經核准的組織出於特定目的近用	• 加值利用之風險 • 身分識別應用之風險考量
法律和監管風險	違反資料保護、智慧財產權或監管要求或相關風險也可能會阻止共享	提供法律專業知識和共通資料標準，以促進合法資料共享	• 業者就當事人同意及去識別化之困難及期待 • 我國推動加值利用之體制問題

本報告之智慧財產權屬於國家通訊傳播委員會

議題	說明	資料中介潛在作用	座談會討論摘要對應
資料共享成本	缺乏資料共享所需的共同基礎建設和技術，且建置成本可能過高	提供資料共享環境，包括應用隱私增強技術等（privacy-enhancing technologies）	• 業者對未來交通運輸應用之期待 • 管理身分識別應用相關技術之制度設計 • 交通運輸應用之制度設計
錯失為公共利益應用資料的機會	資料共享可能帶來經濟和社會效益	在受信任的研究環境中對敏感資料安全近用，為公共利益而進行研究	• 公共利益之目的外利用透明化 • 防疫相關應用之技術及制度設計

資料來源：本計畫整理

本次座談會關於其他問題，專家也有提到幾個需要關注議題，部分在先前座談會也有提到，就是去識別化、告知同意與消費者保護、個資專責機關設立等。當涉及跨領域資料應用需要考慮去識別化處理，並應注意消費者保護與告知事項，讓消費者知悉其資料將如何應用、產生何種價值與去識別化範圍為何，以及提供消費者選擇退出，並使消費者確實了解風險，避免因消費者不了解而抗拒，反而阻礙資料創新。至於消費者保護，專家也建議從消費者八大權利來檢視避免遺漏。此外，我國目前並無個人資料主管機關，專家建議應確立明確的主管機關，並提供相關指引，並強化資料應用之透明性。

除了上述三次座談會專家皆有重申之關注議題外，本次座談會還有提到關於身分識別與建立民眾信賴。專家認為雖然我國電信業者已提供身分識別機制，惟建議電信業者可考慮參考愛沙尼亞具 eID 電子簽章功能的 SIM 卡機制（即 mobile-ID），加強化身分驗證機制與管

本報告之智慧財產權屬於國家通訊傳播委員會

理，還有得參考愛沙尼亞國家資訊系統管理局之個人資料使用監測系統，國民可清楚檢視政府調取資料軌跡，建立國民對政府信賴。還建議強化資料可攜權，更能促進商業目的資料加值應用。

三、 解決方案建議

綜上所述，透過前三大題逐步蒐整專家意見，以思考規劃解決方案建議，由於資料共享應用涉及層面相當廣泛，專家也點出不僅是法律規範，還有技術發展、專責機關設立等皆需要納入考量，並非一蹴可幾，需要從短中長期逐漸推進，且不會僅涉及單一機關，需要政府跨部會合作與溝通，甚至是以國家層級推動整體資料戰略之政策方向。因此本次座談會的第四大題即「基於民眾需求推動電信資料應用，政府機關間可行的分責合作模式為何？」

團隊也透過國際趨勢研究、網路公眾意見諮詢與 2 場實例分享座談會初步提出目前短中長期之規劃。短期目標是建立網路公眾意見諮詢平台，中期則是針對規範面，訂定指引訂定，包含強化當事人權利行使（動態同意）、隱私衝擊評估、透明化要求，透過定型化契約明文取得當事人同意，以及對應我國經濟部制訂去識別化國家標準（CNS29100-2），對於資料有去識別化需求而建立流程管理制度之組織皆適用，表 10 一併整理關於電信事業資安與個資驗證之相關國際與我國國家標準。

表 10 電信事業資安與個資驗證之相關國際與我國國家標準

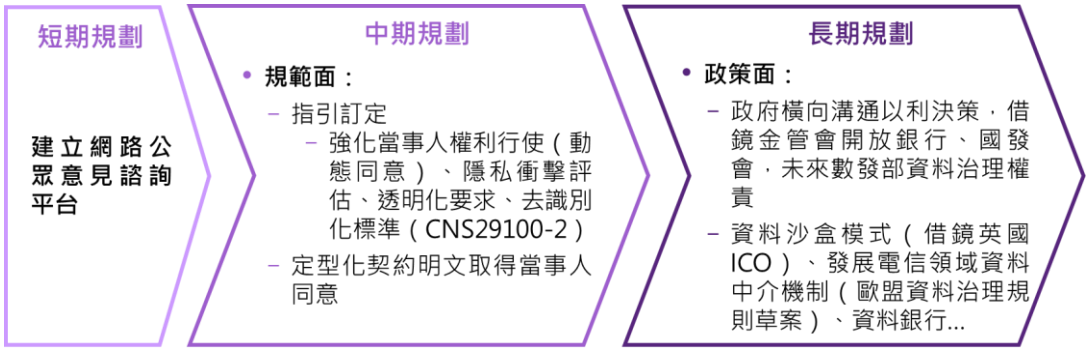
領域	法律要求應通過標準或相關規定	其他相關標準
資通安全	1. 電信事業資通安全管理辦法第4條 2. CNS 27001、ISO/IEC27001 3. 電信事業資通安全管理手冊（附件六 ISO/IEC27011 增項稽核表）	1. ISO/IEC 27017 2. CNS27018、ISO/IEC 27018 3. CNS27701、ISO/IEC 27701

本報告之智慧財產權屬於國家通訊傳播委員會

個資保護	個人資料保護法	1. TPIPAS 臺灣個人資料保護與管理制度 2. BS 10012 3. CNS 29100、ISO/IEC 29100 4. CNS 29100-1 5. CNS 29100-2 6. CNS 29191、ISO/IEC 29191

資料來源：本計畫整理

至於較長遠規劃則是以政策面思考，我國現階段尚無類似資料應用主管機關，仍能借鏡金融監督管理委員三階段自願自律模式推動之開放銀行，以及國家發展委員會的 MyData 機制來思考。2021 年 3 月行政院會通過數位發展部組織法設立數位發展部，資料治理為其重要職掌，未來數發部對於資料治理、資料共享應用政策法制之具體推動亦值得關注。此外，也能思考透過資料沙盒模式推動資料創新應用，或是發展電信領域之資料中介機制或是資料銀行機制。



資料來源：本計畫整理

圖23　短中長期解決方案規劃建議

本次座談會專家就短中長期規劃，於規範面建議應加強對當事人權利行使，讓當事人知悉與調整對資料之同意應用。於政策面之沙盒機制，專家也提到電信數據於大數據領域應用是極有價值資料，但取得不易且成本過高，因此目前現況是透過標準化的商業合作模式取得相關數據。對於電信資料若能夠透過沙盒方式應用相當樂見其成，甚至建議可將資料沙盒模式提前到中期規劃，更有利於電信資料應用之推動。

關於沙盒機制，專家也提到可以借鏡過去推動開放銀行的經驗對

本報告之智慧財產權屬於國家通訊傳播委員會

照，應注意三點包含提供業者更多執行的動力與誘因，訂定適當配套措施鼓勵業者，因為進入沙盒對於新創業者成本過高，亦應注意對中小企業友善，以及對個人資料分級，提升對風險的容忍度。最後亦應考量政策的延續性，始能持續推展沙盒機制。

本報告之智慧財產權屬於國家通訊傳播委員會

第六章 諮詢服務

關於我國個人資料保護法的於通傳領域適用相關爭議，或是國際通傳產業相關趨勢、規範及政策發展，本計畫團隊持續投入研究能量，依現況發展趨勢及通傳會所面臨相關議題，就通傳會業務範圍內相關資料蒐集與研究提供諮詢服務。本工作項預計完成 5 項諮詢服務議題，期中報告提供 3 項諮詢服務議題，分別研析如下。

第一節 議題一：向電信事業蒐集收視行為統計資料適法性研析

通傳會為促進多媒體內容傳輸平臺（MOD）及有線廣播電視事業之健全發展，保障公眾視聽之權益，增進公共利益與福祉，維護視聽多元化之目的，針對 MOD 平臺或有線電視系統經營者與頻道供應事業（下稱渠等事業）間之爭議，並辦理調處事宜，需向渠等事業蒐集相關收視用戶之收視行為統計資料，惠請研析相關適法之程序及見解，並提出具體可行之建議。

一、 適法性分析

(一) 通傳會於執行調處之法定職務必要範圍內，得向渠等事業蒐集含有可識別收視用戶之收視行為資料[225]，惟就「必要性」之判斷，宜審慎為之：

1. 按《個人資料保護法》第 15 條第 1 款規定：「公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：一、執行法定職務必要範圍內。」，可知公務機關在執行法定職務之必要範圍內，得為特定目的蒐集個人資料；又依主管機關之見解，該法定職務之範圍不限於作用法，組織法

[225] 本議題一探討之統計資料係含有可識別收視用戶之收視行為資料。如係未含有可識別收視用戶之統計資料，原則不適用個資法規定。

本報告之智慧財產權屬於國家通訊傳播委員會

之規定亦屬之[226]。

2. 次按「通訊傳播事業間重大爭議及消費者保護事宜之處理」，乃《國家通訊傳播委員會組織法》第 3 條第 9 款規定之通傳會掌理事項，應可認定渠等事業間的爭議調處，當屬通傳會的法定職務；另按《有線廣播電視法》第 55 條「系統經營者與頻道供應事業間有關頻道播送、授權條件及訂戶數認定之爭議，或系統經營者間之爭議，得向中央主管機關申請調處；調處不成時，得依法提起民事訴訟。」規定，亦屬通傳會於作用法明文賦予之法定職務。
3. 據此，通傳會就渠等事業執行調處事宜，應均可認為係屬執行法定職務（縱 MOD 平臺係受《電信法》管制，非受《有線廣播電視法》規制之有線電視系統業者[227]，然按前揭通傳會組織法規定，通傳會之調處亦屬法定職務之執行），從而依《個人資料保護法》第 15 條第 1 款規定，通傳會得於執行調處程序之必要範圍內，蒐集個人資料。
4. 惟按《個人資料保護法》第 5 條規定：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯」，個人資料之蒐集、處理及利用均不得逾越特定目的之必要範圍。

---

[226] 國家發展委員會 110 年 1 月 7 日發法字第 1092001961 號節錄：「按個資法第 6 條第 1 項第 2 款規定『有關病歷、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。但有下列情形之一者，不在此限：...二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。』。另上開所稱『法定職務』，包括『法律、法律授權之命令』（個資法施行細則第 10 條第 1 款規定）。**依國立自然科學博物館組織法第 2 條第 5 款規定，自然科學教育園區之管理係貴館之法定職掌，爰貴館為執行鳳凰谷鳥園生態園區管理之必要範圍內，基於防範人鳥共通疾病傳染之特定目的，蒐集園區工作人員之健康檢查資料，尚符合上開個資法之規定**。」

[227] 雖《電信法》未設有調處機制，而《固定通信業務管理規則》及《電信管理法》均有調處之相關規定。然細究其規定，可知《電信管理法》之調處係限於電信事業間就電信服務相關契約所生之重大爭議；《固定通信業務管理規則》之調處則係針對經營者間之管線基礎設施及電信設備共用等相關爭議，似無針對 MOD 平臺與頻道供應事業發生爭議時之調處機制。

本報告之智慧財產權屬於國家通訊傳播委員會

5. 查調處制度之目的，係為協調渠等事業間之爭議，而調處事由時常涉及頻道之上架或授權之費用爭議。又通傳會於辦理因上開爭議之調處時，可能需要向渠等事業蒐集相關收視行為資料，例如系爭頻道之收視率、特定時段觀看之人數及比例等，以作為調處進行之基礎資訊。
6. 是就通傳會進行調處，有無需要取得含有用戶個資之收視行為統計資料一事則恐有疑慮。渠等事業在調處過程中，可能向通傳會主張其只需提出某段時間收看某頻道之人數即可釐清授權費用爭議，無須提交能辨識用戶（即含有個資）之收視行為資料。
7. 準此，通傳會依據調處目的，有無必要蒐集渠等事業含有用戶個人資料之收視行為統計資料，宜審慎評估需求（例如通傳會在調處過程中，是否有驗證渠等事業提出收視行為資料真實性之需求，此時便需要渠等事業提出可辨識用戶之收視行為資料等），以降低違法蒐集資料之風險。

(二) 惟縱通傳會得為執行調處法定職務之目的，向渠等事業蒐集含有可識別收視用戶之收視行為資料，渠等事業在現行法下，似無明確義務為調處目的提供該資料，併此敘明：

1. 有線廣播電視事業「得」提供含有個資之收視行為資料，惟似尚無「應」提供之明確法律義務：
   (1) 查有線電視系統經營者與頻道供應事業均非公務機關，如提供含有個資之收視行為資料，則屬於個人資料之「利用」，必須符合《個人資料保護法》規定。依據《個人資料保護法》第 20 條第 1 項[228]規

[228] 個人資料保護法第 20 條第 1 項：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為增進公共利益所必要。三、為免除當事人之生命、身體、自由或財產上之危險。四、為防止他人權益之重大危害。五、公務機關或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經蒐集者依其揭露方式無從識別特定之當事人。

本報告之智慧財產權屬於國家通訊傳播委員會

定，非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍內為之。

(2) 惟因有線電視廣播電視業者蒐集用戶資料之目的，應係「履行收視、聽服務契約」，當通傳會因辦理調處事宜，要求有線廣播電視業者提供含有用戶個人資料之收視行為資料時，有線廣播電視業者可能會認為提供個資予通傳會之行為，將構成「特定目的外利用」。

(3) 依《個人資料保護法》第 20 條第 1 項但書第 1 款之「法律明文規定」，包含法律明確授權之命令[229]，因此有線廣播電視事業得主張《有線廣播電視法施行細則》第 21 條第 2 項規定，於特定目的外利用個人資料。是若通傳會要求提供之收視行為資料含有個人資料，業者得依據《有線廣播電視法施行細則》第 21 條第 2 項規定，主張《個人資料保護法》第 20 條第 1 項但書第 1 款之「法律明文規定」為個人資料之目的外利用，將**含有個人資料**之收視行為資料提供給通傳會。

(4) 惟雖《有線廣播電視法施行細則》第 21 條第 2 項檢送相關文件之規定，可解釋為系統經營者間或其與頻道供應事業間因爭議申請調處時，「應」檢送相關文件，即表示若系統經營者或頻道供應事業不檢送相關文件時，可能會得到不利之調處結果，然不利之調處結果似僅為調處不成立，依據《有線廣播電視法》第 55 條後段規定，調處不成立時得提起民事訴訟，有線廣播電視業者可能因其他考量於調處時拒絕提供收視用戶收視行為資料，轉而提起民事

六、經當事人同意。七、有利於當事人權益。」

[229] 個人資料保護法施行細則第 9 條：「本法第六條第一項但書第一款、第八條第二項第一款、第十六條但書第一款、第十九條第一項第一款、第二十條第一項但書第一款所稱法律，指法律或法律具體明確授權之法規命令。」

本報告之智慧財產權屬於國家通訊傳播委員會

訴訟以解決紛爭。

(5) 準此，現行法規似未明確課予有線廣播電視業者必須提供含有個資之收視行為資料予通傳會之義務。換言之，當有線廣播電視業者拒絕提供上開資料時，通傳會得否強制有線廣播電視業者交付相關資料，不無疑義。

2. 《有線廣播電視法修正草案》—或可提高有線廣播電視業者交付收視行為資料之意願：

(1) 按「前項有關頻道授權條件費用爭議，調處不成時，當事人一方得於調處不成之日起三十日內向中央主管機關申請裁決」，「裁決程序之相對人應於中央主管機關通知期間內，提出一定數額之授權條件費用、期間、費用推估標準、理由及相關佐證資料。未提出者，裁決諮詢會得依申請人提出之授權條件費用及現有資料作成裁決諮詢意見。裁決諮詢」，分別訂定於《有線廣播電視法修正草案》第 55 條第 2 項及第 55 條之 3 第 1 項。

(2) 查通傳會已於 110 年 4 月 14 日提出有線廣播電視法修正草案，因過去調處制度成效有限，爰規劃於現行調處機制外，新增裁決制度。於調處不成立時，當事人之一方得向中央主管機關申請裁決，爭議雙方得依裁決價格作為暫付費用之依據，待民事判決後再各自予以找補，以提升爭議處理之效能。而裁決之性質為行政處分，不服裁決者得依法提起行政訴訟，亦能同時兼顧人民之訴訟權利。

(3) 又查《有線廣播電視法修正草案》第 55 條第 2 項規定，裁決程序之相對人得提供相關證據予主管機關，其相關證據係為佐證授權條件費用、期間、費用推估標準之主張，收視用戶之收視行為統計資料亦可能包含於相關證據中。

本報告之智慧財產權屬於國家通訊傳播委員會

(4) 惟要注意者係，上開規定之法條用語係採取「得提供」，並無賦予相對人必須提供相關證據之義務，因此對主管機關而言，上開規定是否能達成獲取收視行為統計資料之目標，不無疑義。

(5) 依據《有線廣播電視法修正草案》第 66 條之 2 規定：「系統經營者、頻道供應事業或頻道代理商違反第五十五條之三第二項規定，未依裁決決定辦理者，中央主管機關應通知限期改正；屆期不改正者，處新臺幣十萬元以上二百萬元以下罰鍰，並得按次處罰」，可知裁決之結果與調處結果不同，調處不成立之結果僅為當事人雙方得另行提起訴訟解決紛爭；然當事人獲得不利之裁決結果時，必須依裁決決定辦理，若不服則須對裁決決定提起行政救濟。

(6) 由此可知，雖然修正草案中沒有處罰不提供相關資料之規定，但相較於調處不成立，當事人較不願得到不利之裁決結果，應可認為當事人在裁決程序中提供相關資料之意願，會遠高於調處程序，進而達到通傳會獲得收視行為資料之目的。

(7) 是故通傳會之《有線廣播電視法修正草案》中，有關於裁決之程序，雖然未對不提供資料之行為訂有處罰規定，然基於當事人雙方不願得到不利之裁決結果，應可認為有較高之意願提供相關資料，有助於通傳會蒐集用戶收視行為資料。

3. MOD 平臺「得」提供含有個資之收視行為資料，惟其亦似無「應」提供之明確法律義務：

(1) 查 MOD 平臺係非公務機關，如提供含有個資之收視行為資料亦屬於個人資料之「利用」，必須符合《個人資料保護法》規定。依據《個人資料保護法》第 20 條第 1 項規定，非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍內為之。

本報告之智慧財產權屬於國家通訊傳播委員會

(2) 惟因 MOD 平臺蒐集用戶資料之目的，應係為「履行服務契約」，則當通傳會因辦理調處事宜，要求 MOD 平臺提供含有用戶個人資料之收視行為資料時，如 MOD 平臺提供資料予通傳會，恐將構成「特定目的外利用」。

(3) 雖然 MOD 平臺並無前述有線廣播電視法規之適用，惟按《個人資料保護法》第 20 條 1 項但書第 2 款規定：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：二、為增進公共利益所必要」，非公務機關為增進公共利益所必要時，亦得為個人資料之目的外利用。

(4) 收視行為資料，如係為解決業者間紛爭，並保障消費者權益，應於個案中評估是否屬增進公共利益所必要，如是，則 MOD 平臺即可依《個人資料保護法》第 20 條第 1 項但書第 2 款之「為增進公共利益所必要」為個人資料之目的外利用，將含有個人資料之收視行為資料提供予通傳會。

(5) 然現行法規亦未課予 MOD 平臺必須提供含有個資之收視行為資料予通傳會之義務，通傳會得否強制 MOD 平臺交付相關資料，亦有疑義。

4. 據此，縱渠等事業得合法交付含有個人資料之收視行為資料予通傳會，然現行法規並未課予渠等事業提供上開資料之義務，即使《有線廣播電視法修正草案》或可提高業者交付之意願，惟仍不具有強制力，併予敘明。

二、 具體可行措施

(一) 建議通傳會就該次調處事宜事前評估，是否存有「取得可

本報告之智慧財產權屬於國家通訊傳播委員會

識別收視用戶之收視行為資料」之必要。倘有疑義，建議向渠等事業取得去識別化之收視行為資料，較能避免風險。退步言之，亦建議減少可識別用戶身分之資訊，以降低用戶權益侵害風險：

1. 如前所述，爭議調處雖為通傳會之法定職務，惟如通傳會為調處目的而蒐集個人資料，在個資法之適用下，仍應檢視是否逾越調處目的之必要範圍。
2. 據此，倘通傳會於該次調處，有意指定渠等事業提交「含有個資之收視行為資料」，宜先行評估所欲取得可識別用戶資訊（例如姓名、身分證號、電話號碼、帳單地址、機上盒號碼等識別符碼）之目的，是否均與調處之目的相符而有必要。具體而言，通傳會宜以**「不取得該項個資，即無法執行調處」**為標準，判斷向渠等事業取得可識別用戶資訊之必要性。
3. 倘通傳會於評估後認定為調處之目的，非以取得可識別用戶身分之資料為必要，通傳會應考慮取得去識別化[230]之收視行為資料。
4. 退步言之，即使通傳會經評估於該次調處事件，有向渠等事業取得「含有個資之收視行為資料」之必要，惟為降低用戶識別、資料安全等風險，亦建議通傳會考量減少可識別用戶身分之資訊。

(二) 如通傳會於調處過程取得含有個資之收視行為資料，原則上僅得於調處目的內利用；若通傳會有意為其他目的利用

[230] 另外根據最高行政法院 106 年判字 54 號判決意旨，所謂個人資料的去識別化必須達到「完全切斷資料內容與特定主體間之連結」的程度。

本報告之智慧財產權屬於國家通訊傳播委員會

收視行為資料，應評估是否合於個資法規範：

1. 按《個人資料保護法》第 16 條本文規定：「公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。」，可知公務機關原則上不得將蒐集之個人資料為目的外之利用。故通傳會若基於調處之目的蒐集含有個資之收視行為資料，亦僅得於調處之目的內利用。
2. 若通傳會有意於調處之目的外利用上開資料，可考慮以下方式：
   (1) 通傳會可將含有個資之收視行為資料去識別化後利用：
      A. 按法務部 103 年 11 月 17 日第 10303513040 號函釋[231]意旨，個人資料一旦去識別化，使其無從直接或間接識別特定個人，即非屬個人資料，此時已去識別化之資料即不受《個人資料保護法》規範，通傳會自得以調處外之目的利用去識別化之收視行為資料。
      B. 然要注意者係，仍需注意去識別化之程度，應達到「完全切斷資料內容與特定主體間之連結」，方為現行實務見解認定之去識別化。
   (2) 如通傳會欲自行利用含有個資之收視行為資料，須評估《個人資料保護法》第 16 條但書第 1、2 款之規定：
      A. 按《個人資料保護法》第 16 條但書第 1、2 款規定：「但有下列情形之一者，得為特定目的外之利用：一、法律明文規定。二、為維護國家安

[231] 法務部 103 年 11 月 17 日法律字 10303513040 號函釋節錄：「編號、護照號碼、…及其他得以直接或間接方式識別該個人之資料。是以，如將公務機關保有之個人資料，運用各種技術予以去識別化，而**依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自非個資法之適用範圍**。」

本報告之智慧財產權屬於國家通訊傳播委員會

全或增進公共利益所必要。」，如通傳會希望於調處目的外利用上開資料，應係基於達成其他法定職務之目的，通傳會可依本條但書第 1 款規定，檢視該法定職務是否有組織法或作用法之依據。

B. 若通傳會係依據本條但書第 2 款規定，基於促進渠等事業之健全發展、保障公眾視聽之權益等公共利益，得將上開資料為目的外利用。惟「公共利益」係一不確定法律概念，於適用上應審慎為之。

(3) 如通傳會欲將收視行為資料提供予其他公務機關或學術研究機構，須評估《個人資料保護法》第 16 條但書第 5 款之規定：

A. 按《個人資料保護法》第 16 條但書第 5 款規定：「但有下列情形之一者，得為特定目的外之利用：五、公務機關或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經蒐集者依其揭露方式無從識別特定之當事人。」

B. 依據實務見解[232]，可知通傳會基於上開公共利益，得將收視資料進行處理，使其無從識別特定用戶後，提供予他公務機關或學術研究機構，作為統計及學術研究之用途；亦可在確保資料接

[232] 法務部 104 年 7 月 2 號法律字第 10403508020 號函釋節錄：「依上開規定，**原保有之公務機關（即提供者）可將得直接或間接識別之個人資料經過處理後，使其無從識別特定個人，再提供予其他公務機關或學術研究機構（即「資料經過『提供者』處理後...無從識別特定之當事人」）；或由原保有之公務機關（即提供者）提供得直接或間接識別之個人資料，交予其他公務機關或學術研究機構（即蒐集者）保有，由蒐集者進行彙整、統計分析後，再以無從識別特 當事人之方式為研究成果之發表**（即「資料經過...『蒐集者』依 其揭露方式無從識別特定之當事人」）（本部 104 年 5 月 5 日法律字第 10400065570 號函意旨參照）。是以，依個資法第 16 條但書第 5 款之規範意旨，公務機關所保有之個人資料，並非一律均須達無從以直接或間接方式識別該特定個人者後，方得提供予其他公務機關或學術研究機構，重點在於統計或學術研究成果發表時，依其呈現或揭露方式必須已無從識別特定之當事人。」

本報告之智慧財產權屬於國家通訊傳播委員會

收者依其統計或研究後之揭露方式，**無從識別特定用戶**之前提下，提供可識別用戶之收視資料予他公務機關或學術研究機構。惟後者因涉及用戶個人資料之提供，對用戶之風險較大，建議通傳會評估以訂定規則或簽訂契約等方式，明確規範或約定接收者對用戶收視資料之義務，併此敘明。

第二節 議題二：電信事業之定型化服務契約條款研析

通傳會依電信管理法第 17 條規定，為審核相關電信事業之定型化服務契約條款內容，其中針對「用戶個人資料蒐集、處理與利用之限制及條件」應如何檢視審理，以避免人格權遭受侵害，並促進電信事業合理利用用戶個人資料，以下研析相關適法之程序及見解，並提出具體可行之建議。

一、 定型化契約之限制與對策

(一) 電信管理法第 17 條之制度設計

1. 按《電信管理法》第 17 條第 1 項：「經主管機關認定之電信事業應訂定定型化服務契約條款，載明與用戶之權利義務關係，並於實施前送主管機關核准；變更時，亦同」，可知電信事業之定型化契約必須於實施前送交主管機關核准。
2. 又依據上開條文之立法理由，送交主管機關（即通傳會）核准之目的係為使通傳會得審查業者對用戶權利義務之擔保，以減少電信消費之爭議。
3. 故本研究建議，通傳會得要求電信事業於定型化服務契約條款中，加入以下條文：

   第 OO 條

   I. 甲方（電信業者）為提供服務，依個人資料保護法

本報告之智慧財產權屬於國家通訊傳播委員會

蒐集、處理、利用乙方（用戶）個人資料（包含但不限於通信或帳務紀錄）。甲方應對其負保密義務及採取適當安全措施，提供乙方查詢、閱覽、製給複製本、補充或更正個人資料，並依法提供有關機關調閱。

II. 前項個人資料，如甲方有個資蒐集目的外之利用，應先取得乙方同意。惟經甲方去識別化，並確認無法回溯而再識別乙方之資料時，得提供予第三人使用。

III. 如甲方於本服務契約外另有個資蒐集目的，應善盡告知義務並取得乙方同意。

(二) 定型化契約之限制

1. 雖然通傳會基於減少電信消費爭議之目的，要求電信業者將載有「用戶個人資料蒐集、處理與利用之限制及條件」之定型化契約送交並核准。然如前所述，記載之內容僅係重申《個人資料保護法》之誡命，此時通傳會恐無法藉由單純審核定型化契約，發揮監理之功能，並達到減少電信消費爭議之目的。
2. 若通傳會希望藉由審查「用戶個人資料蒐集、處理與利用之限制及條件」，達到電信監理目的，本研究建議通傳會仍應實質審視電信事業之「個人資料告知聲明」。然電信事業依據《個人資料保護法》第 8 條規定訂定之應告知事項，是否有必要載入定型化契約[233]，一併送交主管機關核准，則有討論空間。
3. 按《電信管理法》第 17 條規定，似認為應將「用戶個人資料蒐集、處理與利用之限制及條件」，均記載在定型化

[233] 定型化契約是否均應記載至同一份文件中，尚有討論空間。依據《消費者保護法》第 2 條第 7 款規定：「定型化契約條款：指企業經營者為與多數消費者訂立同類契約之用，所提出預先擬定之契約條款。定型化契約條款不限於書面，其以放映字幕、張貼、牌示、網際網路、或其他方法表示者，亦屬之」，可知定型化契約條款不需記載於同一份文件，甚至得以牌示、網路等方式表示。

本報告之智慧財產權屬於國家通訊傳播委員會

契約中，一併送交主管機關核准，然其中是否包含個人資料告知聲明，仍有所疑義。

4. 對電信業者而言，個人資料告知聲明因應電信科技的發展，常有調整之需要，若將其作為定型化契約之一部分，可能造成每次調整時，均需再送交通傳會核准，除了提高業者之成本外，亦可能造成個人資料告知聲明僵化、沒有彈性之反效果。此時，站在主管機關之立場，若要求電信業者將其個人資料告知聲明一併作為定型化契約送交核准，反而無法達到保護消費者，及減少電信消費爭議之目的。
5. 再考量現今各主管機關訂定之定型化契約應記載及不得記載事項，對於個人資料之規定，幾乎僅出現在不得記載事項中，例如不得對消費者個人資料為契約目的必要範圍外之利用、不得約定消費者預先拋棄或限制個人資料權利之行使等。對於業者蒐集、處理及利用個人資料之行為，似無嚴格要求需經主管機關審查管理。
6. 準此，本研究建議，於定型化契約管制之實務現狀下，似不宜將電信業者之個人資料告知聲明作為定型化契約之一部分，進而需依據《電信管理法》第 17 條送交主管機關（即通傳會）核准。

(三) 通傳會得以行政檢查或行政指導之方式，強化定型化契約之核准效果

1. 縱如前所述，個人資料告知聲明不需送交通傳會核准，亦可達到主管機關保護電信消費者之目的，及監理之有效性。通傳會應得於行政檢查之法定職權範圍內，要求電信業者提交個人資料告知聲明以供檢查。
2. 除了行政檢查以外，通傳會亦可依據《行政程序法》第 165 條規定，採取行政指導之方式，以輔導、協助、勸告、建議等不具法律上強制力之方法，請電信業者提供

本報告之智慧財產權屬於國家通訊傳播委員會

個人資料告知聲明，以供通傳會協助或輔導電信業者，調整個人資料告知聲明之內容，確認其之適法性。

二、 個人資料告知聲明之檢視基準

(一) 隱私權政策／個人資料告知聲明之檢視基準

1. 依據《個人資料保護法》第 8 條第 1 項[234]規定，非公務機關依同法第 19 條規定向當事人蒐集個人資料時，應盡告知義務，因此各大電信業者均訂有隱私權政策或個人資料告知聲明，以符合《個人資料保護法》之要求。
2. 除《個人資料保護法》第 8 條要求告知之內容外，依據《個人資料保護法施行細則》第 16 條之規定，告知之方式，應以足使當事人知悉或可得知悉之方式為之。故通傳會亦應檢查電信業者告知之形式，茲將告知形式之檢查標準整理如下表，其中有部分備註內容係參考歐洲個人資料保護委員會發布之透明性原則指引。

[234] 個人資料保護法第 8 條：「公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，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。」

本報告之智慧財產權屬於國家通訊傳播委員會

表 11 告知之形式上要求檢查清單

告知形式之要求	備註
□足使告知之對象易於理解	1. 業者之告知內容應依照受告知人之年齡、生活經驗及理解能力，以容易理解、清楚簡單之語言或文字為之，並使受告知人得充分瞭解其個人資料之後續利用狀況[235]。 2. 基於電信業者服務之客戶年齡差距甚大，應提供各年齡層都可以清楚理解之文字。
□告知事項便於取得	1. 例如業者在網站上公布個人資料告知聲明時，應以常用之術語表示個人資料告知聲明之連結，如隱私權政策、個資告知聲明、個人資料條款等；且連結之位置需置於網站上容易發現之處[236]。 2. 在實體門市可將個資告知聲明張貼在明顯可見的櫃檯或布告欄等位置，讓民眾方便閱讀。
□符合對行動應用程式（APP）之告知要求	APP的告知聲明資訊應在下載前得從網路商店（APP Store 或 Google Play Store）取得；下載後，相關資訊仍需在 APP 中易於取得，除此之外，該個人資料告知聲明宜針對 APP 設計，不應僅使用推出 APP 公司之個人資料告知聲明[237]。

[235] 國家發展委員會 108 年 3 月 12 日發法字第 1082000384 號節錄:「業者另應踐行個資法第 8 條第 1 項相關法定應告知事項，徵諸上開立法理由，應使當事人得以充分瞭解後審慎為之，是業者之告知方式**應符合學童之年齡、生活經驗及理解能力，以容易理解、清楚簡單之語言或文字為之，並使該學童得以充分瞭解其個人資料之後續利用**。」

[236] 此基準參考歐洲個人資料保護委員會 EDPB 發布之 Guidelines on transparency。

[237] 此基準參考歐洲個人資料保護委員會 EDPB 發布之 Guidelines on transparency。

本報告之智慧財產權屬於國家通訊傳播委員會

告知形式之要求	備註
□採用清晰簡明之文字	告知內容不應模糊或概括[238]，以下臚列不良之案例[239]： 1. 我們可能會使用您的個人資料來開發新服務（該「服務」為何或該資料將被如何使用以協助開發皆不明確）； 2. 我們可能會將您的個人資料用於研究目的（該「研究」為何並不明確）； 3. 我們可能會使用您的個人資料以提供個人化服務(何謂「個人化」並不明確)。
	以下亦提供優良之範例[240]： 1. 我們將保留您的購物歷史記錄並使用您之前購買產品的詳細資訊，以便為您提供我們認為您也會感興趣其他產品之建議(此語句清楚表示將運用何種類型之資料、當事人將成為精準廣告對象且其資料將用於達到此目的)； 2. 為了瞭解用戶如何使用我們的網站，以便我們可以改善網站的直觀性，我們將保留和評估您最近造訪我們網站之資訊以及就您於網站上點選不同區塊之行為進行分析。(此語句清楚表示將運用何種類型之資料以及將進行何種類型之分析)； 3. 我們將會記錄您所點擊之本網站文章，依據您所閱讀的文章等相關資訊辨識

238 法務部 102 年 06 月 11 日法律字第 10203503280 號函釋節錄：「本參考範本所列「符合個人資料相關法令以自動化機器或其他非自動化之利用方式」之個人資料利用之方式，其內容過於模糊、概括，應予修正，俾使當事人明確知悉其利用方式為何。」

239 此基準參考歐洲個人資料保護委員會 EDPB 發布之 Guidelines on transparency。

240 此基準參考歐洲個人資料保護委員會 EDPB 發布之 Guidelines on transparency。

本報告之智慧財產權屬於國家通訊傳播委員會

告知形式之要求	備註
	出您的興趣，並於本網站對您提供精準行銷（清楚表示個人化所需為何，以及如何辨識當事人之興趣）。

資料來源：本計畫製作

3. 就告知之實質內容檢查，本文謹將《個人資料保護法》第 8 條要求之告知事項須注意之要點，整理如下表的檢查清單，供通傳會做為行政檢查之標準：

本報告之智慧財產權屬於國家通訊傳播委員會

表 12 《個人資料保護法》第 8 條要求之告知事項檢查清單

告知事項	檢查事項	備註
非公務機關名稱	□電信業者有完整呈現非公務機關之全名	盡量以非公務機關全名稱呼，例如「中華電信股份有限公司」而非「中華電信」，避免民眾閱讀時誤會是其子公司或是相關企業。
蒐集目的	□電信業者有臚列蒐集個人資料之特定目的 □蒐集目的與電信服務契約之目的具正當合理之關聯。	1. 特定目的可參考法務部公布之「個人資料保護法之特定目的及個人資料之類別[241]」，縱使非屬「個人資料保護法之特定目的及個人資料之類別」列舉之特定目的，亦可以將其表列，重點係要以民眾可以理解之方式呈現。 2. 蒐集目的必須與電信服務契約內容具正當且合理之關聯，不應臚列與電信服務契約內容不相關的特定目的（例如衛生行政）。
個人資料類別	□民眾得清楚知悉將被蒐集的個人資料種類為何	1. 須讓民眾閱讀後清楚知悉將被蒐集的個人資料種類為何，可參考「個人資料保護法之特定目的及個人資料之類別」，或以民眾可以理解之方式呈現。

[241] 法務部主管法規查詢系統，https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=FL010631（最後瀏覽日：2021/09/11）。

本報告之智慧財產權屬於國家通訊傳播委員會

告知事項	檢查事項	備註
	□電信業者有將蒐集的個人資料類別清楚羅列 □電信業者沒有以概括之方式描述將蒐集之個人資料類別。 □個人資料之類別與蒐集之目的具正當合理之關聯	2. 以分別羅列各資料類型，並舉例表示為妥。例如：「帳務資訊：包含您於本申請書填寫的之識別類及特徵類個人資料（須依法提供身分證明文件）、我們指配給您的號碼、通信紀錄、帳單紀錄與繳費方式、服務歷程紀錄，以及其他與您的帳號相關之個人資料。」 3. 不得概括表示，以免囊括範圍過大。例如：「依主管機關公告之個人資料類別（包括但不限於載於各項申請文件的客戶、其代理人及法定代理人的個人資料等）」。 4. 電信事業不得隨意臚列所有個人資料之類別，其仍需與個人資料之蒐集目的具有正當合理之關聯。
個人資料利用期間	□電信業者有表明個人資料之利用期間	除了具體描述利用期間之長短，至少應表明利用期間為「契約存續期間」，或「依法律規定得保存的期間」。
個人資料利用地區	□電信業者有表明其會在哪些地區利用個人資	尤應檢視電信事業是否載明個人資料傳輸至境外何地區利用，並評估是否經主管機關限制或禁止之。

本報告之智慧財產權屬於國家通訊傳播委員會

告知事項	檢查事項	備註
	料	
個人資料利用對象	□電信業者有表明會對哪些第三方機構或對象利用當事人之個人資料 □電信業者沒有以概括之方式描述上開對象 □將當事人個人資料提供予第三方之行為符合蒐集之目的	1. 建議具體描述對象之類型或提供範例，例如：「我們可能會將您的個人資料提供給受我們委託之關係企業或第三人（例如行銷／分析／廣告／公關業者、物流業者、金流業者、資訊服務業者等）。」 2. 而非概括式的描述，如「本公司、本公司委託或有合作、業務往來關係之關係企業及合作廠商」。 3. 如遇跨業行銷之情形，請注意提供予第三方之行為有無符合電信服務契約及蒐集之特定目的。例如電信公司與遊戲公司合作，需要將資料提供予遊戲公司，此與電信服務契約及蒐集之特定目的不符，應另行取得當事人同意，方得為之。
個人資料利用方式	□電信業者有清楚羅列利用個人資料之各個方式	1. 清楚羅列各種利用方式，並簡述內容，例如「寄送帳單／催繳訊息至您或實際使用本服務者之地址或電子郵件信箱；藉由電話聯繫或簡訊通知您或實際使用本服務者有關繳費／催繳的資訊。」

本報告之智慧財產權屬於國家通訊傳播委員會

告知事項	檢查事項	備註
	□電信業者沒有以概括方式描述利用當事人個人資料之方式	2. 不建議採概括式的描述，概括描述甚至可能違反《個人資料保護法》規定，因為無法清楚告知當事人其利用方式的具體內涵為何，例如：「合法範圍之利用」。
當事人依第 3 條規定得行使的權利及方式	□電信業者有清楚羅列《個人資料保護法》第 3 條規定之當事人權利 □電信業者有提供當事人行使權利之管道	羅列《個人資料保護法》第 3 條規定之當事人權利，及當事人行使權利的管道。例如：您得依法行使請求查詢、閱覽、補充、更正；請求提供複製本；請求停止蒐集、處理、利用；請求刪除個人資料等權利，欲行使權利請洽本公司免費客服電話：0800-xxx-xxx 或 E-mail: xxxxx@xxxxx.com
當事人得自由選擇提供個人資料時，不提供將對其權益的影響	□電信業者有清楚說明當事人不提供個人資料時會對其造成哪些影響	清楚說明若當事人不提供相關個人資料，可能對當事人造成的影響為何，例如：「將無法即時收到與本服務相關的必要資訊。」

資料來源：本計畫製作

本報告之智慧財產權屬於國家通訊傳播委員會

(二) 電信事業以同意作為蒐集及處理用戶個人資料之依據時，需確認同意是否有效

1. 按《個人資料保護法》第 19 條第 1 項第 5 款規定：「非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：五、經當事人同意」。可知若電信事業以「經當事人同意」作為個人資料蒐集及處理之合法事由時，亦有檢視用戶之「同意」是否為有效同意之必要。
2. 次按同法第 7 條第 1 項規定：「第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示」，用戶之「同意」必須在蒐集者揭露應告知事項後，始能提出同意之意思表示，因此同意是否有效，亦應檢視蒐集者是否已合法告知用戶應揭露之事項。
3. 又按《個人資料保護法》第 8 條第 1 項規定，電信業者於蒐集客戶之個人資料時，必須告知其所規定之事項，若電信業者之個人資料告知聲明不合乎《個人資料保護法》之要求，其所取得客戶之「同意」亦會有所瑕疵，並非有效之同意。關於個人資料告知聲明之審查標準已陳明於本研究「個人資料告知聲明之檢視基準」之章節，供通傳會參考。

(三) 電信事業以同意作為目的外利用之依據時，亦需確認同意是否有效

1. 按《個人資料保護法》第 20 條第 1 項第 6 款規定：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：六、經當事人同

本報告之智慧財產權屬於國家通訊傳播委員會

意」。通傳會除了審查電信業者蒐集用戶個人資料時，應揭露之告知聲明以外，若業者將來以「經當事人同意」作為目的外利用之事由時，亦需檢視用戶之「同意」是否合法。

2. 又按《個人資料保護法》第 7 條第 2 項規定：「第十六條第七款、第二十條第一項第六款所稱同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示」，據此，電信事業即應清楚告知當事人預計增加之特定目的、需要之個人資料範圍，以及若當事人不提供時可能產生之影響，其取得當事人對目的外利用個資行為單獨表示之同意，始為合法。

(四) 有效同意之補充判斷標準

1. 綜上所述，若個人資料之蒐集處理及個人資料之目的外利用，以「經當事人同意」作為合法事由時，即需審查其當事人之「同意」是否合法。
2. 除了上開我國個資法第 7 條第 1 項與第 2 項的「知情同意」明文規定外，比較法上對於「同意」之其他要件，似亦可解釋為我國個資法關於「同意」之內涵。本研究茲整理歐洲個人資料保護委員會EDPB發布關於同意之指引，提出有效同意之要件如下表，供通傳會參酌[242]。

表 13 有效同意之要件

有效同意之要件	
自主性	當事人需自主給予同意，具有選擇與控制權，並非受到強迫而做出同意。 例如有一 APP 要求使用者提供逾越其核心服務之個人資料，且使用者若不同意即無法使用服務，此同意

[242] 本表僅供通傳會參考，若電信業者對如何取得當事人有效同意有所疑義，通傳會得依本表內容進行行政指導。

本報告之智慧財產權屬於國家通訊傳播委員會

有效同意之要件	
	無法被認定為自主給予。
特定性	當事人必須針對一個或數個「特定」目的給予同意，且當事人對個別目的均有選擇權。 例如：某電信業者基於用戶同意蒐集用戶個人資料，依用戶之使用習慣針對用戶提出個人化建議。一段時間後，該電信業者決定要讓第三方依照用戶之使用習慣進行精準行銷。為了此一新目的，必須另行獲得同意[243]。
知情性	當事人在給予同意前必須先了解自己同意之內容。 若係針對業者蒐集客戶個人資料之同意，此時即應檢視業者之個人資料告知聲明是否合乎《個人資料保護法》之要求；如針對業者目的外利用之同意，則應檢視業者告知之特定目的、範圍及同意與否之影響。
明確性	當事人必須以行動表示清楚明顯之行為。 例如：在安裝軟體時，應用程式要求當事人同意利用非匿名的當機報告以優化軟體。藉由主動勾選「我同意」之框格，使用者即可有效作出「清楚肯定之行為」以同意運用個資。
可撤回性	當事人之同意可以被撤回。 倘業者基於當事人同意合法蒐集、處理之個人資料，而當事人事後撤回其同意。則自其撤回時起，如蒐集個人資料之特定目的或要件已不存在，除有上開個資法第 11 條第 3 項但書規定之情形外，業者應主動或依當事人之請求，刪除、停止處理或利用該等個人資料[244]。

資料來源：本計畫製作

[243] 參見歐洲個人資料保護委員會 EDPB 發布之 Guidelines on consent，改編自其中案例。

[244] 參見國家發展委員會，個資法問與答，https://pipa.ndc.gov.tw/News_Content.aspx?n=7D3602579D2BF23F&sms=2F28806F8A42AE16&s=C179B0C8D448D449（最後瀏覽日：2021/08/25）。

本報告之智慧財產權屬於國家通訊傳播委員會

3. 符合上開要件後，電信業者仍需透過各種方式，以取得客戶之同意，本研究參考歐洲個人資料保護委員會EDPB發布之指引，臚列數個電信業者可取得同意之方式如下[245]：

(1) 藉由書面聲明確認同意

電信業者可確保當事人於書面聲明中簽名，以避免將來之質疑，且得於發生爭議時舉證。

(2) 以雙向簡訊取得同意

例如電信業者希望將用戶個資提供予第三方進行行銷，因此需要用戶同意目的外利用，爰發送雙向簡訊，讓用戶得藉由回覆指定數字提供明確同意（例如回覆1為同意；回覆2為不同意）。

(3) 藉由口頭上告知取得同意

只要相關告知內容清楚且可理解，亦可以透過電話或當面對話獲得明確同意。例如：進線電信業者電話客服時，客服以錄音或口頭方式進行告知並取得客戶同意後，再開始蒐集客戶個人資料。

(4) 雙階段認證

舉例而言，當事人收到一封電子郵件，業者在信中解釋，基於特定目的請求同意使用特定資訊。如當事人同意其使用個人資料，業者要求以電子郵件回覆「我同意」之聲明。當事人在寄出回覆後，即收到必須點選之驗證連結，或含有驗證碼在內之簡訊，以此確認同意。

三、 具體可行措施

(一) 通傳會得透過行政檢查或行政指導，檢視電信事業之個資

[245] 此些方式為例示而非列舉，電信業者仍可藉其他方式取得有效之同意。

本報告之智慧財產權屬於國家通訊傳播委員會

告知條款

1. 前已論及，似不宜將電信事業之個人資料告知聲明作為定型化契約之一部分，進而需一併送交通傳會核准。
2. 然為使通傳會仍能發揮監理之功能，爰建議通傳會得於行政檢查或行政指導時，在法定職權內，要求業者交付個人資料告知聲明，供通傳會檢查或協助電信業者調整。

(二) 通傳會參考本文整理之檢查清單，審查電信業者之個人資料告知聲明是否符合《個人資料保護法》之要求

1. 電信事業之個人資料告知聲明是否符合法規範之要求，應區分形式及實質內容之審查。
2. 對個人資料告知聲明形式內容之要求，主要係基於告知聲明呈現之方式，例如需要使告知對象亦於理解、告知內容需便於取得等，此部分請參照表 11 告知之形式上要求檢查清單。
3. 另外，就個人資料告知聲明之實質內容審查，係檢查是否符合《個人資料保護法》第 8 條要求之告知事項，本文亦將其整理成檢查清單，供通傳會於行政檢查及行政指導時使用，請參照表 12 《個人資料保護法》第 8 條要求之告知事項檢查清單。

(三) 通傳會亦應審查用戶之「同意」是否符合《個人資料保護法》之要求

1. 若電信業者於蒐集個人資料時需取得客戶之「同意」，此時依據《個人資料保護法》第 7 條 1 項規定，須先揭露應告知事項予用戶；再依據同法第 8 條第 1 項規定，檢視個人資料告知聲明是否符合《個人資料保護法》之要求；倘電信業者係為目的外利用，此時需檢視《個人資

本報告之智慧財產權屬於國家通訊傳播委員會

料保護法》第 7 條第 2 項規定告知之目的、範圍及影響。

2. 又客戶之「同意」需在「知情」之前提下「自主地」給予「特定」且「非模糊」之意思表示，方屬有效之同意，本文將上開要件整理如表 13 有效同意之要件，供主管機關參酌。
3. 電信業者亦可採取諸多方式取得客戶之同意，無論是透過口頭、電子文件、書面等方式，均得取得客戶有效之同意，通傳會得於行政檢查及行政指導時依具體情形判斷。

第三節 議題三：電信事業提供政府合理利用個資於跨領域共享

國際上因應 COVID-19 疫情發展，疫苗施打覆蓋率相對高之歐盟已逐步開放邊境，其中德國電信（Deutsche Telekom）於 2021 年 6 月底配合政府規劃，研發有關數位疫苗護照行動應用程式，使用藍芽功能與其他裝置接觸，即可提醒和警告接觸新冠病毒的風險。然就我國中央流行疫情指揮中心所規劃之「簡訊實聯制」措施，是否可參考德國該實例作法，如何讓電信事業提供及配合政府合理利用用戶之個人資料，並將用戶之身分認證資料共享予跨領域業務目的之使用（如數位疫苗護照）及其相關應用措施等作為？本計畫將先研析關於德國因應 COVID-19 應用程式 Corona-Warn-APP，以及相關資料應用法律依據，並對照我國現行疫情相關政策措施，以提供具體可行之建議。

一、 德國接觸者追蹤之 Corona-Warn-APP

2020 年 5 月初德國聯邦政府要求德國電信（Deutsche Telekom）子公司 T-Systems、軟體開發公司 SAP，與隸屬於德國聯邦衛生部疾病防治研究單位 Robert Koch Institut（RKI）合作，為德國提供官方追蹤 COVID-19 感染鏈的應用程式 Corona-Warn-APP[246]。該 APP 採取去中心化技術，資料僅儲存於行動裝置端，不會集中儲存，而當用戶

[246] Corona-Warn-APP open-source project, https://www.coronawarn.APP/en/ (last visited Aug. 24, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

接觸感染者，能獲得該 APP 即時通知，以抑制 COVID-19 傳染。2021 年 6 月 Corona-Warn-APP 2.3 版本更新後，用戶得以該 APP 掃描歐盟數位 COVID 證明（EU Digital COVID Certificate）[247]，以數位方式呈現證明疫苗接種狀態[248]。

(一) 運作模式

透過蒐集附近的識別符（identifiers），亦即行動設備上由 Apple 及 Google 共同開發的暴露通知系統（Exposure Notifications System, ENS）廣播滾動式接觸 ID（Rolling Proximity Identifier, RPI），定期掃描其他使用藍芽技術手機的 ID 並儲存。ID 僅在 10 至 20 分鐘內有效，且是 24 小時更換一次的臨時密鑰，並以加密方式產生，APP 將用戶的篩檢結果與症狀比對。而相關篩檢實驗室若有提供電子化流程，篩檢者可以使用其於篩檢時收到的 QR code 來確認結果。如果篩檢結果為陽性，用戶得將最近 14 日的臨時密鑰上傳，但為防止濫用，伺服器會將用戶密鑰加到 COVID-19 確認列表中，該列表定期廣播給所有 APP 用戶。最後該 APP 會確認是否接觸過確診者，亦即在行動設備下載篩檢為陽性用戶的密鑰列表後，暴露通知系統會產生相應的 ID，並檢查這些 ID 中是否與滾動式接觸 ID 匹配，以評估風險，而用戶則會收到相應指示。而前述透過藍芽發送隨機 ID，並不會發送或儲存個人資料、地理位置（geo-location）定位

[247] 從 Corona-Warn-APP 2.5 版本開始，Corona-Warn-APP 支援三類歐盟數位 COVID 證明，包含數位疫苗接種證明（digital vaccination certificate）、數位康復證明（digital recovery certificate）、數位陰性證明（digital test certificate）。

[248] 本文主要以整合接觸者追蹤、疫苗證明等功能之 Corona-Warn-APP 為主要說明，而德國還有專用於數位疫苗接種證明之 APP，亦即由 RKI 發布之 CovPass-APP 供德國人民掃描歐盟數位 COVID 疫苗接種證明，並產生一個 QR code 顯示疫苗接種或康復之證明，該 QR code 顯示資訊僅有接種狀態、名字、生日等資料。詳參 CovPass-APP, https://www.digitaler-impfnachweis-APP.de/en（最後瀏覽日：2021/09/11）。
而用於確認歐盟數位 COVID 疫苗接種證明之 APP 則是由 RKI 發布之 CovPassCheck-APP，檢查者以 CovPassCheck-APP 掃描歐盟數位 COVID 疫苗接種證明，顯示被檢查者之疫苗接種或康復證明有效性，並不會儲存任何資料，只會顯示被檢查人的證明、名字和生日等資料。詳參 CovPassCheck-APP, https://www.digitaler-impfnachweis-APP.de/en/covpasscheck-APP （最後瀏覽日：2021/09/11）。

本報告之智慧財產權屬於國家通訊傳播委員會

或其他位置資料。

(二) 資料安全與隱私保護

為強化用戶信任與資料隱私保護，以及提高 APP 使用率，透過開源架構文檔和使用條款，該 APP 基於 DP-3T 和臨時聯繫號碼協議（TCN，Temporary Contact Numbers Protocol），以及 Apple 和 Google 隱私保護追蹤者接觸（Privacy-Preserving Contact Tracing）規範，並僅處理針對評估個人感染風險與迅速了解篩檢結果之兩大目的所需之個人資料。依據 Corona-Warn-APP 隱私聲明（privacy notice）2.7 版本[249]載明關於該 APP 如何處理用戶數據資料以及用戶擁有的權利。該 APP 由 RKI 代表德國聯邦政府發布，並由其負責資料保護。若用戶篩檢呈陽性，並有使用跨國預警系統（transnational warning system）功能，也可以預警其他國家/地區的官方 COVID-19 應用程式的用戶，在此情況下，RKI 與跨國預警系統的國家衛生主管機關即為資料聯合控制者（joint controllers）。至於人民是否要下載該 APP 並無強制，亦即是否安裝、使用哪些功能以及是否與他人共享資料完全取決於用戶。關於個資傳輸，原則上該 APP 的所有主要功能需要將個資傳輸給 RKI 或其他用戶都要事先取得明確同意。

(三) 資料處理法律依據

依 GDPR 第 6 條(1)(a)[250]應獲得用戶事先明確同意，亦即用戶同意 RKI 出於暴露通知系統紀錄和通知他人之特定目的處理其個資，而涉及健康資料則是依 GDPR 第 9 條(2)(a)[251]規定。而關於數位 COVID-19 相關證明之法律依據

[249] Privacy notice, Corona-Warn-APP, Privacy notice, https://www.coronawarn.APP/assets/documents/cwa-privacy-notice-en.pdf (last visited Aug. 24, 2021).

[250] GDPR 第 6 條合法之處理應至少符合下列要件之一：(a)資料主體同意為一個或多個特定目的處理其個人資料。

[251] GDPR 第 9 條(2) (a) 除歐盟法或會員國法律規定資料主體不得排除第 1 項所定之禁止外，資料主體已明確同意為一個或多個特定目的處理上開個人資料。

本報告之智慧財產權屬於國家通訊傳播委員會

如下：

1. 疫苗接種證明（vaccination certificate）：依據 GDPR 第 9 條(2)(g)[252]與德國傳染病防治法（Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (Infektionsschutzgesetz - IfSG)）第 22 條(5)規定疫苗接種證明有效性認證人員。
2. 篩檢證明（test certificate）：依據 GDPR 第 9 條(2)(g)與 IfSG 第 22 條(7)規定篩檢證明有效性認證人員，以及篩檢陰性證明包含篩檢者姓名、生日、篩檢日期和篩相關資訊。
3. 康復證明（recovery certificate）：依據 GDPR 第 9(2)(g)條與 IfSG 第 22 條(6)規定康復證明有效性，以及康復證明包含篩檢者姓名、生日、篩檢日期和有關篩檢資訊。

為檢查前述證明有效性與真實性，而近用資料，則是依 GDPR 第 6 條(1)(e)[253]與德國聯邦資料保護法（Bundesdatenschutzgesetz, BDSG），第 3 條規定，為了執行控制者負責的任務或行使授予控制者的權力而需要進行處理，則應允許公務機關處理個人資料。此外，RKI 依聯邦衛生部所屬機構設置法（Gesetz über Nachfolgeeinrichtungen des Bundesgesundheitsamtes (BGA-Nachfolgegesetz - BGA-NachfG)）第 4 條規定 RKI 於職責範圍內向公眾報告，因此需要處理資料以提供統計數據。

該 APP 由 RKI 委託 T-Systems 和 SAP 公司營運和維護關於該 APP 基礎設施，如伺服器系統等，亦即這兩家公司是聯邦資料保護法規定之處理者。而歐盟執委會委託此二公司作為次處理者（sub-processor），負責跨國聯合預警系統技術管理。因此德國電信子公司 T-Systems 作為該 APP 資

[252] GDPR 第 9 條(2) (g)尊重資料保護之實質權利，並提供適當及具體之保護措施，以保護資料主體之基本權及利益，而基於歐盟法或會員國法律且與所追求目的合比例性之重大公共利益之理由所必要之處理。

[253] GDPR 第 9 條(2) (e)資料主體明顯已自行公開之個人資料之處理。

本報告之智慧財產權屬於國家通訊傳播委員會

料處理者，而實際上 T-Systems 並未利用到德國電信用戶電信資料，而該 APP 所蒐集資料原則上是透過當事人同意取得。

二、 我國接觸者追蹤措施：臺灣社交距離 APP 與簡訊實聯制

(一) 臺灣社交距離 APP

對照前述德國 Corona-Warn-APP，我國因應疫情接觸者追蹤也有推出以藍芽技術運作 APP，由我國衛生福利部疾病管制署（下稱疾管署）與行政院資安處、台灣人工智慧實驗室（Taiwan AI Labs）2021 年 5 月合作開發提出「臺灣社交距離 APP」[254]，利用行動裝置的藍芽訊號強度偵測使用者彼此間接觸的距離與時間，記錄使用者過去 14 天內接觸史。該 APP 為保護隱私[255]，無須註冊也不用上傳任何個人資料，而是利用藍芽記錄接觸對象藍芽識別碼，並不包含位置資料，資料僅儲存於行動裝置端 14 天，不會上傳到雲端集中儲存。當使用者接獲通知為確診者時，經衛生單位取得確診者同意後上傳資料，APP 將主動通知過去 14 天曾接觸過的對象，提醒用戶注意身體狀況。對照德國 Corona-Warn-APP 與臺灣社交距離 APP，兩者皆未有蒐集個人資料，且完全由用戶自由決定下載使用，以及當接觸確診者後自由決定是否上傳資料，而臺灣社交距離 APP 並無我國電信業者參與，因此並無電信業者配合提供相關電信資料問題。

(二) 簡訊實聯制

除了臺灣社交距離 APP 外，為落實實聯制掌握確診者足跡，我國中央流行疫情指揮中心（下稱指揮中心）於 2021

[254]疾病管制署，「臺灣社交距離 APP」已上架 鼓勵全民下載使用 掌握疫情擴散相關資訊，https://www.mohw.gov.tw/cp-16-60680-1.html（最後瀏覽日：2021/08/26）。

[255] 各國電信事業為公益配合提供電信資料應用案例與規範整理臺灣社交距離 APP 注意事項及個資保護說明，https://ailabs.tw/taiwan-social-distancing-APPpersonal-data-protection-note/（最後瀏覽日：2021/08/26）。

本報告之智慧財產權屬於國家通訊傳播委員會

年 5 月 19 日推出簡訊實聯制，該制度隱私權公告[256]說明由疾管署委託關貿網路公司製作並協助維運，並規定適用範圍、個人資料之蒐集、選擇、利用、共用、查閱與更正、個人資料正確性、資訊安全、自我保護措施、Cookies、公告之修正等，以及隱私權保護諮詢與救濟。

然而，簡訊實聯制推出後，引發許多質疑，如於防疫目的外利用簡訊資料作為犯罪偵查等[257]，因此指揮中心分別於 2021 年 5 月 23 日[258]、2021 年 6 月 29 日[259]發表聲明，簡訊實聯制透過民眾掃描 QR code 發送簡訊，不必註冊會員、不用填任何個人資料，店家也不會收到資料，僅傳送簡訊予民眾使用之電信公司，且只保留 28 天後銷毀，除非因疫調所需才會提供。而電信公司蒐集資料為「手機號碼、發送簡訊當下時間及場所代碼」等 3 項資料，聲明提到「這些資訊都是民眾原本使用的電信公司已有的資訊，是最小範圍的個資提供，且只保留 28 天後就會銷毀，只有當政府有疫調需求時，才會調閱這些資料，進而找出足跡」，對照該制度隱私權公告似無蒐集資料類型、保留期間之相關敘述。此外，聲明還有提到資料應用合法性、正當性、必要性：

1. 合法性：衛福部依傳染病防治法第 37 條第 1 項第 6 款公告「嚴重特殊傳染性肺炎（COVID-19）第三級疫情警戒標準及防疫措施裁罰規定」，規定配合實聯制，為遏止疫情擴散，減少實聯制紙本填寫之接觸，推出「簡訊實聯制」，供民眾及商家使用。
2. 正當性：簡訊實聯制係於經得使用人同意下，掃瞄 QR code 即完成實聯制措施；不會留下個資給店家，活動史

256 簡訊實聯制隱私權公告，https://emask.taiwan.gov.tw/real/info5.html（最後瀏覽日：2021/08/26）。

257 張淵森，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，2021/06/19，https://opinion.udn.com/opinion/story/120701/5542571（最後瀏覽日：2021/08/26）。

258 衛生福利部疾病管制署，網傳「簡訊實聯制監控人民行蹤」 指揮中心：不實訊息勿轉傳以免觸法，https://www.mohw.gov.tw/cp-17-60900-1.html（最後瀏覽日：2021/8/26）。

259 衛生福利部疾病管制署，簡訊實聯制數據係以合法性、正當性、必要性進行使用，絕無違法情事，https://www.cdc.gov.tw/Bulletin/Detail/HS0hjvHxAOTCPtNPmDo7Bw?typeid=9（最後瀏覽日：2021/08/26）。

本報告之智慧財產權屬於國家通訊傳播委員會

簡訊電信業者保留 28 天，僅供指揮中心疫調使用，不會做目的外利用。

3. 必要性：在疫調工作中，衛生單位人員須即時展開接觸者匡列、環境清消等防疫措施，適當的運用簡訊實聯制相關資訊有助防疫。

簡訊實聯制之隱私權公告並無說明關於疾管署與電信業者關係，以及電信業者蒐集資料與保留期間。雖德國官方無類似我國簡訊實聯制的措施，但德國民間 Nexenio 公司開發應用程式 Luca[260]，相當類似我國簡訊實聯制，該 APP 為私人會議和公共活動、商店和餐館提供接觸者管理和追蹤，同時整合德國衛生局資訊，以協助疫調查。而該 APP 隱私權政策[261]即明確提到 APP 之 IT 基礎設施服務（伺服器）由德國電信（Deutsche Telekom AG）提供，德國電信所處理資料包含「聯繫數據、功能數據、電信業者數據、附加輸入數據、臨時使用數據、檢測結果識別資訊、恢復或疫苗接種文件」[262]，以及伺服器所在位置於德國，而涉及電話號碼則會由德國電信處理且最多儲存 60 天。對照我國關於簡訊實聯制隱私公告並未明確說明電信業者處理資料有哪些，以及電信業者蒐集資料類型與保留期間，而是需要從新聞稿相關內容得知。

此外，指揮中心為協助精準疫調而建置「疫調輔助平臺」於 2021 年 7 月 26 日上線[263]，提供熱區地圖、疫調軌跡、簡訊實聯制疫調查詢等功能之整合平臺，並限制疫調之人員登入使用權限。其中關於整合簡訊實聯制資料，提供疫

260 Luca, https://www.luca-APP.de/ (last visited Aug. 27, 2021).

261 Datenschutzerklärung luca APP, https://www.luca-APP.de/APP-privacy-policy/ (last visited Aug. 27, 2021).

262 參照該隱私聲明(Datenschutzerklärung luca APP)C.第 2 條處理資料類型(Datenkategorien)與第 5 條接收者內部處理之個人資料(Empfänger:innen personenbezogener Daten)，亦即 GDPR 第 28 條所指的處理者。

263 衛生福利部疾病管制署，「疫調輔助平臺」7 月 26 日上線 指揮中心：運用資訊科技以便捷疫調工作，https://www.cdc.gov.tw/Bulletin/Detail/rVZ1dkbtACeqf4cypmsrkg?typeid=9（最後瀏覽日：2021/08/26）。

本報告之智慧財產權屬於國家通訊傳播委員會

調人員以電話或場所代碼進行疫調資訊之查詢及參考，調取紀錄詳實記載帳號使用人員、使用時間及內容，並將於日後開放使用紀錄之查詢。此外，關於 COVID-19 相關證明數位化，我國目前尚未推出官方數位證明，但 8 月中旬已在研議建立數位證明簽發平台，推動相關數位證明措施，現階段暫不會作為通行證[264]。對照歐盟推出歐盟數位 COVID 證明，而訂定歐盟數位 COVID 證明規則[265]，第 10 條即有規定個人資料保護，也適用歐盟 GDPR 規定處理個人資料，數位證明中的個人資料應僅應用於驗證其中的資訊，並有規定保留期間，以促進人民於歐盟內部自由移動。

三、 研析建議

綜上所述，本計畫研析關於德國因應 COVID-19 應用程式 Corona-Warn-APP 以及應用法律依據，並對照我國因應疫情相關措施以了解差異與值得參考借鏡之處。首先，關於德國 Corona-Warn-APP 與臺灣社交距離 APP，兩者皆是採取藍芽技術交換 ID，皆未有蒐集個人資料，也沒有涉及位置資料，且人民得自由決定是否下載使用，以及當接觸確診者後也能自願決定是否上傳接觸資料，而臺灣社交距離 APP 並無我國電信業者參與，因此並無電信業者配合提供電信資料問題。

(一) 關於簡訊實聯制隱私聲明應有詳細說明疾管署與電信業者關係，以及電信業者蒐集資料與保留期間

德國 Corona-Warn-APP 整合接觸者追蹤以及相關數位證明，並無類似我國簡訊實聯制措施。而關於我國簡訊實聯制之隱私聲明中並無說明關於疾管署與電信業者關係，以及電信業者蒐集資料與保留期間。然而參照德國 Corona-

[264] 中央社，COVID-19 疫苗數位證明平台 最快 8 月底上路，2021/08/17，https://www.cna.com.tw/news/firstnews/202108170190.aspx（最後瀏覽日：2021/08/26）。

[265] REGULATION (EU) 2021/953 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953 (last visited Aug. 27, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

Warn-APP 隱私聲明與網站問答，皆有詳細說明涉及 APP 資料控制者、處理者以及資料處理之明確法律依據，德國電信子公司 T-Systems 為該 APP 資料處理者，因此應遵守 GDPR 與德國聯邦資料保護法關於資料處理者規定，而實際上該 APP 並未利用德國電信用戶電信資料，而資料透過當事人同意取得。

此外，對照類似我國簡訊實聯制之德國民間公司推出之 Luca 作為接觸者管理和追蹤之應用程式，該 APP 隱私權政策明確提到 APP 之 IT 基礎設施服務（伺服器）由德國電信提供，德國電信所蒐集資料以及伺服器所在位置，而涉及電話號碼則會由德國電信處理以進行驗證且最多儲存 60 天。我國關於簡訊實聯制隱私公告並未明確指出電信業者處理哪些資料以及保留期間，而是於新聞稿內容呈現。

(二) 授權電信業者蒐集個資應有明確法律依據

我國現階段因應疫情相關措施，電信業者配合提供資料，主要是在簡訊實聯制，電信公司蒐集的資料為手機號碼、發送簡訊當下時間及場所代碼等 3 項資料，尚未涉及身分驗證資料，而是後續疫調勾稽確認。因此若需讓電信事業提供及配合政府合理利用用戶之個人資料，並共享予跨領域業務目的使用，於現行法下仍應回歸個資法第 4 條受公務機關委託蒐集、處理或利用個人資料，於個資法適用範圍內，應視同委託機關而應遵循個資法第二章有關公務機關蒐集、處理、利用個人資料之規範。若電信業者係受公務機關委託而蒐集人民個人資料用於公共利益，則電信業者依個資法第 15 條及第 16 條規定公務機關於執行法定職務必要範圍內蒐集處理個資，衛福部係依傳染病防治法第 37 條第 1 項第 6 款公告「嚴重特殊傳染性肺炎（COVID-19）第三級疫情警戒標準及防疫措施裁罰規定」為法律依據，並依個人資料保護法之特定目的及個人資料之類別中代號〇一

本報告之智慧財產權屬於國家通訊傳播委員會

二之「公共衛生或傳染病防治」蒐集個資追蹤接觸史。

政府若需要電信事業提供及配合政府合理利用其用戶之個資，除依據前述個資法規範外，對於法定職權解釋應有明確法律規定，作為合理利用依據，還應融入資料治理概念，事前進行隱私風險評估，甚至是隱私權政策內容應有細緻說明。而面臨後續資料共享建議訂定資料共享相關契約指引，甚至是明確我國去識別化技術，以及推動個資專責機關建立，以利於整體性掌握我國個資合理利用與隱私保護。

(三) 我國數位證明簽發平台仍在研議階段，得借鏡歐盟數位 COVID 證明規則

至於數位 COVID-19 證明，我國數位證明簽發平台仍在研議階段，現階段也暫未推動作為通行證。對照歐盟推出歐盟數位 COVID 證明，而訂定之歐盟數位 COVID 證明規則第 10 條針對個人資料保護規定：

1. 於執行本規則而處理個人資料時，應適用歐盟 GDPR 規定。
2. 根據本規則簽發的證明中所包含的個人資料僅應用於驗證證書，促進歐盟人民於 COVID-19 大流行期間在歐盟內自由移動權利。本規則適用期間結束後，不再能再處理。
3. 本規則第 3 條第 1 款證明包含的個人資料應由目的地或過境成員國的主管機關處理，或由該國家法律要求特定跨境客運服務業者處理。COVID-19 大流行期間的公共衛生措施，僅用於驗證和確認持有人的疫苗接種、檢測結果或康復情況，因此個人資料應僅限必要的資料。根據本項近用個人資料不得保留。
4. 為簽發規則第 3 條(1)的證明（包括簽發新證明）而處理的個人資料，簽發人保留資料不得超過其目的絕對必要的期間，以及該證明可用於行使自由移動權利期間。

本報告之智慧財產權屬於國家通訊傳播委員會

5. 成員國之間根據第 4 條(2)交換的任何證明撤銷清單在本規則適用期間結束後不得保留。
6. 負責簽發第 3 條(1)證明的機關或其他指定機構應被視為 GDPR 第 4 條(7)定義的控制者。
7. 負責 COVID-19 疫苗接種或篩檢的的自然人或法人、公共機關、機關或其他機構應向負責簽發證明的機關或其他指定機構傳送附件中所列之個人資料。
8. 本條第 6 項所述的控制者依 GDPR 第 28 條(3)規定之目的處理不得將個人資料傳輸到第三國。

歐盟面臨疫情已經逐步解封，並透過數位證明以有利於歐盟境內人民自由移動，而關於所涉及證明還有的個資有明確法律依據，亦即歐盟數位 COVID 證明規則與 GDPR 相關規定。我國後續若要推動數位證明仍應有完整評估與法律明確依據。

第四節 議題四：異業合作涉及跨領域業務資料應用促進當事人資料自主運用

歐盟 2021 年 6 月初宣布將推出數位錢包，並為民眾提供全功能的數位身分證明服務，以作為發展數位經濟基礎建設之一；然在國內之電信業者也曾推出 Hami pay、friDay 錢包、Wali 智慧錢包、GtPay，或與金融業、電商業、資訊業等推出異業結盟之行動支付服務等，惟該等服務所涉及跨領域業務目的之資料流通、整合、共享、應用等問題，本計畫將就政府機關角度，在促進當事人資料自主運用上，研析國際上相關作法（如政策或規範等）並提出具體可行之建議。

一、 歐盟數位錢包

歐洲執委會 2021 年 3 月 9 日，提出《歐洲的數位十年：2030 年數位目標》（Europe’s Digital Decade: digital targets for 2030），設定到

本報告之智慧財產權屬於國家通訊傳播委員會

2030 年所有關鍵公共服務皆應可以透過線上方式提供，且歐盟全境需有 80%的公民加入使用電子身分證（eID），以強化歐盟境內所有民眾（包括身心障礙人士）公共服務之近用權（right of access）。為實現此目標，執委會於同年 6 月提出歐洲數位身分（European Digital Identity）的框架，建議創建名為「數位錢包」（digital wallet）的身分認證，可以在 27 個歐盟成員國間使用，用來存取公共服務或是共享電子文件[266]。在此框架下成員國將整合國家數位身分證和其他個人身分證明文件，包括駕照、文憑與銀行帳戶等。在該成員國核可的前提下，數位錢包可以由該國政府或是私人企業來提供。未來任何歐盟公民、居民或是企業皆可使用此數位錢包，作為驗證個人身分以近用整個歐盟的公共或私人數位服務，人民也能夠自由選擇與第三方共享哪些身分資料，並追蹤共享後之利用情況。

(一) 運作模式與使用範圍

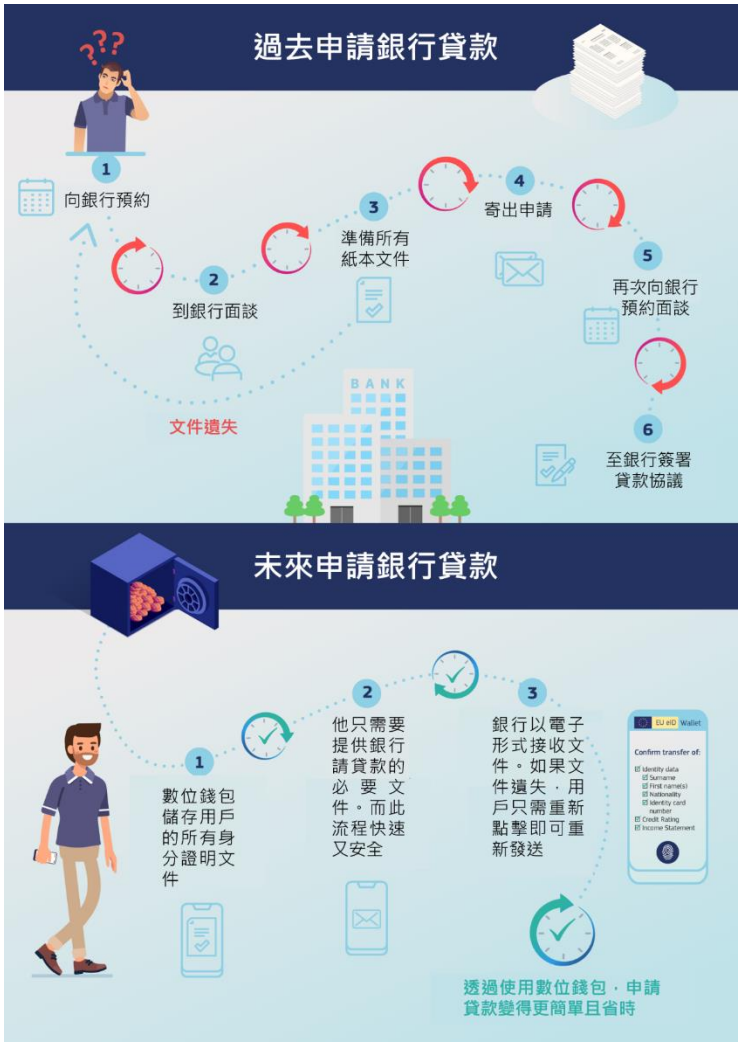
數位錢包的規劃並非字面意義上之數位支付功能，而是透過數位方式識別個人身分、儲存和管理電子格式的身分資料和官方文件，以近用線上服務、共享數位文件，或者證明特定的個人特徵（例如年齡），擴大歐洲發展數位商務的可能性。目前有關數位錢包的具體細節都仍在規劃中，預計要到 2022 年才能確定其運作功能。目前規劃之數位錢包應用情境，例如：公共服務（申請出生證明、醫療證明、地址變更）、開設銀行帳戶、提交納稅申報表、在國內或其他成員國申請大學、儲儲存可在歐洲任何地方使用的醫療處方箋、證明年齡、使用數位駕照租車、入住飯店等等。

以申請銀行貸款為例，過去申請銀行貸款需要安排實體會議、蒐集申請者資料和簽署紙本文件，若文件遺失，則需重複這些步驟。若未來透過數位錢包，申請者只需選擇儲儲存在其數位錢包中的必要文件，即可回覆銀行所需要的

[266] European Commission, Commission proposes a trusted and secure Digital Identity for all Europeans (June 3, 2021), https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663 (last visited Oct. 13, 2021).

本報告之智慧財產權屬於國家通訊傳播委員會

資料以建立可驗證的數位文件，並將其安全地發送給銀行進行驗證，然後銀行可以繼續進行申請流程（參圖 24）。



資料來源：本計畫編譯自 European Digital Identity

圖24　過去與未來申請銀行貸款之差異

(二) 資料安全與隱私保護

歐洲數位身分框架建立在數位錢包的基礎上，讓歐洲公民可以在他們的個人智慧型手機或設備上下載、安裝和使用數位錢包，以擴展國家 eID 的功能和可用性。在標準、技術規範和操作方面，歐盟成員國須有一致的規範，以確保各成員國的數位錢包皆具有最高的安全等級。而為減少技術差異，立法草案提到有關數位簽章的監管變化，以及網路

本報告之智慧財產權屬於國家通訊傳播委員會

瀏覽器如何解析及呈現儲存在傳輸層安全（Transport Layer Security, TLS）[267]證書中的任何身分資料。成員國將對其數位錢包進行認證，以確保它們符合這些要求，並且只有在使用者選擇共享該資料時，該個人資料才會線上共享[268]。

(三) 數位錢包法律依據

數位錢包以現有的可信賴數位身分跨境法律框架、歐洲電子身分和信任服務措施（electronic IDentification, Authentication and trust Servicese，下稱 eIDAS 規則）為基礎，並將其利益擴展到私部門，提供安全、免費、方便使用和保護個人資料的個人數位錢包服務。eIDAS 規則於 2014 年 7 月 23 日通過，引入公共機構、企業和個人之間數位跨境交流框架（cross-border and cross-sector framework），主要側重於電子身分識別、認證（authentication）和網站憑證（website certification）跨境使用的法律基礎架構。然而，因為 COVID-19 大流行導致人民與企業數位活動增加，快速變化的數位與法律環境以及因實施 eIDAS 規則而產生的問題，顯示出此項規則需要進行修訂。

因此，2020 年在公民與企業需要「簡單、可信賴與安全的線上身分識別」的推動下，宣布修訂 eIDAS 規則，而此次修訂之重點則在於資料保護、改善數位跨境服務，以及身分詐欺，並促進各會員國的數位身分（eID）計畫於歐盟境內的互操作性（interoperable），以線上服務的近用[269]。

首先，該修正案第 6a 條第 3 項將歐洲數位錢包定義為「允許用戶以透明可追蹤的方式安全地請求、儲存、選擇、組合與共享與其身分相關的資料及電子憑證（electronic attestation），根據用戶的請求將資料提供給信賴的第三方進

[267] 是一種標準的安全技術，透過資料加密，保護網路瀏覽器連接和線上交易安全。
[268] Jesse Kurtto, Could a pan-European digital identity be a reality by 2022?, Ubisecure (Sep. 13, 2021), https://www.ubisecure.com/authentication/european-digital-identity-framework/ (last visited Oct. 13, 2021).
[269] *Id.*

本報告之智慧財產權屬於國家通訊傳播委員會

行線上或實體的身分驗證，並建立合規的電子簽章。」意即此數位錢包的目的在於確保歐盟內的所有自然人和法人都能安全、可信賴和無縫地近用跨境公共和私人服務，成員國必須透過數位錢包提供驗證機制，以確保可以驗證數位身分的真實性和有效性、允許信賴第三方驗證身分證明是否有效，以及允許依賴第三方和合格的信任服務提供商（trust service providers）驗證用戶身分識別資料的真實性和有效性[270]。

第二，針對個人資料控制權限，修正案第 6a 條第 7 項規定，數位錢包的發行者將不會蒐集與提供錢包服務無關的錢包使用資料，也不會將個人身分資料和任何其他儲存或使用數位錢包相關的個人資料，提供給第三方服務或與其他第三方服務蒐集之個人資料結合。意即得以自主決定是否與第三方共享特定個人資料，並可追蹤其資料之後續利用[271]。

最後，根據第 12b 條，將擴大跨境 eID 計畫的相互承認，降低各會員國於電子身分識別服務的差距；並加強信賴服務提供的整體監管框架，針對信任服務提供商，新增為管理遠端電子簽章和封條（seal）產製設備（creation devices）所建立的新合格信賴服務（Qualified Trust Service, QTS）類型[272]。

二、 我國智慧錢包

(一) 我國智慧錢包發展概況

我國電信業者曾推出 Hami pay、friDay 錢包、Wali 智慧錢包、GtPay，或與金融業、電商業、資訊業等推出異業

[270] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, article 6.
[271] *Id.*
[272] *Id,* article 12.

本報告之智慧財產權屬於國家通訊傳播委員會

結盟之行動支付服務等。

1. Hami pay

   中華電信於 2011 年首次推出行動支付，但因當時行動支付環境尚未完備，因此是以「悠遊 NFC 背夾」PayPass 版登場。2014 年時推出 Easy Hami，2017 年更名為 Hami Wallet，最後於 2018 年 10 月定名為 Hami Pay，並聯合信用卡組織 Visa，新增聯邦銀行及中國信託信用卡及票證聯名卡功能[273]。並且於其 Hami Pay 服務暨隱私權條款與 Hami Point 啟用條款中提到 Hami Pay 已通過支付卡產業資料安全標準 PCI DSS（Payment Card Industry Data Security Standard，PCI DSS）安全認證[274]。

2. friDay 錢包與 friDay57

   2016 年 6 月遠傳電信推出 friDay 錢包，整合悠遊卡與 HappyCash 有錢卡等兩種電子票證，可綁定信用卡使用條碼消費，並結合 HAPPY GO 進行購物積點。2020 年 3 月時，遠傳電信更結合遠東銀行 Bankee 社群銀行與台新 Richart 數位銀行，將 friDay 錢包進行大幅度改版，運用 OPEN API 串接銀行帳戶的存錢計畫 App「friDay57」，可將多個存錢計畫串聯至不同銀行帳戶，有效管理存錢進度。

   使用者可以透過 friDay57 線上開立、或者綁定數位銀行如 Bankee、Richart 的帳戶，將每次的存錢進度與數位銀行帳戶餘額連動，提醒用戶存錢目標是否如期完成，幫助每個人務實達成目標。也可以綁定付款銀行帳號以及遠傳電信、信用卡、水費、停車費等帳單，在 App 內直接繳納帳單費用[275]。

---

[273] 王憶紅，中華電 Hami Wallet 再度更名為 Hami Pay 年底拚 200 萬用戶，自由時報，2018 年 10 月 1 日，https://ec.ltn.com.tw/article/breakingnews/2567367（最後瀏覽日：2021/10/24）。

[274] Hami Pay 服務暨隱私權條款與 Hami Point 啟用條款，中華電信，https://wserv.emome.net/EULAforNewHami（最後瀏覽日：2021/11/08）。

[275] 陳冠榮，friDay 錢包大改版，遠傳攜手 Bankee、Richart 推出存錢計畫 App，TechNews 科技新報，2020 年 3 月 5 日，https://technews.tw/2020/03/05/far-eastone-telecommunications-

本報告之智慧財產權屬於國家通訊傳播委員會

3. Wali 智慧錢包

台灣大哥大行動支付功能「Wali 智慧錢包」App 於 2016 年 1 月推出，結合消費支付、票券券收納，以及悠遊卡、一卡通兩大交通票證功能，希望以使用者為導向，提供電子票券收納與運用 NFC 傳輸技術的小額支付等不同類型的日常生活應用。

Wali 智慧錢包不僅限於台灣大哥大用戶，而是透過智慧型行動裝置下載 Wali App 完成帳號註冊，並選定一張信用卡作為支付設定後，即可開啟掃碼功能購買商品。另外，也可以透過 Wali 購買優惠票券，票券會存入 Wali 中，只要到商家出示電子票券序號與 QR code 就可使用。而在悠遊卡與一卡通之交通票證方面，只要手機是 Android 系統且支援 NFC 的台灣大哥大用戶，可以至全省電信門市可申請更換 NFC SIM 卡，完成儲值後就能開通功能，不用打開 App 就能直接感應，還可以在 Wali 中還看到詳細的儲值記錄、餘額等[276]。

惟台灣大哥大官網於 2021 年 5 月貼公告，自同年 9 月起 Wali 將不再提供服務。有關優惠券、停車費代收與 UUPON 服務移至台灣大哥大行動客服 APP；悠遊卡服務移轉至悠遊付 APP；信用卡服務移至 Google Pay 及 Samsung Pay；而全會員服務則轉至全家便利商店 APP[277]。

4. GtPay

亞太電信 2019 年推出 GtPay，不限於亞太電信用戶只要註冊 GtPay 會員，即可線上透過銀行活存帳戶繳納本人帳單。除支付功能外，GtPay 也結合路邊停車費綁定電

launches-friday-57-app/（最後瀏覽日：2021/10/24）。

[276] 曾靈，台灣大哥大行動支付鳴槍！「Wali 智慧錢包」上線搶 30 萬用戶數，數位時代，2016 年 1 月 28 日，https://www.bnext.com.tw/article/38596/BN-2016-01-28-172613-117（最後瀏覽日：2021/10/24）。

[277] Wail 服務移轉公告，台灣大哥大，https://www.wali.tw/event/13/（最後瀏覽日：2021/10/24）。

本報告之智慧財產權屬於國家通訊傳播委員會

信帳單代收功能，用戶在 GtPay APP 即可輕鬆綁定電信帳單代繳路邊停車費，目前可代收縣市包含新北市、桃園市、新竹市、新竹縣、台中市、台南市等六個縣市。而亞太電信用戶還可申請 PayTaipei 繳費功能，透過電信帳單代收包括臺北市路外停車費、臺北市路邊停車費、臺北市聯合醫療費、北水處自來水費，與學雜費等費用，或是未來臺北市政府智慧支付平台新增服務也自動納入 GtPay 服務代繳範圍[278]。從 GtPay 隱私權聲明中可知，GtPay 對於所有重要的個人資料均會經過安全加密保護，均以國際安全標準的 SSL protocol（Secure Socket Layer 通訊協定）加密處理。並透過 Message Authentication Code（MAC）的處理以確保資料的完整性。而對資料之保密義務，除其他法律規定外，雙方應確保所交換之電子訊息或一方因使用或執行本服務而取得他方之資料，不洩漏與他人，亦不得用於與本服務條款與隱私權條款無關之目的[279]。

(二) 電子支付相關法律依據

由上述業者發展案例可知，目前我國數位錢包之發展仍傾向於電子支付，而非歐盟數位錢包所期待之數位身分認證。有關我國電子支付之歷史，於 2001 年級有業者陸續投入電子支付或第三方支付領域，但當時無專法規範，造成監理與法規遵循的不明確與不安定。直到 2015 年，電子支付條例立法完成[280]。2020 年 12 月，立法院通過電子支付機構管理條例修法，並於 2021 年 7 月 1 日正式施行。本條例施行後將擴大電子支付機構之業務範圍，各電子支付機構

[278] 8 功能最齊全，亞太電信 GtPay 推智慧繳費，ePrice，2019 年 7 月 18 日，https://m.eprice.com.tw/telecom/talk/106/5374182/1/（最後瀏覽日：2021/10/24）。

[279] GtPay 行動支付服務條款與隱私政策，GT 智慧生活，https://gttvweb.wowotv.tw/event/GtPay/（最後瀏覽日：2021/10/24）。

[280] 陳絲倩、陳羿愷，電子支付市場的新變革 － 你需要知道的二三事，Winkler Partners 博仲，2021/05/19，http://www.winklerpartners.com/?p=11167&lang=zh-hant（最後瀏覽日：2021/11/08）。

本報告之智慧財產權屬於國家通訊傳播委員會

（含現行電子票證發行機構）針對新開放之業務項目，包括金流核心業務與附隨及衍生業務，可依規定檢具相關書件向金管會申請許可或備查，彰顯我國儲值支付工具管理法制整合工作之完成，為我國支付服務產業發展之重大里程碑[281]。

三、 研析建議

近兩年來受 COVID-19 疫情影響，遠距辦公或是希望保持社交距離之非接觸式生活方式，加速使用電子文件、電子簽章等數位工具的使用。歐盟數位錢包的主要目的是整合 eIDAS 規則，以一個單一的泛歐框架為公民和企業提供在跨境環境中有效識別自己的方法，並以高度安全、值得信賴和符合 GDPR 的方式交換個人身分資料和憑證。歐洲數位身分及錢包計畫是邁向「後疫情」時代、刺激經濟復甦之一環，現有的私人和公共電子識別參與者需要開始分析新的數位身分框架，考慮調整國家未來認證機制。

而我國有別於歐盟數位錢包之數位身分認證，目前發展大多仍侷限於「錢包」之電子支付功能，是以綁定信用卡之方式為支付工具，並非是將個人資料儲存於該數位錢包而有身分驗證之功能。與此同時，雖然我國欲推行數位身分證（New eID）政策，提供我國人民網路上身分識別之證明，連結政府骨幹網路（T-Road）串接各類電子政府服務，提升民眾近用公共服務的便利性，惟後續因安全性、法源依據等爭議而暫緩推行[282]。

因此，建議我國相關主管機關可參酌歐盟數位身分框架修正案，考量因應科技革新、商業模式創新等要素，對於身分識別相關規範進行修正與更新，以促進電子化政府及電子商務之發展，提供更具安全與信賴性的身分認證法律框架。期望我國政府能夠超前部署，從宏觀

[281] 金管會將於近日發布「電子支付機構管理條例」12 項授權法規命令並自 110 年 7 月 1 日施行，金融監督管理委員會，2021/06/24，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202106240004&dtable=News（最後瀏覽日：2021/11/08）。

[282] 行政院，暫緩數位身分證發行計畫 蘇揆:完善法制後再推動，2021/01，https://www.ey.gov.tw/Page/9277F759E41CCD91/e80e55a2-0102-4031-b6d3-a7c40f4cac6a（最後瀏覽日：2021/11/08）。

本報告之智慧財產權屬於國家通訊傳播委員會

的角度建立數位基礎設施工作。尤其在整合既有各種數位化憑證、疫苗護照及數位貨幣方面，更積極著眼未來於數位轉型並與國際接軌的目標前進。

第五節 議題五：中國大陸個人信息保護法簡介

中國大陸在 2021 年 8 月 20 日通過「個人信息保護法」，並於 11 月 1 日施行，惠請研析其內容重點規範？以及評估對我國電信產業之影響與建議。

一、 《個人信息保護法》重點規範

(一) 核心規範架構

1. 中國大陸於 2021 年 8 月 20 日通過，將於 11 月 1 日施行的《個人信息保護法》，與我國《個人資料保護法（為免混淆，以下稱個資法）》雖然均以歐盟為主要參考對象，然《個人信息保護法》引進諸多 GDPR 之新制度，整體規範密度較《個資法》嚴格。
2. 《個人信息保護法》之規範係以「告知—同意」為核心[283]，且參考 GDPR 之規定，要求「同意」應為當事人在充分知情下，自願且明確作出之決定[284]。且除了提供產品或服務所必須處理之個人資訊（即個人資料，以下稱個資）外，處理者不得將「同意」作為提供產品或服務之前提[285]。除此之外，《個人信息保護法》亦明定當事人撤回同意之權利，處理者需提供便捷之撤回同意方式[286]。

[283] 參見《中華人民共和國個人資訊保護法（草案）》的說明，http://www.npc.gov.cn/npc/c30834/202108/fbc9ba044c2449c9bc6b6317b94694be.shtml（最後瀏覽日：2021/12/29）。

[284] 個人信息保護法第 14 條第 1 項前段：「基於個人同意處理個人資訊的，該同意應當由個人在充分知情的前提下自願、明確作出。」

[285] 個人信息保護法第 16 條：「個人資訊處理者不得以個人不同意處理其個人資訊或者撤回同意為由，拒絕提供產品或者服務；處理個人資訊屬於提供產品或者服務所必需的除外。」

[286] 個人信息保護法第 15 條：「基於個人同意處理個人資訊的，個人有權撤回其同意。個人資訊處理者應當提供便捷的撤回同意的方式。」

本報告之智慧財產權屬於國家通訊傳播委員會

3. 此外，《個人信息保護法》對於敏感個人信息（下稱敏感資料）之認定，其範圍與《個資法》特種個資之規定不同，《個人信息保護法》將生物識別、宗教信仰、特定身分、醫療健康、金融帳戶、行蹤軌跡，以及未滿 14 歲的未成年人資料亦納入敏感資料[287]。
4. 在處理敏感資料時，必須取得單獨同意（或取得未成年人的父母或者其監護人的同意），且應執行事前之「個人信息保護影響評估」並保留紀錄[288]。

(二) 個資處理之原則

1. 透明原則
   (1) 依據《個人信息保護法》規定，個資之處理必須遵循透明原則，公開個資處理規則，並明示處理之目的、方式及範圍[289]。
   (2) 因此，個資處理者在處理前，必須揭露法定資訊，並顯著地以清晰易懂之語言，準確且完整地向當事人揭露。相較之下，我國《個資法》雖訂有應告知之事項，然未對告知之方式訂定規範，亦未明文要求個資之蒐集者是否能讓目標受眾易於理解或方便取得告知事項。
2. 自動化決策之限制
   (1) 中國大陸近年因大數據盛行，頻見「大數據殺熟」之案件，亦即業者利用用戶資訊，描繪出客戶各種偏好之輪廓，進而對價格不敏感者（尤其是熟客），進行同物不同價之價格歧視政策。舉例而言，用戶

[287] 個人信息保護法第 28 條前段：「敏感個人資訊是一旦洩露或者非法使用，容易導致自然人的人格尊嚴受到侵害或者人身、財產安全受到危害的個人資訊，包括生物識別、宗教信仰、特定身分、醫療健康、金融帳戶、行蹤軌跡等資訊，以及不滿十四周歲未成年人的個人資訊。」
[288] 個人信息保護法第 29 條前段：「處理敏感個人資訊應當取得個人的單獨同意。」；第 55 條第 1 款：「有下列情形之一的，個人資訊處理者應當事前進行個人資訊保護影響評估，並對處理情況進行記錄：（一）處理敏感個人資訊。」
[289] 個人信息保護法第 7 條：「處理個人資訊應當遵循公開、透明原則，公開個人資訊處理規則，明示處理的目的、方式和範圍。」

本報告之智慧財產權屬於國家通訊傳播委員會

利用訂房 APP 訂購旅館住宿，後發現其訂購之價格遠高於旅館實際收費，此一價格落差係基於訂房 APP 蒐集用戶個資，判斷其為熟客並對價格較不敏感，便於 APP 之介面中出示較高價格，以賺取更高利潤。

(2) 《個人信息保護法》亦針對大數據殺熟議題作出回應，要求個資處理者在利用個資進行自動化決策時，應確保決策之透明性和結果之公平公正，不得在價格等交易條件上為不合理之差別待遇[290]。上開規定藉由禁止價格歧視，並要求決策之透明性，進而避免大數據殺熟之行為。

(3) 此外，《個人信息保護法》要求個資處理者透過自動化決策方式進行行銷時，應同時提供消費者「不針對其個人特徵行銷」之選項，或便捷之拒絕方式[291]；若透過自動化決策方式作出影響對個人權益有重大影響之決定，當事人有權要求個資處理者說明，並得拒絕處理者「僅」透過自動化決策方式作出決定[292]。

3. 監視器之特別限制

(1) 在大數據、AI 等技術下，商店內監視器錄下之影像，往往被作為分析素材，藉由顧客之性別、年齡等資訊，描繪客群輪廓，進而做出商業決策。

(2) 《個人信息保護法》則對此情形作出規範[293]，若處

[290] 個人信息保護法第 24 條第 1 項：「個人資訊處理者利用個人資訊進行自動化決策，應當保證決策的透明度和結果公平、公正，不得對個人在交易價格等交易條件上實行不合理的差別待遇。」

[291] 個人信息保護法第 24 條第 2 項：「通過自動化決策方式向個人進行資訊推送、商業行銷，應當同時提供不針對其個人特徵的選項，或者向個人提供便捷的拒絕方式。」

[292] 個人信息保護法第 24 條第 3 項：「通過自動化決策方式作出對個人權益有重大影響的決定，個人有權要求個人資訊處理者予以說明，並有權拒絕個人資訊處理者僅通過自動化決策的方式作出決定。」

[293] 個人信息保護法第 26 條：「公共場所安裝圖像採集、個人身分識別設備，應當為維護公共安全所必需，遵守國家有關規定，並設置顯著的提示標識。所收集的個人圖像、身分識別資訊只能用於維護公共安全的目的，不得用於其他目的；取得個人單獨同意的除外。」

本報告之智慧財產權屬於國家通訊傳播委員會

理者在公共場所安裝足以識別身分之設備，應設置顯著提示，且除非取得個人單獨同意，所蒐集之個資只能用於維護公共安全之目的。

4. 經合法公開之個資處理

(1) 對於經本人自行公開，或其他已合法公開之個資，我國《個資法》保護之程度較低，除了在蒐集前不需揭露法定告知事項外，於處理及利用前亦不需另行告知。

(2) 惟《個人信息保護法》認為，雖然在本人未明確表示拒絕之情形下，處理者仍得以在合理之範圍內處理，然若處理者處理上開資料會對個人權益產生重大影響時，應取得個人之同意[294]，雖然此一重大影響為何，目前尚無具體之標準。

(3) 由此可知，依據《個人信息保護法》之規範，個人得藉由明確拒絕使處理者無法繼續處理其個資，若在處理上開資料會對個人造成重大影響時，也應取得個人同意，對經合法公開之個資保護較為周全。

5. 兒少個資之特殊規定：

《個人信息保護法》針對敏感資料中「未滿 14 歲未成年人」之個資，訂有更嚴格之規範，處理者處理上開資訊時除需取得兒少之法定代理人同意外，亦應制定專門之內部處理程序[295]。

6. 基於契約關係之個資處理：

《個人信息保護法》參考 GDPR，將依據契約關係處理之個資範圍限定於訂定、履行契約所必須，故縱使行銷內容與契約有合理關聯，可能仍需取得當事人同意[296]。

[294] 個人信息保護法第 27 條：「個人資訊處理者可以在合理的範圍內處理個人自行公開或者其他已經合法公開的個人資訊；個人明確拒絕的除外。個人資訊處理者處理已公開的個人資訊，對個人權益有重大影響的，應當依照本法規定取得個人同意。」

[295] 個人信息保護法第 31 條：「個人資訊處理者處理不滿十四周歲未成年人個人資訊的，應當取得未成年人的父母或者其他監護人的同意。」

[296] 個人信息保護法第 13 條第 1 項第 2 款：「為訂立、履行個人作為一方當事人的合同所必需，

本報告之智慧財產權屬於國家通訊傳播委員會

(三) 《個人信息保護法》之管轄範圍

1. 不同於中國大陸《網路安全法》和《數據安全法》將其適用限於中國大陸境內，只有在境外活動已嚴重損害境內利益時，例外追究責任。《個人信息保護法》借鑑GDPR，在中國大陸境外處理境內自然人個資之行為符合以下條件，適用《個人信息保護法》[297]：
   (1) 以向中國境內自然人提供產品或服務為目的；
   (2) 分析評估境內自然人之行為；
   (3) 法律或行政法規定之其他情形。
2. 中國大陸當局也提出另一項尚未通過之國家標準「資訊安全技術資料出境安全評估指南—徵求意見稿」，就「向中國境內自然人提供產品或服務」提出考量因素，包括使用中文（簡體字）、以人民幣為結算貨幣、向中國大陸境內配送物流等。若我國業者網站提供簡體字版本、提供向中國大陸配送之選項、APP 在中國大陸 APP Store 上架等，均有可能構成「以對中國境內自然人提供商品或服務為目的」，進而受《個人信息保護法》規範[298]。

(四) 跨境提供個資之規範

1. 我國業者若於中國大陸設廠，將大量中國大陸籍員工之個資傳輸回我國總公司人資部門時，依照《個人信息保護法》規定，將構成境外傳輸。如果處理的個人資料達

或者按照依法制定的勞動規章制度和依法簽訂的集體合同實施人力資源管理所必需」

[297] 個人信息保護法第 3 條：「在中華人民共和國境內處理自然人個人資訊的活動，適用本法。在中華人民共和國境外處理中華人民共和國境內自然人個人資訊的活動，有下列情形之一的，也適用本法：（一）以向境內自然人提供產品或者服務為目的；（二）分析、評估境內自然人的行為；（三）法律、行政法規規定的其他情形。」

[298] 資訊安全技術 資料出境安全評估指南（徵求意見稿）第 3.2 條：「境內運營 domestic operation 網路運營者在中華人民共和國境內開展業務，提供產品或服務的活動。注 1：未在中華人民共和國境內註冊的網路運營者，但在中華人民共和國境內開展業務，或向中華人民共和境內提供產品或服務的，屬於境內運營。判斷網路運營者是否在中華人民共和國境內開展業務，或向中華人民共和境內提供產品或服務的參考因素包括但不限於：使用中文；以人民幣作為結算貨幣；向中國境內配送物流等。注 2：中華人民共和國境內的網路運營者僅向境外機構、組織或個人開展業務、提供商品或服務，且不涉及境內公民個人資訊和重要資料的，不視為境內運營。」

本報告之智慧財產權屬於國家通訊傳播委員會

到規定的數量，原則上只能將資料儲存境內。

2. 《個人信息保護法》要求處理者於中國大陸境內傳輸個資至境外時，應採取必要保護措施，確保境外接收者之個資處理達到該法規範之要求[299]。而台灣業者作為個資之境外接收方，可能需配合認證，或簽訂標準契約，進而基於認證或契約，而有遵守《個人信息保護法》之義務[300]。

(五) 當事人之權利

1. 《個人信息保護法》除了賦予個資主體如知情權、決定權、刪除權等我國《個資法》亦有訂定之權利外，更參考 GDPR，訂定關於資料可攜權之規定。
2. 資料可攜權係允許自然人在符合特定條件時，得要求處理者將個資移轉予其他指定之接收者[301]。我國《個資法》目前無此規定。

(六) 個資處理者之義務

1. 特定企業需於中國大陸境內設立據點
   (1) 依《個人信息保護法》規定，符合特定條件之境外處理者，應於中國大陸境內設立據點或指定代表[302]。
   (2) 因此，境外個資處理者若以向中國大陸境內自然人提供產品或服務為目的；有分析、評估境內自然人

[299] 個人信息保護法第 38 條第 3 項：「個人資訊處理者應當採取必要措施，保障境外接收方處理個人資訊的活動達到本法規定的個人資訊保護標準。」

[300] 個人信息保護法第 38 條第 1 項：「個人資訊處理者因業務等需要，確需向中華人民共和國境外提供個人資訊的，應當具備下列條件之一：（一）依照本法第四十條的規定通過國家網信部門組織的安全評估；（二）按照國家網信部門的規定經專業機構進行個人資訊保護認證；（三）按照國家網信部門制定的標準合同與境外接收方訂立合同，約定雙方的權利和義務；（四）法律、行政法規或者國家網信部門規定的其他條件。」

[301] 個人信息保護法第 45 條：「個人有權向個人資訊處理者查閱、複製其個人資訊；有本法第十八條第一款、第三十五條規定情形的除外。個人請求查閱、複製其個人資訊的，個人資訊處理者應當及時提供。個人請求將個人資訊轉移至其指定的個人資訊處理者，符合國家網信部門規定條件的，個人資訊處理者應當提供轉移的途徑。」

[302] 個人信息保護法第 53 條：「本法第三條第二款規定的中華人民共和國境外的個人資訊處理者，應當在中華人民共和國境內設立專門機構或者指定代表，負責處理個人資訊保護相關事務，並將有關機構的名稱或者代表的姓名、聯繫方式等報送履行個人資訊保護職責的部門。」

本報告之智慧財產權屬於國家通訊傳播委員會

之行為；或法律、行政法有其他規定等情形時，均需於中國大陸境內設立據點。而處理者指定之代表，需負責處理個資保護相關事宜，並擔任主管機關之聯絡窗口。

2. 特定企業需設立個資保護負責人

(1) 《個人信息保護法》參照 GDPR，訂定類似個資保護長（DPO）之規定，要求處理個資超過政府規定數量之處理者，必須指定個資保護負責人[303]。

(2) 個資保護負責人之任務係監督處理者對個資之處理及保護措施，處理者應公開個資保護負責人之聯絡方式，並將其相關資訊提供予主管機關。

3. 特定情形需進行個資保護影響評估

(1) 《個人信息保護法》亦參考歐盟 DPIA，訂定個資保護影響評估之規定，評估報告和處理情形之紀錄應至少保存 3 年，而應評估之項目包括[304]：

A. 個資之處理目的、處理方式等是否合法、正當及必要；

B. 對個人權益之影響與安全風險；

C. 所採取之保護措施是否合法、有效且符合風險程度。

(2) 個人資料處理者在以下情形時，應於事前進行個資保護影響評估[305]：

303 個人信息保護法第 52 條：「處理個人資訊達到國家網信部門規定數量的個人資訊處理者應當指定個人資訊保護負責人，負責對個人資訊處理活動以及採取的保護措施等進行監督。個人資訊處理者應當公開個人資訊保護負責人的聯繫方式，並將個人資訊保護負責人的姓名、聯繫方式等報送履行個人資訊保護職責的部門。」

304 個人信息保護法第 56 條：「個人資訊保護影響評估應當包括下列內容：（一）個人資訊的處理目的、處理方式等是否合法、正當、必要；（二）對個人權益的影響及安全風險；（三）所採取的保護措施是否合法、有效並與風險程度相適應。個人資訊保護影響評估報告和處理情況記錄應當至少保存三年。」

305 個人信息保護法第 55 條：「有下列情形之一的，個人資訊處理者應當事前進行個人資訊保護影響評估，並對處理情況進行記錄：（一）處理敏感個人資訊；（二）利用個人資訊進行自動化決策；（三）委託處理個人資訊、向其他個人資訊處理者提供個人資訊、公開個人資訊；（四）向境外提供個人資訊；（五）其他對個人權益有重大影響的個人資訊處理活動。」

本報告之智慧財產權屬於國家通訊傳播委員會

A. 處理敏感資料；

B. 利用個資進行自動化決策；

C. 委託處理個資、向其他各資處理者提供個資、公開個資；

D. 向境外提供個資；

E. 其他對個人權益有重大影響之個資處理行為。

(七) 處罰規定

1. 《個人信息保護法》參考 GDPR 規定，採取重罰策略，對違法程度較輕者得令其限期改正、沒收違法所得、暫停或終止違法應用程式（APP），不改正得處人民幣 100 萬元以下罰款；另外直接負責之主管和其他直接責任人員也得一併開罰，可處人民幣 1 萬以上 10 萬以下罰款[306]。

2. 有重大違法時，除限期改正、沒收違法所得外，得處人民幣 5000 萬元以下，或前一年度營業額 5%以下罰款，也可令停業或吊銷營業許可及營業執照；對企業主管及其他應負責人員，可處人民幣 10 萬元以上 100 萬元以下罰款，還可禁止在一定期間內，擔任相關企業之董事等高階經理人和個資保護負責人[307]。

二、 對我國電信產業之影響與建議

(一) 電信業者可能適用個人信息保護法之情形

電信產業之態樣眾多，提供服務之種類不勝枚舉，本研

[306] 個人信息保護法第 66 條第 1 項：「違反本法規定處理個人資訊，或者處理個人資訊未履行本法規定的個人資訊保護義務的，由履行個人資訊保護職責的部門責令改正，給予警告，沒收違法所得，對違法處理個人資訊的應用程式，責令暫停或者終止提供服務；拒不改正的，並處一百萬元以下罰款；對直接負責的主管人員和其他直接責任人員處一萬元以上十萬元以下罰款。」

[307] 個人信息保護法第 66 條第 2 項：「有前款規定的違法行為，情節嚴重的，由省級以上履行個人資訊保護職責的部門責令改正，沒收違法所得，並處五千萬元以下或者上一年度營業額百分之五以下罰款，並可以責令暫停相關業務或者停業整頓、通報有關主管部門吊銷相關業務許可或者吊銷營業執照；對直接負責的主管人員和其他直接責任人員處十萬元以上一百萬元以下罰款，並可以決定禁止其在一定期限內擔任相關企業的董事、監事、高級管理人員和個人資訊保護負責人。」

本報告之智慧財產權屬於國家通訊傳播委員會

究以電信業者提供加值應用服務為例，探討是否有被《個人信息保護法》納入管制之風險。雖《個人信息保護法》相關子法尚不完備，然《個人信息保護法》之內容多有參照歐盟GDPR之處，因此本研究亦參考GDPR規定，分析如下：

1. 加值應用服務

(1) 我國電信業者推出許多加值服務，例如與銀行業合作，提供欠缺信用記錄之社會新鮮人，能以手機門號申辦貸款；電信業者亦推出諸多影音服務，諸如音樂串流平台、電子書平台、線上影音平台等，供用戶使用。

(2) 上開加值服務，均以持有手機門號為必要，換言之，電信業者僅提供上述服務予用戶使用。然有疑義者係，用戶使用上開服務時，未必身處於我國境內，可能位於中國大陸境內，此時電信業者提供之加值服務，是否會被視為「以向境內自然人提供產品或者服務為目的」？

(3) EDPB提供之指引提出一案例：一間澳洲公司依據用戶偏好及興趣，提供用戶行動新聞和影音內容服務，該服務係專門為澳洲用戶提供，用戶在訂閱時必須提供澳州之電話號碼。後訂閱該服務之用戶前往德國旅遊，並在德國繼續使用該服務，雖然該用戶於歐盟境內使用該服務，然此服務並非以位於歐盟之個人為「特定目標」，僅以位於澳洲之個人為目標，因此澳洲公司提供之服務不受GDPR規定拘束。

(4) 參考上述案例可知，即使在歐盟境內使用服務，亦未必構成「對歐盟境內之資料主體提供商品或服務」之要件，仍應評估該服務是否以位於歐盟之個人為「特定目標」。

(5) 若將上開論述適用於《個人信息保護法》，可知我國

本報告之智慧財產權屬於國家通訊傳播委員會

電信業者提供之加值應用服務多向持有我國電話門號之用戶提供，係專門為我國電信用戶提供之服務，縱使用戶前往中國大陸境內並使用上開服務，仍非以中國大陸境內之個人為「特定目標」。故我國電信業者提供之電信加值服務，應不構成「以向境內自然人提供產品或者服務為目的」。

2. 小結

雖因《個人信息保護法》相關子法規定尚未訂定周全，然上開法律於法條架構上大量借鏡 GDPR 規定，故 EDPB 依據 GDPR 發布之指引應具有參考價值。我國電信業者提供之服務，仍有構成「以向境內自然人提供產品或者服務為目的」之可能，進而需遵守《個人信息保護法》規定，為此，我國電信業者應及早設計因應措施。

(二) 電信業者應注意之事項

1. 可能需於中國大陸境內設立據點及代表

(1) 若我國電信事業以向中國大陸境內自然人提供產品或服務為目的，或有分析、評估中國大陸境內自然人之行為，依《個人信息保護法》規定，應於中國大陸境內設立據點或指定代表。

(2) 電信業者於設立據點或代表後，應將據點及代表之姓名、聯絡方式等資訊提供予主管機關。

2. 需符合透明性之要求

(1) 我國電信事業於取得中國大陸境內自然人個資前，需揭露法定資訊，並且以「顯著方式」、「清晰易懂之語言」、「真實」、「準確」、「完整地」揭露。

(2) 因我國《個資法》對透明性之要求並不嚴格，因此業者現行作法可能無法滿足《個人信息保護法》之要求。

(3) 故建議電信事業檢視自身之隱私權聲明或個資告

本報告之智慧財產權屬於國家通訊傳播委員會

知條款等相關文件，確認得否讓目標受眾便於取得及易於理解，本研究建議可參考歐盟之指引[308]。

3. 注意自動化決策之相關規定

(1) 我國雖然沒有大數據殺熟之爭議，但早有許多業者採用自動化決策作出決定，我國《個資法》對此卻無相關規定。

(2) 因此，若我國電信事業以自動化決策方式做出決定，應注意《個人信息保護法》之規定，除了要保證決策之透明度與結果之公正公平，亦不得對消費者有不合理之差別待遇。

(3) 除此之外，若電信事業以自動化決策方式向消費者進行行銷，應同時向消費者提供「不根據消費者特徵行銷」之選項，及方便之拒絕方式。

(4) 最後，若自動化決策作出之決定對消費者權益有重大影響，消費者有權要求電信事業說明，也有權拒絕「僅」利用自動化決策之方式作出決定。

4. 已合法公開個資之利用限制

(1) 前已論及，我國《個資法》對已合法公開之個資保護程度較低，除了在蒐集前不需揭露法定告知事項外，於處理及利用前亦不需另行告知。

(2) 然《個人信息保護法》則訂有較嚴格之規定，若希望處理已合法公開之個資（例如利用客戶註冊之email 至社群平台搜尋，取得客戶公開之資料，或客戶公開關注之商品及服務），電信事業可於合理範圍內處理，但客戶有拒絕之權利。

(3) 惟若電信事業之處理可能對客戶產生重大影響（目前仍未有判斷標準），則必須先取得客戶之同意始得處理。

[308] 參考歐洲個人資料保護委員會 EDPB 發布之 Guidelines on consent，國發會翻譯：https://www.ndc.gov.tw/Content_List.aspx?n=F98A8C27A0F54C30 (最後瀏覽日:2021/12/29)。

本報告之智慧財產權屬於國家通訊傳播委員會

5. 注意基於契約關係處理個資之限制

(1) 我國實務上《個資法》允許基於契約關係，於合理範圍內進行行銷，然《個人信息保護法》對此則有較嚴格之要求。

(2) 若電信事業基於契約關係處理客戶個資，依據《個人信息保護法》規定，依據契約關係處理之個資僅限於訂立、履行契約所必需。

(3) 故即使電信事業係基於契約關係，並於合理範圍內處理客戶之個資，仍有可能須取得客戶之同意。

6. 注意兒少個資之特別規定

(1) 我國《個資法》除未將未成年人個資歸類為特種個資外，亦無要求業者對特種個資之蒐集、處理或利用者應制定專門處理程序。

(2) 惟依據《個人信息保護法》規定，未滿 14 歲兒童之個資屬於敏感資料，故電信事業於處理上開資料時，必須檢視特定目的與必要性，同時採取嚴格之保護措施，並告知處理資料之必要性及對個人權益之影響。

(3) 除此之外，電信事業應取得其法定代理人之同意，亦須建立處理兒童少年個資之內部管理程序。

7. 注意個資跨境傳輸規定

(1) 若電信事業於中國大陸境內儲存個資，欲傳送至境外時，需要滿足《個人信息保護法》之規定，例如通過安全評估、經專門機構認證或與境外接收方訂定中國大陸政府制定之標準契約條款等。

(2) 此外，電信事業於傳輸客戶個資至境外前，應向客戶告知境外接收方相關資訊，包含客戶得向境外接收方行使《個人信息保護法》之權利，以及處理之方式及程序，並且需取得客戶單獨同意。

(3) 最後，若電信事業有於中國大陸境內大量雇用員工

本報告之智慧財產權屬於國家通訊傳播委員會

之需求，應特別注意，若處理之個資達到中國大陸政府規定之數量，原則上僅得將個資儲存於中國大陸境內，不得向境外傳輸。

8. 因應資料可攜權

(1) 資料可攜權常常被視為促進創新之關鍵，因其得釋放儲存於政府或民間企業內部之資料，使資料得被更靈活運用。

(2) 《個人信息保護法》亦有資料可攜權之規定，允許自然人在符合特定條件時，得要求處理者將個資移轉予其他處理者。

(3) 我國《個資法》尚無類似規定，因此電信業者除跟進《個人信息保護法》之規定外，應盡早評估因應方式，例如：如何提供結構化、機器可讀、普遍使用之檔案格式，以滿足資料可攜權規定之要求[309]。

9. 可能需設立個資保護負責人

(1) 《個人信息保護法》規定，處理一定數量以上個資之處理者，必須設立個資保護負責人，此一負責人類似於歐盟個資保護長(DPO)，需負責監督處理者對個資之處理及保護措施。

(2) 然「一定數量」為何，目前未有其他規範明定，惟若電信事業有於中國大陸境內大量處理個資之情形，應及早因應，準備設立個資保護負責人。

10. 可能需執行個資保護影響評估

(1) 電信事業處理個資，若包含《個人信息保護法》規定之情形之一，例如：處理敏感資料、利用個資作自動化決策、委託處理個資等，必須在事前執行個資保護影響評估。

(2) 其評估之內容也應依照《個人信息保護法》之規定，包含處理目的或方式之合法性、正當性、必要性，

[309] 參考歐洲個人資料保護委員會 EDPB 發布之 GDPR_Guidelines on the right to data portability。

本報告之智慧財產權屬於國家通訊傳播委員會

或是對客戶之安全風險及保護措施等。

11.注意巨額罰款

(1) 若電信業者違反《個人信息保護法》之規定，除了鉅額罰款外，亦有可能遭停業，或被吊銷業務許可及營業執照。除了對處理者之處罰外，對於企業主管或應負責人員，亦有相對應之罰款。

(2) 相較於我國《個資法》最高 50 萬元新台幣之罰鍰額度，《個人信息保護法》最高可處 5000 萬元人民幣（折合新台幣約 2 億），或上一年度營業額 5%之罰款。

(3) 此外，《個人信息保護法》亦無我國「已盡防止義務者免罰」之規定，因此電信業者應謹慎對待。

三、 結語

中國大陸《個人信息保護法》大量參考 GDPR 規範，加強對個資之保護，相對地也對處理者採取較嚴格之規範。除了高密度管制外，違法時巨額罰款，及可能被迫離開中國大陸市場之處罰，也讓業者必須審慎以對。

我國電信業者若無意進入中國大陸市場，須注意不要落入《個人信息保護法》之管制範圍，審視自身有無「向中國境內自然人提供產品或服務為目的」或「分析評估中國境內自然人」之行為。

若有意經營中國大陸市場者，則須遵循《個人信息保護法》之規定，詳細檢視對其之法遵差異，規劃整體因應方案，以降低業務營運之衝擊。

第七章 電信事業運用數據資料提供創新應用服務治理模式之相關決

本報告之智慧財產權屬於國家通訊傳播委員會

策作業流程標準之建議

第一節 決策流程建議

一、 建立網路公眾意見諮詢平台

本團隊於本次研究中，參考既有之公眾參與網路平台如 vTaiwan、i-Voting 等，以網路問卷方式彙整公眾對研究主題之意見。民眾認為電信業者應優先發展的創新服務，最多人選擇身分識別類（1333 人中有 428 人，32%），交通運輸類次之（352 人，26%），第三為金融科技類（275 人，21%），第四為商業應用類（199 人，15%）。可見本研究進行網路公眾意見諮詢過程中，發現大部分民眾並不反對電信事業運用資料進行創新應用、提供創新服務，惟最大疑慮在於業者是否能妥善保護資料。

建議可參酌本次研究經驗，建立一網路公眾意見諮詢平台，對於創新應用規劃及布建，廣泛徵詢各方利害關係人之意見、提出緩解公眾疑慮的具體作法，並將上開緩解作法納入服務設計，增加信賴。

此外，對於新機制如創新實驗監理沙盒的採行、運用資料提出創新服務指引的擬定，亦可運用該平台與網路公眾進行溝通，以增加周全度。

二、 主管機關間應協力促進電信資料運用之流程透明及安全

不涉及個資的數據資料，較無法規適用疑義，合先敘明。爰以下討論資料運用涉及個資的情形，從電信資料的運用態樣觀之及運用主體來看，可分為以下兩種模式。

(一) 電信事業將電信資料用於提供其他創新服務：

在此模式中，電信事業將資料用於電信服務的創新服務，屬於主動狀態控制資料利用之目的，而當創新服務涉及資料的二次利用（又稱目的外利用）時，除非符合法定目的外利用理由，否則針對新的利用目的及範圍，應獲取當事人

本報告之智慧財產權屬於國家通訊傳播委員會

的知悉同意。將資料進行去識別而進行創新服務應用，仍需基於原蒐集目的內，才能進行資料的「去識別」處理，否則仍需獲取當事人的知悉同意。

由於取得當事人的知悉同意，以充足、詳盡告知其資料利用狀態為前提，爰建議結合科技應用，取得當事人動態同意，以便於新的目的利用產生時，能即時確知當事人的意願。

本研究參考歐洲個人資料保護委員會 EDPB 發布關於同意之指引，試舉例數個電信業者可取得動態同意之方式如下：

1. 以雙向簡訊取得同意
   以發送雙向簡訊方式讓用戶得藉由回覆指定數字提供明確同意（例如回覆 1 為同意；回覆 2 為不同意）。
2. 藉由口頭上告知取得同意
   用戶進線電信業者電話客服時，客服以錄音或口頭方式進行告知並取得客戶同意。
3. 雙階段認證
   業者在 APP 或網站可利用雙階段認證確認並取得客戶同意。

(二) 其他產業提供創新服務而運用電信資料：

在此模式中，指其他非電信事業之產業，提供創新服務而有運用電信資料的需求，此時，電信事業屬於被動狀態，係由資料當事人自主決定是否讓其他產業的創新服務提供者近用電信資料、或提供存取。電信事業對於資料之提供必須依循當事人指示、在服務提供者被授權存取範圍內提供資料。

上述第一種模式，由於資料流全程在電信事業所管理範圍內，因此主管機關依我國個人資料保護法非公務機關之中央目的事業主管機關列表，為國家通訊傳播委員會；以推動電信事業運用數據資料發

本報告之智慧財產權屬於國家通訊傳播委員會

展創新服務這個角度而言，參酌其他國家作法，亦會由個資法的監管機關訂定相關指引，以期涉及資料的監理準則及資料創新運用作法之治理的標準齊一，爰運用資料提供創新服務之指引可由國家通訊傳播委員會主責。惟在我國機關間分工現況下，電信事業的新興技術創新及研究發展目前是由交通部郵電司主責，蓋「促進電信事業產業創新及研究發展輔導獎勵辦法」亦由交通部主管，爰如創新實驗監理沙盒機制、或資料中介機制等積極作為之採行，在我國目前似宜由交通部主導規劃，或於將來政府組織改造後相關業務併移由數位發展部主導。

上述第二種模式，由於資料利用目的係依其他產業的創新服務需求，則主管機關為該產業的中央目的事業主管機關。惟於現行社會分工複雜、產業型態多元情況之下，異業間的資料流動（即使以當事人同意為中心）如何確保資料全程使用之安全性，十分仰賴透過契約、合作協議明定保護作法、釐清分工負責範圍，在我國尚無統一的資料專責主管機關前，此尚有待目的事業主管機關間的協力討論、協調及給予明確的依循準則，亦有可能就各自主管範疇提出相關指引。

第二節 法規面建議

一、 現行法規困境

由於我國現行個資法規定較為框架性，電信業者利用電信資料進行創新應用時，經常在發想階段即遭遇阻撓，加上我國對於去識別化規範亦不甚清楚。座談會中亦有學者表示，我國的個資法跟不上科技時代，也沒有個資保護專責機關，若電信事業發展加值應用容易產生爭議。

雖然個資法修法非通傳會權責，惟座談會中眾與會學者專家均對個資法應盡速修法頗有共識，並提出許多修法建議，茲整理如下：

(一) 訂定去識別化標準[310]；

[310] 去識別化是保護使用者隱私的基本作法之一，惟目前我國個資法對於去識別化尚未有明確定義，因此尚待我國主管機關盡速修訂個資法關於去識別化之定義。此外，在個資法修法之前，本研究建議通傳會可於《安維辦法》或相關指引中訂定去識別化定義，以符實務所需。

本報告之智慧財產權屬於國家通訊傳播委員會

(二) 強化當事人權利行使；

(三) 設置個資保護專責機關；

(四) 隱私衝擊評估；

(五) 建立透明化之要求。

二、 修訂《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》或增訂相關指引

我國個資法修法進程不確定，針對電信事業若要運用數據資料提供創新應用遭遇不確定適法因素阻擾狀況下，本研究茲彙整座談會專家學者意見，並由通傳會為電信事業個資事項之中央目的事業主管機關角度出發，提出修訂《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》（下稱 NCC 安維辦法）或增訂指引之意見，如下：

(一) 動態取得同意及透明化要求；

(二) 電信資料去識別化標準或指引；

(三) 隱私衝擊評估；

(四) 強化當事人權利。

本研究依據上述幾點建議，草擬 NCC 安維辦法修正草案條文如下表。未來通傳會於修訂相關辦法或增訂指引時，為求與個資法的一致性，亦可評估請國家發展委員會就修訂內容提供意見。

通傳會或可考慮於《電信法》或《電信管理法》等電信相關法律中，明定加值應用之定義，並允許電信事業使用去識別化資料及群集資料，並以子法進一步訂定去識別化的定義、作法及資料保護的做法。

惟若通傳會認為修法程序恐緩不濟急，通傳會亦可考量透過指引方式，俾供電信業者利用電信資料進行加值創新應用服務時作為參考依據。

準此，若能修訂前開規定或訂定相關指引供電信業者遵循，方能讓業者在個人資料保護的前提下，加速發展運用電信資料進行各項加值創新應用服務。

表 14 草擬《國家通訊傳播委員會指定非公務機關個人資料檔案安全

本報告之智慧財產權屬於國家通訊傳播委員會

維護辦法》修正草案條文對照表

修正條文	現行條文	說明
第二條 本辦法所稱非公務機關包括下列各款： 一、第一類電信事業。 二、第二類電信事業。 三、有線廣播電視系統經營者及有線電視節目播送系統。 四、電視事業。 五、訂戶數達三千戶以上之直播衛星廣播電視服務事業。 六、經營國內新聞台頻道或購物頻道之衛星或他類頻道節目供應事業。 本辦法用詞定義如下： 一、電信資料：指電信管理法第 9 條所稱通信紀錄及帳務紀錄。 二、加值應用[311]：指在	第二條 本辦法所稱非公務機關包括下列各款： 一、第一類電信事業。 二、第二類電信事業。 三、有線廣播電視系統經營者及有線電視節目播送系統。 四、電視事業。 五、訂戶數達三千戶以上之直播衛星廣播電視服務事業。 六、經營國內新聞台頻道或購物頻道之衛星或他類頻道節目供應事業。	新增第二項關於電信資料、加值應用及去識別化之用詞定義。

[311] 此處加值應用定義係參考《宜蘭縣門牌位置資料使用及收費辦法》、《花蓮縣地理資訊系統數值及實體圖資流通管理辦法》等關於「加值應用」之定義所擬訂。因加值應用定義恐涉及通傳會

本報告之智慧財產權屬於國家通訊傳播委員會

修正條文	現行條文	說明
電信服務契約之特定目的外運用人工智慧、大數據或其他數位科技處理、分析相關資料之全部或部分後，再行發售或傳輸之加值產品或服務。 三、去識別化[312]：指對特定欄位重新整編給碼加密，或重新模糊化，或予以增刪若干欄位，或將個人資料予以遮蔽、標註，以無從辨識特定之當事人。		
第七條 電信事業利用電信資料進行加值應用，應辦理下列事項： 一、應公開加值應用之目的及方法，		一、本條新增。 二、針對電信事業利用電信資料進行加值應用，為要求電信事業公開透明其創新應用處

跨部會權管業務，本研究為求篇幅一致，初步建議於《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》第 2 條納入「加值應用」之名詞定義，惟若通傳會於採行本研究報告建議時，如認於《安維辦法》修訂「加值應用」之定義不妥，亦建議通傳會可於《電信法》、《電信管理法》及其子法修訂「加值應用」之定義，併此敘明。

312 此處去識別化定義係參考《全民健康保險保險人資訊整合應用服務中心作業要點》、《全民健康保險資料人工智慧應用服務試辦要點》等關於「去識別化」之定義所擬訂，並納入個人資料保護法「無從識別特定之當事人」之文句。

本報告之智慧財產權屬於國家通訊傳播委員會

修正條文	現行條文	說明
如需取得用戶同意，應確認用戶已受充分告知，且自主表示同意，並提供用戶便於撤回同意之方式。 二、應讓用戶便於行使個資法之當事人權利。 三、如加值應用之電信資料涉及個人資料，應進行去識別化，且不得再重新識別。如依契約關係須將加值應用相關資料提供予他人，應於契約中明文規定接收者不得將資料再識別。 四、如涉及利用生物資料、大規模分析追蹤、資料庫比對、自動化決策等高風險之處理或利用時，應事先進行隱私風險評估。		理電信資料之方式及目的，並強化當事人行使個資法權利，以降低民眾對電信業者進行創新應用之疑慮，爰參考 EDPB 發布的同意指引、GDPR 透明性指引及韓國《大數據個人資料保護準則》等關於有效同意及透明化要求等規範，訂定第一款及第二款。 三、如加值應用之電信資料涉及個人資料，為保護用戶隱私，應進行去識別化，且不得再重新識別。爰參考日本「假名化加工資料」、韓國 KCC《大數據個人資料保護準則》等關於去識別化規範，訂定第三款。 四、如電信業者利用電信資料進行加

本報告之智慧財產權屬於國家通訊傳播委員會

修正條文	現行條文	說明
五、前項隱私風險評估至少應包含以下項目： 1. 說明進行資料處理或利用之目的與流程。 2. 衡酌資料處理或利用帶來之利益及伴隨之負擔與風險，評估執行該處理或利用是否符合比例原則。 3. 對所預見之潛在風險提出相應之安全措施，以降低風險對用戶可能造成之危害。		值應用涉及較高風險時，例如利用生物資料、大規模分析追蹤、資料庫比對、自動化決策等，應先進行隱私衝擊評估，並公布及評估結果，爰參照歐盟 GDPR 關於隱私衝擊評估（Data protection impact assessment）之規範，增訂第四款及第五款。
第八條 本辦法自發布日施行。	第七條 本辦法自發布日施行。	條次變更。

資料來源：本計畫製作

本報告之智慧財產權屬於國家通訊傳播委員會

第三節 政策與資料治理面建議

針對電信監理沙盒的具體作法，已可見有韓國的前例，而日本對於資料信託制度（又稱資料銀行）亦已有成熟討論，此屬廣義的資料中介類型之一，以下介紹之。

一、 韓國監理沙盒及大數據個人情報保護準則

(一) 前言

韓國引進監理沙盒的概念源自於 2017 年 12 月所發表的「2018 經濟政策方向」(2018 년 경제정책방향)，該政策方向指出現有的基本監理體制已無法因應新興產業與新技術，預期往後 1 年的籌備期，用以建立監理沙盒制度。文在寅政府並提出「消極監理系統」(네거티브 규제시스)，以原則許可例外禁止，期望對新產業、新技術打造監理革新，減輕發展障礙，2019 年 1 月正式執行監理沙盒制度。

相較於其他國家監理沙盒多以金融領域為中心，韓國除了金融領域[313]，亦同時有資訊與通信科技整合(ICT)[314]、產業整合(산업융합)[315]、監理自由特區(규제자유특구)[316]、智慧城市(스마트도시)[317]等數個領域執行；依 2021 年 2 月 9 日韓國政府因應監理沙盒 2 週年而發表《監理沙盒執行 2 年主要案例》(규제샌드박스 시행 2 년 주요 사례[318])刊物，公布 2 年間韓國執行監理沙盒制度的成果，依該刊物統計結果，現在已有 410 件申請通過審核，其中 137 件為金融領域、102 件為產業整合領域、90 件 ICT 整合領域、

313 例如使用信用卡也可以進行轉帳作業。
314 例如任意距離無線充電技術，藉由光照即可提供各 IT 機器進行無線充電。
315 例如設立公用美容院，使美甲師、美髮師、按摩師等各類型美容師得利用公用美容院自由營業。
316 例如在釜山地區，水產流通過程所有資訊得透過區塊鏈紀錄。
317 開發視覺障礙者導航應用程式。
318 《監理沙盒執行 2 年主要案例》全刊 https://www.opm.go.kr/flexer/view.do?ftype=pdf&attachNo=104945 （最後瀏覽日：2021/10/12）。

本報告之智慧財產權屬於國家通訊傳播委員會

65 個自由監理特區，及 16 個智慧城市等。2 年來韓國總共投資了 1 兆 4000 億韓幣，而監理沙盒也顯著影響產業的經濟，不僅提高銷售額，亦創造就業機會[319]。

(二) 組成要素

韓國的監理沙盒有「實證特例」、「臨時許可」與「迅速確認」等三大組成要素，其中「實證特例」為監理沙盒制度的核心，當運用新技術的事業依現行法規無法取得許可，且依相關法令亦無法申請許可時，得賦予該新技術在符合一定條件下於市場上進行實證測試（實驗），若實證結果指出有改善規定之必要，政府應對相關法規進行修正。「臨時許可」係指當新技術被認為不會引發安全性問題時，因現行法規之基準及條件均無法賦予許可時，優先使該技術得於市場上進行銷售之臨時許可，而主管機關應改善有關之監理制度。最後，「迅速確認」則指欲使用新技術之企業，就監理與否不明而有判斷之必要，得向監理主管機關申請迅速確認，主管機關於收到申請之日起 30 天內確認該新技術是否需要監理，若未收到主管機關的回信，該新技術即可被推定為無需監理。

韓國政府認為，透過此三大組成要素，得以在新技術、新服務、新產業等發展的同時，減輕國民生命安全的疑慮、事前預防環境損害；因此與國民生命安全有關的部分，必須經過實證特例，而實驗執行過程中發生問題時，將取消該特例，並規定實證特例有義務加入事前責任保險，以強化賠償責任，而故意過失的舉證責任亦改由事業者承擔[320]。

[319] 整理自[디지털피디아] 규제 샌드박스(Regulatory Sandbox), http://www.digitaltoday.co.kr/news/articleView.html?idxno=264600 （最後瀏覽日：2021/10/12）。

[320] 整理自《監理沙盒執行 2 年主要案例》，頁 15 https://www.opm.go.kr/flexer/view.do?ftype=pdf&attachNo=104945（最後瀏覽日：2021/10/12）。

本報告之智慧財產權屬於國家通訊傳播委員會

(三) 電信監理沙盒[321]

與電信技術有關的監理沙盒，被歸類在 ICT 整合領域，電信事業得向「情報通信產業振興院」（정보통신산업진흥원）提出申請，並經由「新技術・新服務審議委員會」進行審議，以確認新技術及新服務是否需透過監理沙盒制度進行。

ICT 整合領域的「實證特例」法源為「情報通信整合法施行令」第 38 條之 2 第 1 項「欲運用新規情報通信整合等技術・服務之事業者，符合下列任一款而執行事業有困難時，為對該技術・服務為限制性實驗・技術驗證，而以無需適用相關規定之全部或部分向科學技術情報通信部長申請實證之監理特例。(1)新規情報通信整合等技術・服務，無法依其他法令申請許可時；(2)為申請許可依據之法令其所定之基準・規格・要件等適用不明或有不合理情形時」[322]，主要是透藉由限制測試規模、地區等產出實驗及驗證成果，並以國民之生命、健康、安全及使用者保護方案、個人資料議題等為考慮事項；「臨時許可」法源為「情報通信整合法施行令」第 37 條第 1 項「欲運用新規情報通信整合等技術・服務之事業者，符合下列任一款時，為使該技術・服務進入市場，得向科學技術情報通信部長申請臨時之許可等（以下稱臨時許可）。(1)該當新規情報通信整合等技術・服務，不適用許可依據之法令所定基準・規格・要件等；(2)申請

321 本段落整理自 ICT 監理沙盒網站 https://www.sandbox.or.kr/main.do（最後瀏覽日：2021/10/12）。

322 原文為「신규 정보통신융합등 기술・서비스를 활용하여 사업을 하려는 자는 다음 각 호의 어느 하나에 해당하여 사업 시행이 어려운 경우 해당 기술・서비스에 대한 제한적 시험・기술적 검증을 하기 위하여 과학기술정보통신부장관에게 관련 규제의 전부 또는 일부를 적용하지 않는 실증을 위한 규제특례를 신청할 수 있다. 1.신규 정보통신융합등 기술・서비스가 다른 법령의 규정에 의하여 허가등을 신청하는 것이 불가능한 경우 2.허가등의 근거가 되는 법령에 따른 기준・규격・요건 등을 적용하는 것이 불명확하거나 불합리한 경우」。

本報告之智慧財產權屬於國家通訊傳播委員會

許可依據之法令其所定之基準・規格・要件等適用不明或有不合理情形時」[323]，為使新技術及新服務得迅速進入市場而給予臨時許可，惟執行時仍應考慮國民之生命、健康、安全及使用者保護方案、個人資料議題等事項。「迅速確認」的法源為「情報通信整合法施行令」（정보통신융합법 시행령）第 36 條第 1 項「欲運用新規情報通信整合等技術・服務之事業者，得依法就有關新規情報通信整合等技術・服務，向科學技術情報通信部長申請確認其許可・承認・註冊・認可・驗證等(以下稱許可等)之必要與否。」[324]，主要是確認是否存有相關規定及必要認可事項，若被認為有監理之必要時，始得提出「臨時許可」或「實證特例」之申請。

「迅速確認」由科學技術情報通信部（과학기술정보통신부，簡稱科技資通部）負責，「臨時許可」及「實證特例」則由「新技術・服務審議委員會」（신기술·서비스 심의위원회）決定。

(四) 電信事業監理沙盒案例

《監理沙盒執行 2 年主要案例》所列之 ICT 整合領域總計有 10 件，其中與電信事業有關為「告別書面通知，開啟新時代！手機電子通知」，及「開啟行動電話遠端開通時代」2 項新服務，兩者均被認為安全性無虞，故直接取得臨

323 原文為「신규 정보통신융합등 기술・서비스를 활용하여 사업을 하려는 자는 다음 각 호의 어느 하나에 해당하는 경우 해당 기술・서비스의 시장출시 등 사업화를 위하여 과학기술정보통신부장관에게 임시로 허가등 (이하 “임시허가”라 한다)을 신청할 수 있다. 1.허가등의 근거가 되는 법령에 해당 신규 정보통신융합등 기술・서비스에 맞는 기준・규격・요건 등이 없는 경우 2.허가등의 근거가 되는 법령에 따른 기준・규격・요건 등을 적용하는 것이 불명확하거나 불합리한 경우」。

324 原文為「신규 정보통신융합등 기술・서비스를 활용하여 사업을 하려는 자는 과학기술정보통신부장관에게 해당 사업에 대한 신규 정보통신융합등 기술・서비스와 관련된 법령에 따른 허가・승인・등록・인가・검증 등(이하 “허가등”이라 한다)의 필요 여부 등을 확인하여 줄 것을 신청할 수 있다.」。

本報告之智慧財產權屬於國家通訊傳播委員會

時許可進入市場。

「告別書面通知，開啟新時代！手機電子通知」的概念為改變行政機關、公共機關傳統書面通知的方法，改由以手機簡訊（文字訊息）為通知。此新服務所涉及之法規範有二，一為「情報通信網法」上就連結個人資料所生之資訊（Connecting Information, CI，以下稱連結資訊），其產生方法及提供程序並無明文規定，且實名認證機關在處理連結資訊時，依現行放送通信委員會之告示，未取得本人個別同意下，禁止任意轉換個人資料與連結資訊，又稱為一貫轉換禁止，因此欲將行政程序上的書面通知改以手機簡訊通知，將面臨如住民登錄號碼與連結資訊（例如手機號碼）進行轉換，因未經過本人個別同意情況，新服務的運用將遭遇困難。本次主管機關賦予此新服務的臨時許可期間為 2 年，實驗內容係由包含 KT、KAKAOPAY、NAVER 等相關企業參與 ICT 監理沙盒，由行政機關透過企業所提供的服務傳送電子通知，國民得直接自手機受領通知，該通知與書面相同具有法律效力；惟本新服務在運作過程中仍需具備保護使用人個人資料之技術性保護措施，並應確保使用人對於新服務的了解與同意、得拒絕利用之權利。本次實驗減輕行政機關過去寄發通知而花費高達 95.5 億元的郵務費用，提高行政機關在通知上的效率，例如 2020 年因新冠肺炎疫情重創韓國經濟，韓國政府透過簡訊對各中小企業經營者寄送中小企業新希望支援金說明，使中小企業經營者只需要透過手機即可申請支援金，無需再透過繁瑣的行政作業，而政府透過簡訊進行政策宣導的方式，亦被視為助於政府與國民間的溝通[325]。

「開啟行動電話遠端開通時代」的概念源自傳統申辦行動通訊服務必須要實際確認本人身分時所帶來的不便。

[325] 整理自《監理沙盒執行 2 年主要案例》，頁 40-42，https://www.opm.go.kr/flexer/view.do?ftype=pdf&attachNo=104945（最後瀏覽日：2021/10/12）。

本報告之智慧財產權屬於國家通訊傳播委員會

在「電子通信事業法」修法前，欲在韓國辦理行動通訊服務，為防止不正申辦及冒名的行為，必須本人親自臨櫃辦理，或以得證明本人身分之「公認認證書」[326]、「信用卡」等透過網站與電信業者締約，相當不便。隨著遠距時代的來臨，線上服務蓬勃發展，若仍強制以「公認認證書」或「信用卡」作為申辦服務的必備文件，對於沒有「信用卡」或無法取得「公認認證書」的使用人造成相當大的不便，因此各電信業者研發出得輕易作為本人認證系統的應用程式「PASS」，使得國民得以「PASS」及銀行帳戶連結後辦理行動通訊服務。而為了避免個人資料外洩及冒名的風險，此新服務在「電子通信事業法施行令」修法前，以電信業者必須加入責任保險作為通過臨時許可之條件。由於目前「PASS」應用程式係由各電信業者自行研發與推出，提供給各自的用戶使用，因此韓國政府有意整合各電信業者的應用程式，並研擬操作指引供使用人參考。目前此新服務的實驗仍在進行中，欲變更行動通訊服務電信業者之消費者，透過此項服務無需再親自訪問實體門市，亦不用再花費行政規費申請公認認證書，對使用人的便利性具有極高的助益[327]。

(五) 大數據個人情報保護準則

如前所述，韓國放送通信委員會（방송통신위원회，以下稱 KCC）於 2014 年 12 月 23 日公布「大數據個人資料保護準則」（以下稱保護準則），作為處理大數據時兼顧個人資料保護與應用之具體性基準，以防範個人資料遭到誤用或濫用。

本研究茲將保護準則全文翻譯如附錄 13，主要內容為以下五項：

326 공인인증서，韓國政府所發行用於線上傳輸時確認國民身分的認證書，認證書的有效期限為發行後兩年，可用於登錄網路銀行、線上報稅等服務。

327 整理自《監理沙盒執行 2 年主要案例》，頁 52-54，https://www.opm.go.kr/flexer/view.do?ftype=pdf&attachNo=104945（最後瀏覽日：2021/10/12）。

本報告之智慧財產權屬於國家通訊傳播委員會

1. 自蒐集開始即應對可識別個人之資料進行徹底的去識別化措施
2. 確保處理大數據之事實或目的等透明公開
3. 個人資料經再識別後，應立即為廢棄或去識別化措施
4. 禁止對敏感資料或通信秘密為蒐集、利用、分析等處理行為
5. 對被蒐集的個人資料為保存或管理時，應實行技術性、管理性保護措施

(六) 小結

綜上所述，本研究建議通傳會可參考金管會之《金融科技發展與創新實驗條例》，訂定《電信加值發展與創新實驗條例》，並參考韓國監理沙盒模式、相關法規及實例，納入「實證特例」、「臨時許可」與「迅速確認」等三大組成要素。

同時，本研究亦建議通傳會參考韓國 KCC「大數據個人資料保護準則」重要內容，訂定「電信數據個人資料保護指引」，即可有效掌握並監督電信事業利用電信數據發展對個人資料保護的狀況，在兼顧保護個人資料的同時，有效提升電信數據創新服務的發展性。

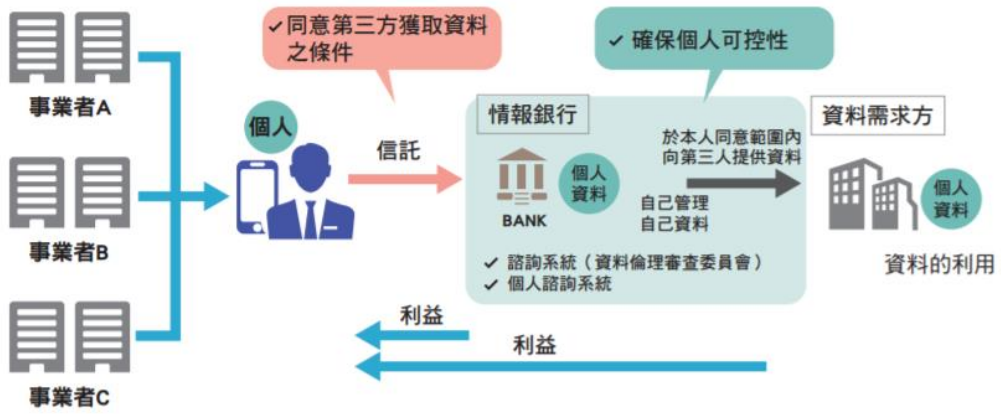
二、 資料銀行

日本政府希冀建構一個使個人能夠參與，進而促進資料流通與利用的機制，稱為「資料信託機制」(情報信託機能)。2008 年日本在「社會 5.0 政策」的指引下，由內閣官房長官公布的「未來投資戰略：2018」（未来投資戦略 2018—「Society5.0」「データ駆動型社会」への変革—）中，將「資訊信託機制認定指引」(情報信託機能の認定に係る指針 ver1.0）列為未來發展方向。

日本「未來投資戰略 2018」主題為「邁向 Society5.0」「資料驅動型社會的改革」(「Society 5.0」「データ駆動型社会」への変革)，其中特別提到「資料霸權主義」的現象，即國家或是特定企業獨占特定資料，因此為了避免資料的獨占現象，推動資料信託機制最主要的原

本報告之智慧財產權屬於國家通訊傳播委員會

因就在於促進資料的自由流通，進而推動各式的創新應用。日本資料銀行運作架構如下圖所示[328]。



資料來源：本計畫編譯

圖25　日本資料（情報）銀行運作架構

由此可知，日本之資料銀行制度係以信託方式進行個人資料管理，由信託人（一般民眾或擁有大量個資的業者）通過信託行為，預先指定或設定條件將其資料信託予受託人（資料銀行），並由受託人按信託人設定信託之目的，為其管理個人資料，並應善盡管理個人資料之義務。如遇須將個人資料提供予第三人使用之情形，資料銀行亦得於必要時對資料作匿名化。

日本經產省於 2019 年 10 月公布「資料信託功能認定指引第二版[329]」，該標準除明定資料銀行功能與個資當事人間之關係說明外，亦規定四大面向之資料銀行認證標準：

1. 設置及營運規劃：如業者是否具備一定程度損害賠償能力及是否有效遵循日本個資法規範；
2. 資訊及個資保護安全性:如是否取得 ISMS 認證或 JISQ15001 個資保護標章等；
3. 內部治理：如對外諮詢管道健全性及公司透明性（如定期公

[328] 顧振豪，〈觀察先進國家以個人為中心之資料運用模式〉，《台灣經濟論衡》，18 卷 1 期 (2020)，頁 22-29。

[329] 〈情報信託機能の認定に係る指針 ver2.0〉，情報信託機能の認定スキームの在り方に関する検討会（2019），https://www.meti.go.jp/press/2019/10/20191008003/20191008003-3.pdf（最後瀏覽日：2021/12/29）。

本報告之智慧財產權屬於國家通訊傳播委員會

告、報告等）；

4. 業務內容：如是否依照模範條款訂立相關應記載事項，是否有於契約明確記載取得個資本人同意將資料提供與第三人等。

實務上，日本資料銀行之認證以產業協會「IT 團體連盟」為實務執行單位，並於 2019 年 6 月首先公布兩家業者獲取「P 認證」，意即該等業者對資料銀行設置及營運等規劃內容符合前述認定標準，可開始籌設資料銀行。而於資料銀行成立後，業者需依原規劃內容辦理，並持續檢討、改善，以續獲 IT 團體連盟核發之「一般認證」。迄本年 12 月止，IT 團體連盟共進行 6 次認證，目前獲「P 認證」之業者共 5 家，獲「一般認證」之業者則有 2 家[330]。

此外，資料銀行亦須設置「資料倫理審查委員會」諮詢體制，成員應包含外部委員。資料銀行業者應定期對該委員會提出報告，並針對資料銀行與個人間契約內容、資料銷售第三方的選定條件等項目進行審議，以確保資料銀行業務內容不會與個資本人產生利益衝突。

準此，為鼓勵電信業者進行創新加值應用，避免囿於法規而有所侷限，通傳會可評估參酌日本做法建置資料銀行制度，藉由可信任之第三方機構作為資料流通基礎，鼓勵並促進電信資料加值再利用。

[330] 情報銀行推進委員会，https://www.tpdms.jp/index.html（最後瀏覽日：2021/12/29）。

本報告之智慧財產權屬於國家通訊傳播委員會

第八章 執行與研究發現

第一節 電信事業配合執行維護國家安全公共利益電信資料應用研析

未來資料共享政策的變化，最重大挑戰之一將是資料隱私的社會需求和道德處理。由於全世界對於民眾的數位設備追蹤已經隨著不同地區、社會和政府而有不同的政策，關於本計畫研析國家如愛沙尼亞作為電子化政府的模範國家，其認為發展電子治理不需針對特定領域建立全面性立法體系，僅應針對資料敏感性等重要議題，在保持技術中立性的情況下，透過分析現行法並找出差異，以及法律可能對電子治理發展造成障礙的領域，逐步檢視調修，建議在規劃過程中應諮詢法律專家，及早進行法律風險分析，避免過度監管或是造成監管障礙。

而英國則是由上而下擬定整體國家資料策略，當面對疫情衝擊帶來的挑戰，亦認為在立法和政策面不僅需要彈性，亦不能忽視人民所關注之隱私和資料安全問題。為了獲得公眾信賴，資料儲存和使用應完全透明，並有進行資料風險評估，至於政府使用電信公司提供之群集匿名位置資料來評估資源分配，以及社交距離措施，但仍可能有重新識別個人風險，且當前去識別化技術尚不足以個人提供完全隱私保護，且有數位落差問題亦應考量，因此數位技術發展不僅加快政府應變能力，也需思考技術帶來倫理和技術挑戰。

日本制定個人資料保護法作為國家、地方自治團體與業者須遵循之個人資料保護共通規範，為協助業者適當使用資料，個人資料保護委員會制定了個人資料保護法指引通則，並依不同狀況再細分為確認與紀錄義務篇、向外國第三方提供篇，與匿名加工資料篇。此外，總務省針對電信通訊業者，亦制定了電信通訊事業個人資料保護指引，以兼顧電信通訊服務之便利性與個人資料保護。

而韓國的電信事業配合國家安全公共利益電信資料應用部分，向來多以配合檢警機關犯罪偵查所需，提交特定位置、通訊紀錄等資訊，特別是韓國政府打造智慧城市時，借助電信事業各基地台連線及使用者的位置資訊，始能打造完整的追蹤中心，便於搜索通緝車輛及緝捕

本報告之智慧財產權屬於國家通訊傳播委員會

犯嫌等。由於 COVID-19 在全球大流行，為確實控制該傳染病在韓國境內的擴散，電信資料逐漸自單純的社會安全應用延伸至保健衛生議題，韓國國會配合政府政策對「傳染病防治法」進行修正，使相關主管機關得直接依法授權取得電信資料，並藉此與電信業者合作開發智慧檢疫系統，落實對傳染病來源的控管。而隨著 K-MyData 的運作，預期未來將由當事人作為包含電信資料等個資的主宰，得自由授權傳遞及應用個人資料，使個資在應用上得以發揮更大的效果。相較於前述國家，美國現階段就個人資料保護雖無統一適用的專法，而是依照各個領域分門別類制定相關個資保護規範，且於 COVID-19 疫情的推波助瀾下，美國政府重新思考使用電信資料來評估人員流動所帶來的效益，以在公益及隱私之間進行取捨。

觀察透過資通訊技術傳輸資料來達成維護國家安全公共利益之案例中，各國因應疫情而開發各種接觸者追蹤應用程式，有些有涉及位置資料的蒐集、處理或利用；另外有些僅採取藍芽傳輸且匿名交換 ID，即未涉及用戶電信資料，合先敘明之。至於其他應用大多針對位置資訊應用於人口動向分析，採取匿名統計資料分析，或是防災救援目的，則是透過告知得到當事人同意。

第二節 電信服務業創新應用現況實際應用案例與政策法制研析

電信事業對於資料應用依據社會經濟對於資料應用需求，且隨著大數據應用分析，資料往往不會侷限於特定項目或應用領域，而會多方與異業合作，找出未來電信產業新的發展面向。觀察各國電信產業與異業資料應用結合，也激盪出更多元商業模式與更便利服務。然而也需要考量當電信業者將資料提供第三方分析作為服務應用基礎時，資料當事人隱私保護不容忽視。

而各國也面臨挑戰如愛沙尼亞國家資料庫中擁有大量個人資料，只要資料主體同意就有可能開放這些資料用於開發創新服務。然此種做法的爭議在於無法得知此類服務是否將資料傳輸給第三方服務提供者，也無法取得資料主體之同意近用其個人資料。

本報告之智慧財產權屬於國家通訊傳播委員會

而德國則在 2021 年兩項電信相關規範之修法，包含電信現代化法是為協調歐盟現有之電子通訊法律框架，並針對電信監管框架進行全面性修正，希望在保持網路和服務的可近用性和安全性之餘，能夠提高共同合作及投資的意願，並增加終端使用者的利益。另一項修法則是電信與電子媒體資料與隱私保護法，作為保護數位世界中的資料與隱私，並平衡數位服務使用者利益與公司經濟利益，解決因電信法、電信媒體法（Telemediengesetz, TMG）與 GDPR 同時並行，使消費者、電信服務提供者以及監管機關不確定如何適用上開法律之情況。

日本於 2020 年與 2021 年對個人資料保護法做出多項重大修正，2020 年之修正旨在衡平資料創新應用與個人資料保護，而 2021 年為了因應數位社會形成基本法之制定，則修正個人資料保護法，使全國、地方政府與民間適用統一之個人資料保護規範。上開修正將有助於促進資料流通，有助於電信業者進行更多元之資料創新應用服務。

而美國的電信網路快速適應人類生活、工作、學習和娛樂方式所發生的改變。透過較彈性之監管方式，以促進競爭及減少規範，並鼓勵新電訊傳播科技的迅速部署。英國則以國家資料戰略作為整體推動方向，輔以 Smart Data 計畫作為英國共享消費者資料框架，讓消費者掌握自己的資料，因應未來跨域資料應用，同時也有利於第三方業者開展出創新資料商業模式與服務。此外，英國政府也考量資料對於數位市場競爭，還有政府開放資料對於民間影響，並發展從公私資料中獲取價值的共享模型。

隨著第四次工業革命的來臨，韓國的電信業者無不投入發展大數據資料分析及應用等相關產業，三大主要電信業者各推出「巨量資料服務平台」，並以各自所有之電信資料為基礎，分別對不同領域進行分析及應用，使電信資料不再僅限特定個人，更得以擴展應用於包含商業、不動產、金融等服務，促進異業結合，特別是在 COVID-19 大流行嚴重影響地方經濟時，電信業者利用電信資料而衍伸之大數據資料分析成果，提供異業規畫適合的行銷服務及商業推廣，並給予相當優惠等，適度的減緩嚴重傳染疾病對社會帶來的衝擊。而 2020 年韓國「個人情報保護法」引進假名情報的概念，明確立法規定假名情報

本報告之智慧財產權屬於國家通訊傳播委員會

得用於統計編制、科學研究或保存公益紀錄等領域，此次新法施行減輕各電信業者在應用電信資料進行統計編制或科學研究時可能遇到的阻礙，例如何種電信資料可以進行應用，何種電信資料不可，有益各電信業者應用電信資料進行大數據分析服務的發展。

第三節 電信事業運用數據資料創新應用服務治理模式研析（網路公眾意見諮詢與 2 場實例分享座談會）

本團隊蒐集前述各國電信事業運用資料創新應用服務之案例及治理模式後，復透過網路公眾意見諮詢及邀請專家學者參與座談會等方式彙整、分析各方意見，針對電信事業運用資料創新應用服務治理模式提出建議如下：

一、 修訂《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》（短期建議）

建議通傳會可參考 EDPB 發布的同意指引、GDPR 透明性指引及韓國 KCC《大數據個人資料保護準則》等相關規範，於《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》增訂之電信資料加值應用相關規範，建議內容如下：

(一)有效取得同意及透明化要求；

(二)電信資料去識別化標準或指引；

(三)隱私衝擊評估；

(四)強化當事人權利。

詳參本研究提出之《國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法》修正草案。

本報告之智慧財產權屬於國家通訊傳播委員會

二、 建立網路公眾意見諮詢平台（短期建議）

建議通傳會可參酌本次研究經驗，建立網路公眾意見諮詢平台，以使政策制定過程透明化，並使相關法規政策更加符合實務需求，增進治理之效益。

此外，電信事業進行監理沙盒實驗時，亦可運用該平台使電信事業與網路公眾進行溝通對話，促進民眾對通傳會及電信事業之信任度。

三、 訂定電信監理沙盒規範，鼓勵業者以監理沙盒模式進行創新試驗（中期建議）

建議通傳會可參考金管會之《金融科技發展與創新實驗條例》，訂定《電信加值發展與創新實驗條例》辦理監理沙盒模式，並鼓勵電信業者就身分識別及交通運輸類等創新服務進行實驗，而後更能進一步接軌法規落地。

四、 建置資料銀行制度（長期建議）

為鼓勵電信業者進行創新加值應用，避免囿於法規而有所侷限，通傳會可評估建置日本資料銀行制度，藉由可信任之第三方機構作為資料流通基礎，鼓勵並促進電信資料加值再利用。

第四節 電信事業運用資料創新應用服務治理模式研析

一、 數據資料應用種類與態樣

關於電信業者所蒐集資料類型，原則上關於民眾申辦電信服務時所提供之資料與實際使用電信服務時所產生之資料，依個資法皆屬為提供服務蒐集、處理、利用資料之目的。當業者對於電信數據資料加值利用則是依個資法第 20 條規定，除非符合公益考量，或進行去識別化，原則上進行資料加值應經過當事人同意。亦應注意電信事業對於資料保存期限法律規定。

在維護公眾利益、促進國家發展範疇下，為確保政府機關使用電

本報告之智慧財產權屬於國家通訊傳播委員會

信資料的正當性，建議應有明確的規範，及透明的審核監管組織或系統。還有從風險角度建議區別資料的風險層級，定期檢視調整考量改變風險等級的情事。此外，也需要解決資料標準化與格式化問題，並應確保資料去識別化。

二、 電信業者應用時面臨資料應用問題

關於電信業者目前所面臨資料應用問題，並綜整網路公眾意見諮詢與 2 場實例分享座談會意見，應關注包含資料去識別化、告知同意與消費者保護、個資專責機關設立等。透過讓消費者知悉其資料之應用、價值，提供消費者選擇退出，以及去識別化範圍。由於我國目前並無個人資料主管機關，專家建議應確立明確的主管機關，並提供相關指引，並強化資料應用之透明性。此外，亦應注意關於身分識別與民眾對於政府信賴建立，以及強化當事人資料可攜權，更能促進商業目的資料加值應用。

三、 解決方案建議

關於短中長期規劃，規範面應強化當事人權利行使，並讓當事人能清楚知悉與調整對資料之同意應用。另一值得討論是電信資料應用之沙盒機制，得借鏡開放銀行的經驗對照，應提供業者誘因並友善中小企業，訂定適當配套措施鼓勵業者，並對個人資料分級，提升風險容忍度，政策面也需要考量延續性。

第五節 諮詢服務

一、 議題一：向電信事業蒐集收視行為統計資料適法性研析

通傳會基於調處之目的，欲向 MOD 平臺或有線電視系統經營者與頻道供應事業（下稱渠等事業），蒐集相關收視用戶之收視行為統計資料一案，本團隊研析相關適法之程序及見解，並提出具體可行之建議如下：

(一)適法性分析

1. 通傳會於執行調處之法定職務必要範圍內，得向渠等事業蒐

本報告之智慧財產權屬於國家通訊傳播委員會

集含有可識別收視用戶之收視行為資料，惟就「必要性」之判斷，宜審慎為之。

2. 惟縱通傳會得為執行調處法定職務之目的，向渠等事業蒐集含有可識別收視用戶之收視行為資料，渠等事業在現行法下，似無明確義務為調處目的提供該資料，併此敘明。

(二)具體可行措施

1. 建議通傳會就該次調處事宜事前評估，是否存有「取得可識別收視用戶之收視行為資料」之必要。倘有疑義，建議向渠等事業取得去識別化之收視行為資料，較能避免風險。退步言之，亦建議減少可識別用戶身分之資訊，以降低用戶權益侵害風險。

2. 如通傳會於調處過程取得含有個資之收視行為資料，原則上僅得於調處目的內利用；若通傳會有意為其他目的利用收視行為資料，應評估是否合於個資法規範。

二、 議題二：電信事業之定型化服務契約條款研析

有關通傳會如何檢視審理電信事業之定型化服務契約條款內容，及如何避免人格權遭受侵害，並促進電信事業合理利用用戶個人資料，本團隊研析相關適法之程序及見解，並提出具體可行之建議如下：

(一)本研究認為，雖電信業者不需將其個資告知聲明送交通傳會核准，通傳會仍得以行政檢查或行政指導之方式，要求電信業者提交個資告知聲明以供檢查。

(二)為協助通傳會檢視審理電信事業之定型化服務契約條款內容，本研究將《個人資料保護法》第 8 條要求之形式及實質告知事項須注意之要點整理成表格，並製作檢查清單（checklist）供通傳會於行政檢查時勾選，以審視電信業者之隱私權政策或個資告知聲明是否符合《個人資料保護法》規範。

(三)此外，通傳會亦需確認用戶提供之「同意」是否符合《個人資料保護法》規範，因此本研究針對「以同意作為目的外利用之依據」及「以同意作為蒐集及處理用戶個人資料之依據」，整理「有效同

本報告之智慧財產權屬於國家通訊傳播委員會

意之要件」表格供通傳會參酌，通傳會得於行政檢查及行政指導時依具體情形判斷同意是否有效。

三、 議題三：電信事業提供政府合理利用個資於跨領域共享

本計畫研析關於德國 Corona-Warn-APP 以及其隱私聲明、相關法律依據，作為我國因應疫情相關措施借鏡參考。首先關於德國 Corona-Warn-APP 與臺灣社交距離 APP，兩者運作原理類似皆採取藍芽技術交換 ID，並未蒐集個人資料或位置資料，且都是人民得自由決定是否下載使用，以及當接觸確診者後也能自願決定是否上傳接觸資料，因此人民對於是否提供資料供防疫，仍有自主決定空間，然而此等措施仍為較被動防疫措施，若使用 APP 人數不足，則接觸者追蹤效益並不大。此外，臺灣社交距離 APP 並無我國電信業者參與，因此此部份亦無電信業者配合提供電信資料問題。因此以下主要著重於我國簡訊實聯制資料應用之研析：

(一)關於簡訊實聯制隱私權公告應有詳細說明疾管署與電信業者關係，以及電信業者蒐集資料與保留期間

我國簡訊實聯制由各用戶透過其電信公司發送簡訊以完成實聯制，然而該隱私權公告中僅有說明由疾管署委託關貿網路公司製作並協助維運。參照德國 Corona-Warn-APP 隱私聲明與網站問答，皆有詳細說明涉及 APP 資料控制者、處理者以及資料處理之明確法律依據。此外，對照類似我國簡訊實聯制之德國 Luca 接觸者管理和追蹤應用程式，該 APP 隱私權政策明確說明德國電信所蒐集資料以及伺服器所在位置，而涉及電話號碼則會由德國電信處理以進行驗證且儲存天數。我國關於簡訊實聯制隱私公告並未明確指出電信業者處理哪些資料，以及保留期間，反而是新聞稿內容呈現。因此建議隱私權公告應有詳細說明與電信業者關係，以及電信業者蒐集資料與保留期間，始能衡平資料合理利用與資料應用透明度，使人民得以信賴。

(二)授權電信業者蒐集個資應有明確法律依據

簡訊實聯制下，電信公司蒐集的資料為手機號碼、發送簡訊

本報告之智慧財產權屬於國家通訊傳播委員會

當下時間及場所代碼等 3 項資料，尚未涉及身分驗證資料，因此若需讓電信事業提供及配合政府合理利用用戶之個人資料，並共享予跨領域業務目的使用，於現行法下仍應回歸個資法第 4 條、第 15 條及第 16 條規定公務機關於執行法定職務必要範圍內蒐集處理個資。

政府若需要電信事業提供及配合政府合理利用其用戶之個資，除依據前述個資法規範外，對於法定職權解釋應有明確法律規定，作為合理利用依據，還應融入資料治理概念，事前進行隱私風險評估，甚至是隱私權政策內容應有細緻說明。而面臨後續資料共享建議訂定資料共享相關契約指引，甚至是明確我國去識別化技術，以及推動個資專責機關建立，以利於整體性掌握我國個資合理利用與隱私保護。

(三)我國數位證明簽發平台仍在研議階段，得借鏡歐盟數位 COVID 證明規則

至於數位 COVID-19 證明，我國數位證明簽發平台仍在研議階段，現階段也暫未推動作為通行證。歐盟面臨疫情已經逐步解封，並透過數位證明以有利於歐盟境內人民自由移動，而關於所涉及證明還有的個資有明確法律依據，亦即歐盟數位 COVID 證明規則與 GDPR 相關規定。我國後續若要推動數位證明仍應有完整評估與法律明確依據。

四、 議題四：異業合作涉及跨領域業務資料應用促進當事人資料自主運用

有別於歐盟數位錢包之數位身分認證，我國目前發展大多仍侷限於電子支付功能。與此同時，雖然我國欲推行數位身分證（New eID）政策，提供我國人民網路上身分識別之證明，連結政府骨幹網路（T-Road）串接各類電子政府服務，惟後續因安全性、法源依據等爭議而暫緩推行。而歐盟數位錢包的主要目的是整合 eIDAS 規則，以一個單一的泛歐框架為公民和企業提供在跨境環境中有效識別自己的方法，並以高度安全、值得信賴和符合 GDPR 的方式交換個人身分屬性

本報告之智慧財產權屬於國家通訊傳播委員會

和憑證。

五、 議題五：中國大陸個人信息保護法簡介

(一)中國大陸《個人信息保護法》大量參考 GDPR 規範，加強對個資之保護，相對地也對處理者採取較嚴格之規範。除了高密度管制外，違法時巨額罰款，及可能被迫離開中國大陸市場之處罰，也讓業者必須審慎以對。

(二)我國電信業者若無意進入中國大陸市場，須注意不要落入《個人信息保護法》之管制範圍，審視自身有無「向中國境內自然人提供產品或服務為目的」或「分析評估中國境內自然人」之行為。

(三)若有意經營中國大陸市場者，則須遵循《個人信息保護法》之規定，詳細檢視對其之法遵差異，規劃整體因應方案，以降低業務營運之衝擊。

第六節 電信事業運用數據資料提供創新應用服務治理模式之相關決策作業流程標準之建議

針對電信事業運用數據資料供創新應用服務治理模式之相關決策流程標準之建議，本研究從決策流程、法規面、及政策與資料治理面提出建議。現行運用電信資料所適用之法規，以管制型為主，如個人資料保護相關法規，較欠缺直接賦予產業在特定狀況下得利用特定種類資料（如群集化資料、去識別化資料）的空間，此為產業主管機關未來規劃推動產業活用資料時，可考量以法律明定劃設出資料活用空間。

此外，去識別化資料，雖較無法規遵循的難題，但倘若資料自始係個人資料、是經過處理才變成去識別化資料，此時究竟是否完全去識別化或加上其他識別因子可能再被重行識別，我國法體系如何定義與看待，仍無一定標準。

另由於電信資料的運用態樣及運用主體不同，其他中央目的事業

本報告之智慧財產權屬於國家通訊傳播委員會

主管機關的所管產業皆有可能需近用或存取電信資料以提供創新服務，此亦應受到該主管機關的重視，當特定異業合作模式趨於成熟且常態，則透過契約來妥善劃定資料提供方與利用方權責，以保障資料流全程安全，相當十分重要，此亦有待目的事業主管機關間的協力討論、協調及給予明確的依循準則。

最後針對以積極作為來推動電信事業運用數據資料，國際間尚有促成資料流動機制的新興作法如資料中介機制、創新實驗監理沙盒等機制之熱烈討論中，其發展動向，值得我國持續關注。

本報告之智慧財產權屬於國家通訊傳播委員會

第九章 結論

本研究透過蒐集國際上電信資料應用實例及立法例、徵詢公眾意見、整理專家座談會建議，聚焦於三大重點議題：一、電信事業配合國家安全公共利益目的之電信資料應用；二、電信事業在數據資料創新應用趨勢之下，需自主採行適切治理模式以保障個資並兼顧資料的可運用性；三、電信事業的中央目的事業主管機關透過法制規範或機制採行，促進環境更加完備，以利電信事業運用數據資料提供創新應用服務。茲整理觀察與研究結論如下。

一、 電信事業配合國家安全公共利益目的之電信資料應用

(一)由具有**電信**資料利用目的的執法機關**主導服務設計並提出相關準則**

在以國家安全、公共利益脈絡下由電信事業所為之資料應用、提供或揭露，絕大部分狀況，皆不是由電信業者自主發動，而是由電信業者基於配合角色，依具有資料蒐集、處理或利用之特定目的機關的指示，配合進行資料的處理。在此情境下，電信業者是歐盟 GDPR 所稱的資料處理者（Data processor），主導資料利用目的機關則是資料控制者（Data controller），由資料控制者主導整體服務設計，並擬定服務提供之相關應遵循規則，電信事業配合遵循之。如本研究所舉出針對為因應 COVID-19 運用電信資料情形發現，係由當地國之衛生醫療執法部門主導及擬訂相關法規、指引等規範。

在我國未有個資法專責機關、係由各目的事業主管機關就所轄事業進行規管，電信資料的現況之下，類似上開情境，亦需由具有資料利用目的的執法機關主導服務設計並擬定、提出相關準則；電信監管機關則就電信事業之所責範圍內進行監管，確保電信事業於主導者指示範圍內、依其提出規則，進行資料處理。

(二)對於資料「國家安全」、「公共利益」目的之利用需採取限縮解釋

由於「國家安全」、「公共利益」為不確定的法律概念，難以

本報告之智慧財產權屬於國家通訊傳播委員會

被明確指明界線，因此不能將「國家安全」及「公共利益」無限上綱。我國個資法中，以「為維護國家安全或增進公共利益所必要」作為公務機關將個資進行目的外利用的條件（個資法第 16 條），亦以「為增進公共利益所必要」作為非公務機關蒐集、處理及利用個資的條件（個資法第 19 條）及目的外利用個資的條件（個資法第 20 條），但對於如何判定公共利益內涵，卻缺乏相關操作標準，爰於實際遇有援引此要件而產生爭議的情形，將訴諸個案判斷，具有操作上相當不確定性，故鮮少適用或被引用。

觀諸本研究觀測的國外以防疫為目的之各項電信服務應用（諸如位置資料蒐集、藍芽資料傳輸），即便防疫目的具有公共利益、也與廣泛的國家安全意義相通，但未見有任何實際案例以此為由，而「強制」民眾加入特定電信服務使用，亦未有無明確法源而強令電信公司調取特定民眾的電信資料的情事發生。絕多數例子，皆是於推行防疫目的相關的服務時，盡可能向民眾告知完整的服務資訊供民眾自由選擇加入，給予選擇退出權利，且由民眾自主決定是否允許該服務存取位置資料等電信資料，獲取民眾自主信任及利用。

(三)倘欲強制使電信業者配合調取個人資料則需有法律明定程序及範圍

倘欲強制使電信業者配合提供資料，鑒於公權力節制的必要性，則宜以法律層級訂定調取資料的目的、範圍及程序。我國「通訊保障及監察法」即為以法律層級規範的著例，其明定有權監察單位基於特定目的而進行通訊監察、調取通信紀錄、或通信使用者資料的程序及形式。又如，韓國有感於透過蒐集電信位置資料掌握接觸史，有益於傳染病防治工作，爰修正其傳染病防治法，明文要求電信業者應提供使用者位置資訊，即為以防免傳染病擴散之目的，由電信業者應配合政府提供使用者位置資訊，強化追蹤確診者及回溯感染源等防疫措施。

(四)相關實務應用需遵行資料最少蒐集原則

「資料最少蒐集原則」是指限於資料利用目的而蒐集必要的

本報告之智慧財產權屬於國家通訊傳播委員會

資料，此原則是個資保護的普世價值，如我國個資法中所規定「特定目的之必要範圍」等語，即揭示此一原則。

對照國外將電信資料運用於防疫防災目的之實例，確實體現了資料最少蒐集原則：即便是在充分給予當事人選擇自由是否加入該服務的狀況下，其服務設計及提供，也並未因基於當事人同意就因此盡可能蒐集個人相關資料，而是盡可能不觸及資料當事人其他的資料，當有必要因防疫需求而揭露資訊時，亦以可達成目的為限，避免提供多餘資訊。以愛沙尼亞官方推出的防疫 APP（HOIA）為例，在手機使用者曾有密切接觸者確診 COVID-19 後，會發出通知告知使用者，但此一告知不會告知感染者身分或是接觸的時間及地點，確保無法間接識別感染者身分，以維護個人隱私。

二、 產業端數據創新應用趨勢下的適切資料治理模式

(一)業者應盤點所保管具有廣泛創新應用可能性的電信數據資料類別

電信事業所管理與用戶及使用行為端相關的數據資料，可分為「用戶資料」、「通信紀錄」及「因利用電信服務所產生的其他資料」等三種，其中，用戶資料屬於個人資料而受到個資法之保護，固無疑問，通信紀錄中則涵蓋得間接識別個人之資料，如通信日期、位址、位置資訊等，爰亦屬個人資料的範疇。茲述其內容如下：

「用戶資料」在我國現行法規中，指電信用戶姓名或名稱、身分證或營利事業統一編號、地址、電信號碼等資料，並以用戶申請各項電信業務所填列之資料為限。(「電信事業用戶查詢通信紀錄作業辦法」第 3 條第 4 項)。

「通信紀錄」係指電信使用人使用電信服務後，電信系統所產生之發信方、受信方之電信號碼(指電話號碼或用戶識別碼)、通信日期、通信起訖時間等紀錄，並以電信系統設備性能可予提供者為原則（電信法」第 2 條第 8 款)。另依通保法，通信紀錄尚

本報告之智慧財產權屬於國家通訊傳播委員會

包括位址、服務型態、信箱或位置資訊等紀錄（通訊保障及監察法第 3-1 條第 1 項）。

「因利用電信服務所產生的其他資料」之定義，參照美國電信法第 222 條規定，其係指用戶在電信服務關係中的電信使用行為所生、且由電信事業所蒐集、近用的資料，包含使用電信所涉及的用量、技術組態、型態、總量等資料，此於我國現行法中雖無特別定義，但諸如資料下載速率、流量等資訊（行動寬頻業務服務品質規範實施要點）可認為屬此類資料。

上述資料型態各有其內涵，所對應的業法規定可能涉及不同的保管規則及期間等規定。惟具有個人資料屬性的資料，皆需遵守個人資料保護法的要求，基於特定目的之蒐集，需於該特定目的下進行處理、利用且不得逾越必要範圍（個資法第 5 條），若欲進行特定目的外之利用，則必須符合法定條件。

(二)對個人資料應落實個資相關法規遵循並確保消費者權益

舉凡電信事業所保有之資料，具個人資料性質者，一旦進入規劃利用階段，即應檢視與原蒐集、處理及利用目的是否有所不同，倘若不同，利用者是否擁有二次利用的正當權源。

獲得資料當事人的知悉同意是最為正本清源方法，且告知當事人的內容需具完整性、亦應使讓當事人便利行使權利，實務上，日本電信業者訂定資料憲章（NTT Docomo 個人資料憲章－革新創造行動準則）揭示在保護當事人個資前提上進行資料利用，可作為參考範例。另可考量結合技術應用，發展動態同意機制，落實以當事人同意為核心的資料活用。

三、 政府端促成電信事業運用數據資料之環境整備

(一)可透過訂定指引或定型化契約範本協助業者落實法遵

依據法務部「個人資料保護非公務機關之中央目的事業主管機關列表」，以通傳會為電信事業個資事務的中央目的事業主管機關，通傳會並依個資法授權，訂定「國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法」（簡稱安維辦法），此辦

本報告之智慧財產權屬於國家通訊傳播委員會

法所涵蓋項目屬於為保護個人資料於技術上、組織上應該採行的措施，但對於指向資料利用（或進行目的外利用）宜踐行的程序，尚有欠缺。

1. 訂定指引作為電信業者發展創新服務運用數據資料的具體依循

   諸如資料風險衝擊影響評估、確保資料利用權源正當等事項，在我國現行規範架構中，尚缺乏細部依循。此外，在電信相關數據實際上多屬配搭其他產業領域資料或應用需求合為利用的情形，如何與外部單位分工負責確保資料當事人權利保障及資料安全性，十分重要，然就此亦無細部依循。

   爰建議可參考美國由產業協會（無線通訊產業貿易協會 CTIA）發布位置服務開發部署指南，定義價值鏈中各角色（程式創建者、位置資料蒐集、供應網路位置資料營運者）之作法，就電信領域資料可能與其他領域資料搭配互用的情境，如何使資料當事人知悉同意原蒐集目的外之資料處理利用、如何滿足當事人請求權利（請求閱覽、補充、更正、停止蒐集、處理或利用、請求刪除）、以及電信事業如何與外部單位分工負責以確保資料安全性等事項，以及創新服務上架前進行影響衝擊評估等具體作法，可由通傳會或敦促產業自律訂定指引，以供業者運用數據資料設計、提供創新應用服務時有所依循。

2. 訂定定型化契約範本確保資訊透明化

   依據電信管理法第 17 條：「...電信事業應訂定定型化服務契約條款，載明與用戶之權利義務關係。前項定型化服務契約條款，應包含下列事項：...用戶個人資料蒐集、處理與利用之限制及條件。...」據此，主管機關可考量擬定定型化契約範本，引導業者於契約中完整揭示如何使用資料、使用資料條件、在何種情況下將使用何種方法重行獲得當事人知悉同意、及在何種條件下將配合公權力揭露資料；並清楚使消費者知悉可以行使權利的管道、賦予消費者充分的選擇權（選擇進入、選擇退出）及退出後效果...。藉以強化消費者對於業者利用資料的信賴，

本報告之智慧財產權屬於國家通訊傳播委員會

避免因不了解產生抗拒情形。

(二)針對群集化及去識別（匿名）資料的利用予以法源基礎

倘若資料自始並非個人資料，則無個資法的適用，合先敘明。惟當資料原始為個人資料，係經過特定方式處理、刪除、遮蓋或代換使之無法單獨識別特定個人，或以統計方式呈現，在我國個資法的適用脈絡之下，將個人資料進行上開處理使其無從識別特定個人、或使其以統計方式或群集化方法呈現，由於定性為資料的「處理」，必須依據原先蒐集時之同一合法事由為之（參照法務部法律字第 10703512280 號書函）。換句話說，將資料進行去識別化或群集化等「處理」不在原先蒐集時之特定目的內，除非符合法定目的外利用的事由，否則應重新獲得資料當事人的知悉同意。

現行個資法規範下，並無可供電信事業適用的法定目的外利用事由，致使欲於原蒐集目的外將電信資料進行去識別處理或群集化處理，需重行獲得資料當事人同意，在對當事人顯無傷害且無其他不利益情形時，此等法律適用狀況無異徒增資料應用成本。爰建議可評估何種情境的資料群集化或去識別化之利用對當事人權益無侵害或無其他不利益，將該情境於電信相關法律（電信法、或電信管理法）中予以明定，使之成為個資法的特別規定，使電信事業運用群集化或去識別化資料獲致穩固法源基礎。例如美國於電信第 222 條規定，允許電信業者在電信服務目的外使用、揭露群集化資料、或將之提供近用，此使美國電信業者將電信有關客戶資料之群集化處理，直接獲得合法權源。

(三)可考量創建創新實驗空間促進電信事業運用數據資料創新

現行我國在金融領域及無人載具產業領域皆有創新實驗機制的採行，此係透過法律制度創建一安全實驗空間，使創新實驗過程中免於觸法疑慮。我國電信事業是否本身為高度監理事業，而使得其利用數據資料進行創新服務將增高觸法風險，導致事業的創新想法或活動將受到壓抑，值得持續觀察、探討。倘經衡量認有以法律制度創設特別創新實驗空間之必要，則立法形式上，

本報告之智慧財產權屬於國家通訊傳播委員會

可採取制定專法方式，或於現行法（電信法、或電信管理法）中增訂專章，敘明得申請創新實驗的條件，並例示創新實驗過程中得排除之法規。

(四)可考量推行其他促成電信事業數據運用的機制

近期主要國家討論資料中介機制或資料銀行等機制，以促成資料的流通及共享，惟觀諸此類機制在國外的發展，多屬小規模的試作，其中以攸關民生經濟 Open Banking 概念，使同一當事人在不同機構間的資料流通（以當事人同意為前提）之運作最具成熟度，然此機制確實可能成為不同類型資料混搭、異業結合運用數據資料進行創新服務的雛形，值得持續保持關注。

本報告之智慧財產權屬於國家通訊傳播委員會

附錄

附錄1：電信加值應用大調查問卷



您好！歡迎來到本次網路公眾意見諮詢

本問卷採匿名制，系統不會留下您的任何資料，期待您能安心的提供寶貴意見，以供政府施政之參考：

＊電信資料的定義：電信業者對其用戶或電信使用人使用電信服務後所產生的資料，例如：電信號碼、消費紀錄、位置資訊、身分驗證等。

議題一、為了公共利益，您認為電信事業該如何配合政府使用電信資料？

1您是否支持政府因應疫情，採用簡訊實聯制的方式進行防疫工作？ *

在簡訊實聯制下，電信業者會取得個人資料，例如：手機號碼、當下時間及場所代碼等資訊，當政府有防疫需求時，才會使用這些資料。

- ○ 我完全支持
- ○ 有條件支持，如果政府能清楚說明：
- ○ 我完全不支持，因為：

本報告之智慧財產權屬於國家通訊傳播委員會

議題一、為了公共利益，您認為電信事業該如何配合政府使用電信資料？

1您是否支持政府因應疫情，採用簡訊實聯制的方式進行防疫工作？ *

在簡訊實聯制下，電信業者會取得個人資料，例如：手機號碼、當下時間及場所代碼等資訊，當政府有防疫需求時，才會使用這些資料。

- ◉ 我完全支持
- ○ 有條件支持，如果政府能清楚說明：
- ○ 我完全不支持，因為：

英國政府推出新冠肺炎接觸史追蹤app「NHS COVID-19 app」供民眾使用，並宣稱政府無法透過該app蒐集的資料識別使用者。但仍有報導指出，英國政府曾考量將該app蒐集資料用於辨識使用者，引發民眾質疑與討論。

議題一、為了公共利益，您認為電信事業該如何配合政府使用電信資料？

1您是否支持政府因應疫情，採用簡訊實聯制的方式進行防疫工作？ *

在簡訊實聯制下，電信業者會取得個人資料，例如：手機號碼、當下時間及場所代碼等資訊，當政府有防疫需求時，才會使用這些資料。

- ○ 我完全支持
- ◉ 有條件支持，如果政府能清楚說明：
- ○ 我完全不支持，因為：

本報告之智慧財產權屬於國家通訊傳播委員會

我有條件支持，如政府能清楚說明： *

請選擇 1 ~ 3 個選項

複選 此題必填

- ☐ 如何做好資安以防止資料外洩
- ☐ 發生資料外洩時的應變措施
- ☐ 政府不會在防疫的特定目的外利用電信資料（例如警察利用簡訊實聯制取得的資訊偵辦犯罪）
- ☐ 電信資料將於保存期限（28天）後刪除
- ☐ 其他

議題一、為了公共利益，您認為電信事業該如何配合政府使用電信資料？

1 您是否支持政府因應疫情，採用簡訊實聯制的方式進行防疫工作？ *

在簡訊實聯制下，電信業者會取得個人資料，例如：手機號碼、當下時間及場所代碼等資訊，當政府有防疫需求時，才會使用這些資料。

- ○ 我完全支持
- ○ 有條件支持，如果政府能清楚說明：
- ◉ 我完全不支持，因為：

我完全不支持，因為： *

請選擇 1 ~ 3 個選項

複選

- ☐ 有資安疑慮
- ☐ 政府有可能在防疫的特定目的外利用電信資料（例如警察利用簡訊實聯制取得的資訊偵辦犯罪）
- ☐ 不確定政府是否會於保存期限（28天）後將電信資料刪除
- ☐ 可能暴露自己的日常活動行蹤
- ☐ 簡訊實聯制對疫調幫助有限
- ☐ 簡訊實聯制可能會耗費龐大政府預算
- ☐ 其他

本報告之智慧財產權屬於國家通訊傳播委員會

2 您是否支持政府因應疫情，採用電子圍籬智慧監控系統的方式進行防疫工作？ *

電子圍籬系統是透過手機與基地台之間的聯繫，確認民眾的所在位置，因此政府可以透過追蹤門號確認居家檢疫者所在位置。

- ◉ 我完全支持
- ○ 有條件支持，如果政府能清楚說明：
- ○ 我完全不支持，因為：

新加坡政府也推出新冠肺炎居家檢疫系統，供入境人士使用，政府每天會不定時向居家檢疫者發送簡訊，居家檢疫者則必須開手機GPS功能回傳位置資訊，違反規定的人將面臨比台灣更嚴厲的處罰，包含罰金及有期徒刑，甚至會註銷簽證。

2 您是否支持政府因應疫情，採用電子圍籬智慧監控系統的方式進行防疫工作？ *

電子圍籬系統是透過手機與基地台之間的聯繫，確認民眾的所在位置，因此政府可以透過追蹤門號確認居家檢疫者所在位置。

- ○ 我完全支持
- ◉ 有條件支持，如果政府能清楚說明：
- ○ 我完全不支持，因為：

我有條件支持，如政府能清楚說明： *

請選擇 1 ~ 3 個選項

複選 此題必填

- □ 如何做好資安以防止資料外洩
- □ 政府不會在防疫的特定目的外利用電信資料（例如警察利用電子圍籬系統取得的資訊偵辦犯罪）
- □ 如何確保在居家檢疫期間結束後，政府會刪除留存資料，且不再持續追蹤定位
- □ 其他

本報告之智慧財產權屬於國家通訊傳播委員會

2您是否支持政府因應疫情，採用電子圍籬智慧監控系統的方式進行防疫工作？ *

電子圍籬系統是透過手機與基地台之間的聯繫，確認民眾的所在位置，因此政府可以透過追蹤門號確認居家檢疫者所在位置。

- ○ 我完全支持
- ○ 有條件支持，如果政府能清楚說明：
- ◉ 我完全不支持，因為：

我完全不支持，因為： *

請選擇 1 ~ 3 個選項

複選

- ☐ 有資安疑慮
- ☐ 政府有可能在防疫的特定目的外利用電信資料（例如警察利用電子圍籬系統取得的資訊偵辦犯罪）
- ☐ 不確定政府是否會於居家檢疫期間結束後，停止追蹤及將電信資料刪除
- ☐ 可能因為手機定位不準確，反而造成困擾
- ☐ 對防疫幫助有限，因為有漏洞可鑽（例如：偷溜出門故意不帶手機）
- ☐ 電子圍籬監控可能會耗費龐大政府預算
- ☐ 其他

議題二、您同意電信業者加值利用電信資料嗎？

1您是否希望電信業者利用電信資料提供「身分識別」相關的創新服務？ *

在愛沙尼亞，由電信業者提供手機身分證服務，不需要讀卡機，手機即可作數位身分證使用。您是否希望我國電信業者提供類似服務？

- ○ 是，我完全支持
- ○ 如果能達成以下條件，我願意支持：
- ○ 否，因為：

本報告之智慧財產權屬於國家通訊傳播委員會

1 您是否希望電信業者利用電信資料提供「身分識別」相關的創新服務？ *

在愛沙尼亞，由電信業者提供手機身分證服務，不需要讀卡機，手機即可作數位身分證使用。您是否希望我國電信業者提供類似服務？

◉ 是，我完全支持

○ 如果能達成以下條件，我願意支持：

○ 否，因為：

> 台灣網路公司也嘗試建立TWID身分識別中心，用戶需向電信業者提供手機號碼及身分證字號，由電信業者確認該用戶是否為申辦門號的本人，這個服務也應用在我國因應疫情實施的「口罩實名制2.0」上，讓用戶能利用手機門號進行身分認證，在智慧型手機上登記購買口罩。

1 您是否希望電信業者利用電信資料提供「身分識別」相關的創新服務？ *

在愛沙尼亞，由電信業者提供手機身分證服務，不需要讀卡機，手機即可作數位身分證使用。您是否希望我國電信業者提供類似服務？

○ 是，我完全支持

◉ 如果能達成以下條件，我願意支持：

○ 否，因為：

如果能達成以下條件，我願意支持電信業者應用電信資料提供「身分識別」相關的創新服務： *

複選

☐ 確保身分不會被盜用

☐ 手機遺失時可立即停用身分識別功能(類似信用卡遺失時的銀行止付功能)

☐ 其他

本報告之智慧財產權屬於國家通訊傳播委員會

1您是否希望電信業者利用電信資料提供「身分識別」相關的創新服務？ *

在愛沙尼亞，由電信業者提供手機身分證服務，不需要讀卡機，手機即可作數位身分證使用。您是否希望我國電信業者提供類似服務？

○ 是，我完全支持

○ 如果能達成以下條件，我願意支持：

◉ 否，因為：

我不希望電信業者應用電信資料提供「身分識別」相關的創新服務，原因為： *

複選

☐ 我擔心身分被盜用

☐ 我擔心手機遺失時無法立刻停止身分識別功能(類似信用卡遺失時的銀行止付功能)

☐ 其他

2您是否希望電信業者利用電信資料提供「金融科技」相關的創新服務？ *

韓國電信業者、銀行業者和金融徵信機構三方合作，由電信業者以AI分析其使用者的電信帳單信用紀錄，交由銀行業者依據信用紀錄提供該使用者金融服務方面的優惠。您是否希望我國電信業者提供類似服務？

○ 是，我完全支持

○ 若能達成以下條件，我願意支持：

○ 否，因為：

本報告之智慧財產權屬於國家通訊傳播委員會

2 您是否希望電信業者利用電信資料提供「金融科技」相關的創新服務？ *

韓國電信業者、銀行業者和金融徵信機構三方合作，由電信業者以AI分析其使用者的電信帳單信用紀錄，交由銀行業者依據信用紀錄提供該使用者金融服務方面的優惠。您是否希望我國電信業者提供類似服務？

◉ 是，我完全支持

○ 若能達成以下條件，我願意支持：

○ 否，因為：

> 我國電信業者與國內銀行已於2019年試辦手機門號辦理貸款服務，讓還沒有信用紀錄的年輕人能透過電信費的繳費情形獲得信用加分，向銀行取得小額貸款。

2 您是否希望電信業者利用電信資料提供「金融科技」相關的創新服務？ *

韓國電信業者、銀行業者和金融徵信機構三方合作，由電信業者以AI分析其使用者的電信帳單信用紀錄，交由銀行業者依據信用紀錄提供該使用者金融服務方面的優惠。您是否希望我國電信業者提供類似服務？

○ 是，我完全支持

◉ 若能達成以下條件，我願意支持：

○ 否，因為：

若能達成以下條件，我願意支持電信業者應用電信資料提供「金融科技」相關的創新服務： *

複選

☐ 電信業者與銀行共享資料，不會對我造成不利影響（例如因遲繳電信費用的紀錄造成銀行信用等級降低）

☐ 確保資料安全性

☐ 不會被用在行銷用途（例如一直接到貸款行銷簡訊或電話）

☐ 其他

本報告之智慧財產權屬於國家通訊傳播委員會

2 您是否希望電信業者利用電信資料提供「金融科技」相關的創新服務？ *

韓國電信業者、銀行業者和金融徵信機構三方合作，由電信業者以AI分析其使用者的電信帳單信用紀錄，交由銀行業者依據信用紀錄提供該使用者金融服務方面的優惠。您是否希望我國電信業者提供類似服務？

- ○ 是，我完全支持
- ○ 若能達成以下條件，我願意支持：
- ◉ 否，因為：

我不希望電信業者應用電信資料提供「金融科技」相關的創新服務，原因為： *

複選

- □ 電信業者與銀行共享資料，可能會對我造成不利影響（例如因遲繳電信費用的紀錄造成銀行信用等級降低）
- □ 擔心資料安全性問題
- □ 擔心電信資料會被用在行銷用途（例如一直接到貸款行銷的簡訊或電話）
- □ 其他

3 您是否希望電信業者利用電信資料提供「交通運輸」相關的創新服務？ *

在英國，電信業者EE與Atkins工程公司合作，利用電信資訊監控M25高速公路上的交通流量，該路段有機場、工業區與民眾通行要道等，EE將電信資料經匿名處理轉化為可分析資料，交由工程公司應用分析規畫道路工程的時間安排，保持高速公路的暢通。您是否希望我國電信業者提供類似服務？

- ○ 是，我完全支持
- ○ 若能達成以下條件，我願意支持：
- ○ 否，因為：

本報告之智慧財產權屬於國家通訊傳播委員會

3 您是否希望電信業者利用電信資料提供「交通運輸」相關的創新服務？ *

在英國，電信業者EE與Atkins工程公司合作，利用電信資訊監控M25高速公路上的交通流量，該路段有機場、工業區與民眾通行要道等，EE將電信資料經匿名處理轉化為可分析資料，交由工程公司應用分析規畫道路工程的時間安排，保持高速公路的暢通。您是否希望我國電信業者提供類似服務？

- ◉ 是，我完全支持
- ○ 若能達成以下條件，我願意支持：
- ○ 否，因為：

國內電信業者於國一暨臺74線匝道處設置諸多先進智慧交通偵測設備，即時監控區域交通狀況，並大幅降低人力支援成本；除此之外，亦有他電信業者利用統計過去3個月的特定景點平均人流量，設計台灣景點人潮警示燈號。

3 您是否希望電信業者利用電信資料提供「交通運輸」相關的創新服務？ *

在英國，電信業者EE與Atkins工程公司合作，利用電信資訊監控M25高速公路上的交通流量，該路段有機場、工業區與民眾通行要道等，EE將電信資料經匿名處理轉化為可分析資料，交由工程公司應用分析規畫道路工程的時間安排，保持高速公路的暢通。您是否希望我國電信業者提供類似服務？

- ○ 是，我完全支持
- ◉ 若能達成以下條件，我願意支持：
- ○ 否，因為：

若能達成以下條件，我願意支持電信業者應用電信資料提供「交通運輸」相關的創新服務： *

複選

- ☐ 不會被電信業者或第三方追蹤自己的位置資訊
- ☐ 資料提供給第三方時，不可辨識出我的身分
- ☐ 資料不會被用來查緝交通違規事件
- ☐ 其他

本報告之智慧財產權屬於國家通訊傳播委員會

3 您是否希望電信業者利用電信資料提供「交通運輸」相關的創新服務？ *

在英國，電信業者EE與Atkins工程公司合作，利用電信資訊監控M25高速公路上的交通流量，該路段有機場、工業區與民眾通行要道等，EE將電信資料經匿名處理轉化為可分析資料，交由工程公司應用分析規畫道路工程的時間安排，保持高速公路的暢通。您是否希望我國電信業者提供類似服務？

- ○ 是，我完全支持
- ○ 若能達成以下條件，我願意支持：
- ◉ 否，因為：

我不希望電信業者應用電信資料提供「交通運輸」相關的創新服務，原因為：（可複選） *

複選

- ☐ 不想被電信業者或第三方追蹤自己的位置資訊
- ☐ 不確定資料提供給第三方時，是否仍能辨識出我的身分
- ☐ 不確定資料會不會被用來查緝交通違規事件
- ☐ 其他

4 您是否同意電信業者利用電信資料提供「商業應用」相關的創新服務？ *

在韓國，電信業者KT成立BigSight平台，將用戶分類為觀光人口、商圈人口及生活人口等類別進行分析，並向商家銷售人口分析數據及商業規劃服務。您是否希望我國電信業者提供類似服務？

- ○ 是，我完全支持
- ○ 若能達成以下條件，我願意支持：
- ○ 否，因為：

本報告之智慧財產權屬於國家通訊傳播委員會

4 您是否同意電信業者利用電信資料提供「商業應用」相關的創新服務？ *

在韓國，電信業者KT成立BigSight平台，將用戶分類為觀光人口、商圈人口及生活人口等類別進行分析，並向商家銷售人口分析數據及商業規劃服務。您是否希望我國電信業者提供類似服務？

- ◉ 是，我完全支持
- ○ 若能達成以下條件，我願意支持：
- ○ 否，因為：

> 我國電信業者亦推出人潮分析平台，以行動位置、客群輪廓、開放資料為基礎，統計分析每小時全台各地區域的人潮流量及客群樣貌，協助商家進行商業規劃。

4 您是否同意電信業者利用電信資料提供「商業應用」相關的創新服務？ *

在韓國，電信業者KT成立BigSight平台，將用戶分類為觀光人口、商圈人口及生活人口等類別進行分析，並向商家銷售人口分析數據及商業規劃服務。您是否希望我國電信業者提供類似服務？

- ○ 是，我完全支持
- ◉ 若能達成以下條件，我願意支持：
- ○ 否，因為：

若能達成以下條件，我願意支持電信業者應用電信資料提供「商業應用」相關的創新服務： *

複選

- ☐ 電信業者提供給商家或企業的資料，無法辨識出我的身分
- ☐ 電信業者或商家必須提供合理的補貼（例如：折抵電話帳單費用），不能無償將我的個人資料統計分析後營利
- ☐ 確保沒有個資外洩的風險
- ☐ 保證不會被商家行銷訊息騷擾
- ☐ 其他

本報告之智慧財產權屬於國家通訊傳播委員會

4 您是否同意電信業者利用電信資料提供「商業應用」相關的創新服務？ *

在韓國，電信業者KT成立BigSight平台，將用戶分類為觀光人口、商圈人口及生活人口等類別進行分析，並向商家銷售人口分析數據及商業規劃服務。您是否希望我國電信業者提供類似服務？

- ○ 是，我完全支持
- ○ 若能達成以下條件，我願意支持：
- ◉ 否，因為：

我不希望電信業者應用電信資料提供「商業應用」相關的創新服務，原因為： *

複選

- ☐ 不確定電信業者提供給商家或企業的資料，是否仍能辨識出我的身分
- ☐ 不想讓電信業者無償將我的個資統計分析後營利
- ☐ 有個資外洩的疑慮
- ☐ 以後可能被商家行銷訊息騷擾
- ☐ 其他

5 您認為電信事業創新應用電信資料時，應重視下列何項「個人資料保護」相關議題？ *

請選擇 1 ~ 5 個選項

複選

- ☐ 有無事先做過隱私風險評估
- ☐ 資料會不會提供給第三方
- ☐ 提供給第三方的資料，是否仍能辨識出我的身分
- ☐ 如果需要創新利用我的個資，應事先取得我的同意
- ☐ 應讓我更方便地行使個資相關權利（例如可請求刪除、請求停止利用等權利）
- ☐ 應確保資料安全（包含第三方的資安能量）
- ☐ 電信業者應確保第三方遵守個資法規範
- ☐ 資料是否會傳輸到台灣以外的地區
- ☐ 應確保資料於保存期限後，徹底刪除

本報告之智慧財產權屬於國家通訊傳播委員會

6 您認為在數位化的浪潮下，電信業者應最優先發展哪一領域的創新應用？ *

- ○ 身分識別類
- ○ 金融科技類
- ○ 交通運輸類
- ○ 商業應用類
- ○ 以上都不應該發展
- ○ 其他

若您對電信產業為了公共利益或商業創新而利用電信資料的議題還有其他寶貴意見，歡迎留下您的建言：

請填入文字

本報告之智慧財產權屬於國家通訊傳播委員會

附錄2：電信加值應用大調查問卷結果

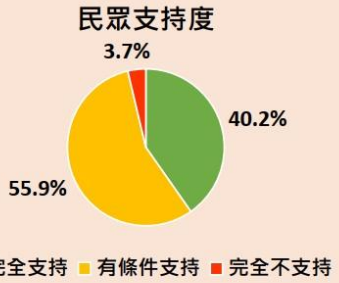




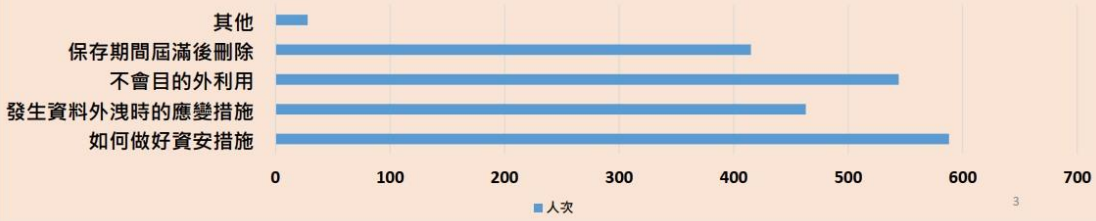
本報告之智慧財產權屬於國家通訊傳播委員會

用簡訊防疫？

民眾是否支持政府因應疫情，採用簡訊實聯制的方式進行防疫工作？



有條件支持的民眾希望政府清楚說明的事項（複選題，至多選擇三項）



3

用簡訊防疫？

民眾完全不支持的原因（複選題，至多選擇三項）



其他民眾考量因素

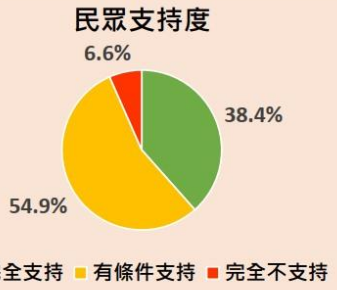
- ✓ 希望能完整揭露運作與技術框架
- ✓ 希望電信業不得以此資料串連其他資料
- ✓ 希望能有明確法令授權依據
- ✓ 讓當事人有權查詢追蹤個資如何被使用

4

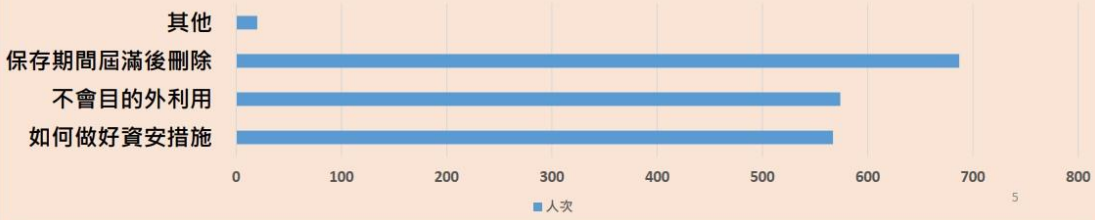
本報告之智慧財產權屬於國家通訊傳播委員會

用電子圍籬來防疫？

民眾是否支持政府因應疫情，採用電子圍籬智慧監控系統的方式進行防疫工作？



有條件支持的民眾希望政府清楚說明的事項（複選題，至多選擇三項）



5

用電子圍籬來防疫？

民眾完全不支持的原因（複選題，至多選擇三項）



其他民眾考量因素

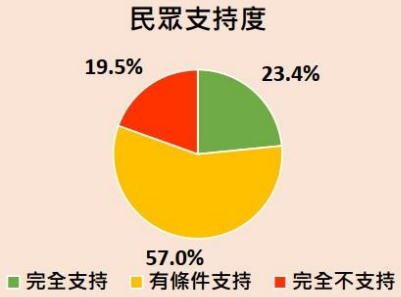
- ✓ 希望建立適當的事後定期稽核機制
- ✓ 人民有其活動的隱私權，縱使定位不精確也會侵害其隱私權
- ✓ 希望能有明確法令授權依據
- ✓ 希望能完整揭露運作與技術框架

6

本報告之智慧財產權屬於國家通訊傳播委員會

身分識別

民眾是否希望電信業者利用電信資料提供「身分識別」相關的創新服務？



有條件支持的民眾希望能達成的條件（複選題）



7

身分識別

民眾完全不支持的原因（複選題）



其他民眾考量因素

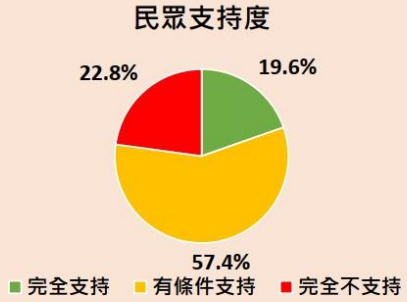
- ✓ 台灣販賣人頭門號的情況嚴重，可能會擴大冒用身分犯罪問題
- ✓ 希望能禁止串連其他資料
- ✓ 手機權限安全性相對於電腦較差，若要限制機種則會有近用權的問題
- ✓ 希望相關軟體能開放原始碼，杜絕隱匿後門的可能

8

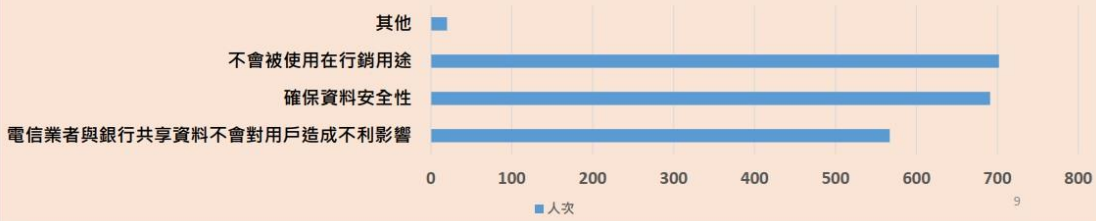
本報告之智慧財產權屬於國家通訊傳播委員會

金融科技

民眾是否希望電信業者利用電信資料提供「金融科技」相關的創新服務？



有條件支持的民眾希望能達成的條件（複選題）



9

金融科技

民眾完全不支持的原因（複選題）



其他民眾考量因素

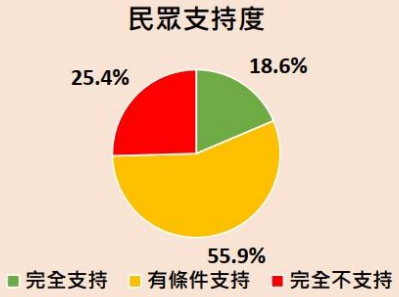
- ✓ 希望不要讓電信與金融業者資料共享，因為其掌握著使用者重要個資，雞蛋不要放在同一個籃子裡
- ✓ 電信及金融業者的聯合可能造成壟斷的情形
- ✓ 民眾與電信、銀行業者間資訊不對稱
- ✓ 電信資料並未如其他信用評級的資料，可以作為信用評鑑的依據

10

本報告之智慧財產權屬於國家通訊傳播委員會

商業應用

民眾是否希望電信業者利用電信資料提供「商業應用」相關的創新服務？



有條件支持的民眾希望能達成的條件（複選題）



11

商業應用

民眾完全不支持的原因（複選題）



其他民眾考量因素

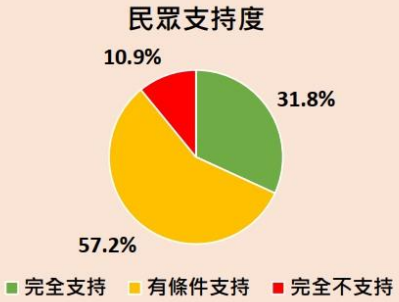
- ✓ 人不是商品，需考量人性尊嚴
- ✓ 完整揭露運作與技術框架
- ✓ 可能讓電信業者有壟斷的可能
- ✓ 應讓使用者能選擇對同一公司之各別創新服務分別提供資料，而不是同意同一公司之個人資料條款後所有服務均可以使用其個資

12

本報告之智慧財產權屬於國家通訊傳播委員會

交通運輸

民眾是否希望電信業者利用電信資料提供「交通運輸」相關的創新服務？



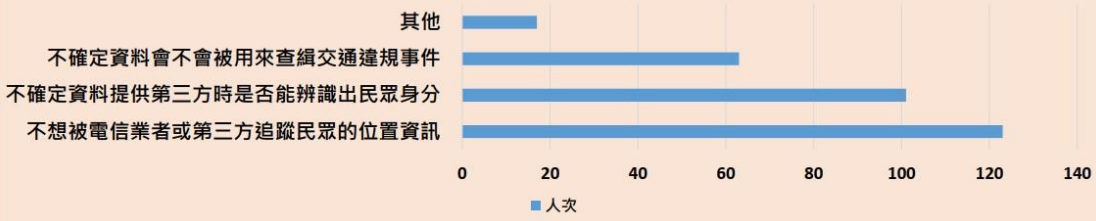
有條件支持的民眾希望能達成的條件（複選題）



13

交通運輸

民眾完全不支持的原因（複選題）



其他民眾考量因素

- ✓ 希望能定期銷毀相關電信交通運輸資料
- ✓ Google 等網路服務業者已經在這個領域取得成功，電信業者有發展的必要嗎？
- ✓ 可能會有政府監控人民行蹤的疑慮
- ✓ 希望能完整揭露運作與技術框架

14

本報告之智慧財產權屬於國家通訊傳播委員會





本報告之智慧財產權屬於國家通訊傳播委員會

附錄3：110 年 8 月 2 日座談會（一）會議紀錄

110 年度電信事業運用數據資料提供創新應用服務治理模式

座談會（一）

一、 時間：110 年 8 月 2 日下午 14:00 至 17:00

二、 地點：財團法人資訊工業策進會科技法律研究所行遠講堂

三、 與會人員：詳參簽到表

四、 會議記錄：

議題一： 電信事業加值利用之障礙	14：10 至 14：40
中華電信大數據處 闕仁斌總監	1. 目前電信資料於身分識別的加值應用，很適合運用在政府服務，像最近預約疫苗的健保快易通，便是利用健保卡後幾碼加上電信的動態 IP 確認身分，完成 APP 的雙因子認證。若透過以往自然人憑證的方式，無法如此快速提供手機線上認證服務。 2. 電信數據加值也運用在交通流量管控部分，因為許多地方沒有電子道路收費系統（ETC），為了交通控管，要設立許多監視器或其他儀器來監測紅綠燈或行人的影像，我覺得比較不適當。如果透過電信人流人潮資料，經過演算法變成車流數據後，就可以讓交通管理單位知道有沒有塞車的情形。 3. 電信業者運用數據配合政府完成創新服務，比較容易成功，因為政府在用資料時會研議相關法令，電信業者在合法前提與政府合作配合上沒有障礙的；和民間業者合作資料創新運用比較容易受到質疑~是否超越資料蒐集之目的外使用。 4. 中華電信推出資料加值創新運用主要仍是希望能幫新世代建立更好的未來服務，遵守個資法的規定並限制於目的內使用；由於資料在目的外利用需要本人的同意時，墊高了資料運用成本，這讓中華電信

本報告之智慧財產權屬於國家通訊傳播委員會

議題一： 電信事業加值利用之障礙	14：10 至 14：40
	在每一次創新時，都會希望不要踩到紅線，在規劃流程時都會與法務討論確認有無符合法規。 5. 加值利用的服務，常在發想的階段就因為法規的關係而無法推行，因此在現今法規下能應用的方面其實沒那麼寬，我國電信業者常常被拿來跟國外的發展比較，說我們發展很慢，而我們走得很慢是因為法規的限制。
達文西法律事務所 葉奇鑫律師	我過去在中華電信服務時，也常常被諮詢關於個資法的問題，中華電信其實是相當守法的企業，每件事情都會確認是否合法。其實目的外利用需要取得當事人同意的部分造成的問題不大，不過在加值應用時，不能去識別化會比較麻煩，因為當初在蒐集個資的時候沒辦法把蒐集目的寫得那麼詳細跟特定，就變成中華電信有很多的資料，但要做目的外的加值利用是比較困難的事情，因為即使希望用去識別化的方式，但我國對於去識別化也沒有清楚的規範，這部分也請遠傳的江律師發表意見。
遠傳電信 江奎徵律師	1. 公司推出新的產品或服務時，都會諮詢法遵的意見。電信業者擁有個資本身，是沒有問題的，但法律關注的重點是在於怎麼適法的處理個資，首先需要取得當事人同意，這樣資料就可以去活用，如果沒辦法取得當事人同意時，就必須去識別化。 2. 電信業者的障礙是希望公部門能有更明確的規則，只要規則明確了，大家就可以用創新的方式找到解決之道。舉例而言，像是針對「同意」的部分，我就有在遠傳電信宣導，只要有取得明確的同意，就可以進行利用，而其實在產品介面的設計，都可以很明確的呈現蒐集目的等等要件來去取得使用者同意。 3. 同樣的，電信業者希望「去識別化」能夠有一個很明確的標準，因為去識別化沒有很明確的規範，所以我們在實行上比較有問題，電信業者也期待政府能有個明確的規範去畫一個框架，這樣大家能在這個框架下做更多的創新。
達文西法律事務所 葉奇鑫律師	其實不只是電信產業，連醫療產業也會很想要將個資去識別化運用，但他們也不知道具體標準是什麼，目前也

本報告之智慧財產權屬於國家通訊傳播委員會

議題一： 電信事業加值利用之障礙	14：10 至 14：40
	還沒找到有哪個國家有訂定好的去識別化標準。
東吳大學法律學系 余啟民副教授	1. 電信事業不完全等於電信業，因為電信管理法會依據第 21 條去認定特定的電信事業，依照電信管理法第 21 條需要綜合考量，所以消費者保護會浮現出來，會進一步去要求定型化契約，這時候消費隱私的問題也會浮現，所以我們第一個問題是要定義電信事業。 2. 第二，電信事業的過去和現在，在個資法上都是被高度關切的議題，而根據問卷的結果，我們可以知道漸進式的發展可能會比較好，我們也需要關注交換資料的「對口」承接的成熟度，如果對口的承接度不夠成熟，會有很大的風險，這時候就會涉及法規的鬆綁或調適。舉例來說，像在交通運輸的運用可能沒問題，但到了金融科技的服務，有時候會涉及身分識別，而身分識別是很跨出去的議題，我相信金管會很注意這個議題，甚至未來金管會就會進行法規的鬆綁或評估。 3. 所以我覺得電信事業的個人資料應用太過浮濫，這個浮濫並不是指電信事業濫用個人資料，而是很多人濫用蒐集的個資。我舉個例子，我的車貸資料給銀行後，從此以後我時常收到很多行銷廣告，這部分就涉及到應用的資料太過複雜，所以我覺得在做創新應用的時候，從交通運輸到金融科技，甚至在到身分識別的過程中，要透過一定的篩選，這階段應用完後，下一個階段要加入一些因子去阻斷，讓這些資料不能繼續利用，我認為對於民眾而言會增加他們的信心。 4. 還有很重要的是中華電信的雙因子認證，其實只能認證出門號的使用者，不一定代表門號的申請者，當初簽署個資蒐集同意書的人可能是門號的申請者，而不是門號的使用者，這部分也是可以思考的問題。
中央研究院法律學研究所 邱文聰主任	1. 首先我提出第一個問題，透過電信門號進行身分識別，像是疫苗預約的案例，我同意在個人同意的前提下協助個人方便的應用，但後端的問題是，像這

本報告之智慧財產權屬於國家通訊傳播委員會

議題一： 電信事業加值利用之障礙	14：10 至 14：40
	樣的身分識別資訊被留下來後，會不會被進一步的應用或串連，變成用戶的數位足跡，這是身分識別上需要加以考慮的問題。 2. 第二個問題是，身分識別的加值利用是大家認為最該優先發展的，但也是大家會有所疑慮的，這會涉及後端再利用如何管控的問題，因為這些創新利用很多都是涉及個資的再利用，要應用去識別化的技術可能會面臨挑戰，而電信門號的去識別化可能會遇到困難，因為去識別化通常會把門號去掉用另一個代號去替代，但這個代號是可能被換回來的，在歐盟的標準下這可能是沒有做到去識別化的，這也讓去識別化作為二次利用的基礎是比較薄弱的。 3. 第三，我倒覺得可以從如何更便利的行使個資相關權利這點去出發，像是中華電信可以提供客戶去查詢中華電信有沒有利用他們的資料，讓客戶很便利地行使他們的權利，讓再利用可以獲得客戶的同意。
中華民國消費者文教基金會 蘇錦霞律師	這個議題主要跟電信業者有關，但電信業者的難處也是消費者的難處，因為業者在推動時還是得符合消費者的認知跟傾向，所以最主要的除了個資利用外，還要考慮科技技術的水準到達什麼程度，因為消費者希望的是穩定性，希望個資不要有外漏的情形，也就是說電信業者能夠保護消費者的資料到什麼程度，這部分電信業者必須讓消費者知道在科技技術上能做到什麼程度。
世新大學法律學系 翁逸泓主任	1. 從英國的經驗來看，前陣子金管會有受到開放銀行的磨練，現在電信事業比較像英國 2020 年 8 月推動的開放通訊，開放通訊其實就是想讓消費者根據自己的意願去進行通傳業者的產品運用，結合支付跟第三方業者的資料共享，讓資料更加流通，這很像歐盟想做的資料治理，當然公眾諮詢時也面對很多問題，像是要標準化等等。 2. 而擁有很多資料的業者會有警惕，因為怕新創業者也來蒐集這些資料，但比較重要的還是讓消費者可以完全的控制自身的資料，以剛剛健保快易通的行動門號認證來說有一點是做得很好的，我們確實是可以看到手機認證的合約，不過我比較好奇的是，

本報告之智慧財產權屬於國家通訊傳播委員會

議題一： 電信事業加值利用之障礙	14：10 至 14：40
	為什麼合約在事後會不容易找到呢？這也是英國在關於開放通訊的公眾意見諮詢中所收到的諮詢意見，也就是要清楚地知道這個資料處理（利用）契約的內容。 3. 關於通知或動態的同意，就是讓消費者知道他們的資訊被再利用的情況，電信業者跟其他行業在這上面不一樣的地方，在於電信業者是最容易跟消費者溝通的行業，之前我在我國處理過的問題就是醫療資料的再同意，而在醫療的再同意過程中，研究者本都感到十分地耗費精力；但理論上電信業者做起來會佔有優勢，可以像健保快易通一樣，告訴使用者打疫苗跟篩檢的結果，讓民眾知道自己的資料在哪裡，使民眾能更容易的接近這些資訊，而更有效率地進行動態的同意。 4. 我國不管是開放銀行或開放通訊都會遇到很大的阻礙，首先是我國的法規沒有那麼清楚，只有一個個資法，而且是跟不上科技時代的個資法；也沒有一個專責機關。像是對於單純的電信業的加值利用，一定是國家通訊傳播委員會要作為主管機關，但如果是跨領域的應用，這時候主管機關的認定又會有爭議。
輔仁大學法律學系 張陳弘助理教授	1. 我們需要電信業者具體的說你們遇到的障礙是什麼，才能來討論這些障礙需要怎麼的協助，目前聽起來主要有兩個問題，一個是目的外利用取得當事人同意的成本過高，第二就是去識別化的標準是什麼。 2. 這兩個也是實務上常常遇到的問題，但從我的角度來看仍有點抽象，譬如說去識別化的標準會取決於電信業者是針對哪一類個資在什麼目的下做什麼利用，這都會影響在法律規範下應該要去識別化的程度，而資安的水準也會影響到去識別化程度的判斷，所以業者可能可以提出更具體的案例，這樣在討論上比較能順利進行。 3. 而取得當事人同意的部分也一樣，也會因為針對哪一類個資在甚麼目的下做甚麼利用而有所差別。譬

本報告之智慧財產權屬於國家通訊傳播委員會

議題一： 電信事業加值利用之障礙	14：10 至 14：40
	如說在健康個資的再利用，業者的疑問是一開始在 A 目的下取得同意，但業者要目的外利用時就遇到障礙，因為特種個資必須用書面同意的方式取得，事後要取得書面同意是很難做到的，這就是比較具體的障礙，有具體的問題我們就可以討論，如果在現行個資法的解釋無法解決，就可以考慮啟動修法。 4. 剛剛邱老師有提到，這些障礙的克服有根本性的困難時，我們可以考慮用強化當事人權利的方式，透過事後當事人權利的行使，來達到資訊保護的目的，像是加州的 CCPA 就跟歐洲個資保護採取不同的立法方式，CCPA 一開始不要求蒐集者取得當事人同意，而是強化業者讓當事人的權利可以更便利的行使，這也是我們立法上能考慮的方式。我認為業者可能必須把障礙描述得更具體一點，這樣我們才有辦法討論出更具體的解決方式。
達文西法律事務所 葉奇鑫律師	因為時間的關係，所以電信業者沒辦法很具提的提出問題，但在稍後的議題，也就是電信業者的加值利用，我們可以進行更深入的討論。

議題二：公共利益	14：50 至 15：20
台灣人權促進會 周冠汝專員	1. （回應議題一部分）我想先延續前面這一題的討論，我們在討論的都是消費者買了這個服務而留下資料，而業者可以如何的利用。我想要補充的是在消費者的資料被當作石油時，我們要怎麼達成政府、業者跟人民間權利的平等。 2. 像是在交通運用上，當一個政府利用位置資料分析人流活動，依據這個分析要在哪裡設公車站牌時，這樣的決策方向可能會忽略沒使用手機或不想被追蹤的人的需求，另一方面表示政府及業者只服務那些服膺於這個體制下的人。 3. 2004 年紐約也曾經釋出計程車的資料，這個資料就被研究拿出來再識別，識別出脫衣舞俱樂部的常客名單，這個問題在於，消費者常常在本身不知道的情形下，其所留下的資料已經對他造成了影響。 4. 另外像是行銷訊息，我們相較之下比較能知道是誰

本報告之智慧財產權屬於國家通訊傳播委員會

議題二：公共利益	14：50 至 15：20
	洩露了我的個資，像是現在使用臉書，使用者可以去看到部分內容，例如「商家上傳有我聯絡資料的廠商」，其中也包含我曾使用過但不是用我的名字註冊的門號，如果臉書沒有公開這個資料，我永遠都不會知道這些商家有使用我的個資，所以民眾有辦法查詢自己個資的現況這點很重要。 5. 既然我們的身分資料那麼重要，是不是需要優於個資法的保護？企業當然會看是否符合個資法，但現在再強調企業社會責任時，我們可能可以試看看給消費者更多的保護。 6. 回到這一個議題，最近簡訊實聯制的案子，我們知道不只檢警，在沒有疫情前，像是經濟部也會跟電信業者調取資料，但這些調取本身都是用公文，不像通保法有一個比較完整的機制，所以希望政府在跟電信業者調資料的時候，還是得有一個完整的流程，和定期公布請求次數和依據。在討論目的外利用時，也要先釐清過去各機關調取電信用戶資料的狀況，才能劃出需要排除目的外利用的確切範圍。 7. 另外一部分，業者能做的事情像是中華電信跟台灣大哥大在企業社會責任這邊揭露配合政府交出民眾個資的比例，但仍未同國際網路平台和電信業發布的透明報告公布請求次數，不只電信事業，其他事業也可以告訴民眾說當政府來調個資的時候，我是用什麼方式去決定，或是我同意多少不同意多少等等。
達文西法律事務所 葉奇鑫律師	確實目前法規有很多檢討的空間，檢警爭議我們是拿來做一個特例來帶出目的外利用的議題，原本衛福部保證簡訊時聯制的資料不能被目的外利用，但檢方的意見可能是：在犯罪偵查時本來就可以調資料，為什麼行政機關可以阻礙我們的犯罪偵查呢？衛福部沒有權利去禁止行政機關調取這個資料。像是英國經驗，就是用全部匿名化的方式去處理這個問題，但缺點就是沒辦法把資料拿來作疫調。
中央研究院法律學研究所 邱文聰主任	1. 公共利益這個帽子是個魔戒，你只要有資料後，不管你再怎麼保證不會目的外利用，只要面對公共利益這個基礎，就會被擴大他的使用範圍。 2. 英國的做法其實是透過去中心化的方式去處理，讓

本報告之智慧財產權屬於國家通訊傳播委員會

議題二：公共利益	14：50 至 15：20
	政府跟業者無法去追蹤到個人，但當我們的簡訊實聯制是透過門號傳送到集中的資料庫時，這就不可能做到去識別化，我相信電信業者非常清楚這點。 3. 在討論去識別化的時候，一開始設定系統時，就必須把這個概念設定進去，不要有功能轉換或目的轉換。簡訊實聯制有這個問題，是因為政府當初就是覺得以後可以將資料做其他用途的利用來設計的，所以我們在一開始設計制度的時候就要決定我們的設計設想是什麼，這是很重要的。
中華電信大數據處 闕仁斌總監	1. 以簡訊實聯制來說，我們可以回頭說說原本是怎麼做的。一開始是民眾進商家時，要手寫電話跟個人資料，接下來有超商發展他們各自的實聯制系統，這時候唐鳳政委認為全國個資散落的情形不太好，所以要求電信業者幫忙。 2. 不過我們最初就有客戶的足跡，而我們也有在 14 天（應是 28 天）後完全刪除，所以希望大家知道，電信業者不是主動來做簡訊實聯制的，是因應政府的要求。 3. 回到最開始的問題，電信業者每走一步就會被刁難，因此最好的方法，就是政府帶著電信業者做。 4. 疫調最重要的就是確診者的軌跡，在疫調時很多人不會想公開他們的軌跡，如果沒有實聯制，政府很難畫定熱區來做疫調。
輔仁大學法律學系 張陳弘助理教授	1. 台灣社交距離 APP 跟簡訊實聯制的設計不太一樣，但同樣地資料保護影響評估（DPIA）程序都很重要，透過這個程序我們就可以確保 28 天後資料能夠自動刪除。 2. 我從新聞報導裡面認知的是，簡訊實聯制沒有發揮很大的作用，就是說我們沒辦法透過簡訊實聯制找出確診者跟有接觸的人。 3. 台灣社交安全距離 APP 現在有一樣的問題，我猜可能是因為資料撈不出來？所以我想要問的是，這兩種 APP 都很明顯，就是為了防疫，但是要如何說服民眾他們貢獻了個資，會有實質上的作用？
中華電信大數據處 闕仁斌總監	1. 簡訊實聯制資料不會撈不出來，因為資料就只有電話號碼跟場所代號，這概念很簡單，就是以人去看地方，再去看地方裡有誰，我也不知道為什麼新聞

本報告之智慧財產權屬於國家通訊傳播委員會

議題二：公共利益	14：50 至 15：20
	有這樣的報導，其實現在利用資料來做疫調是沒問題的。 2. 但社交安全距離 APP 的問題是確診者必須要自己上傳，使用者又必須先開啟藍芽，我是覺得不容易，而且他沒辦法確認時間，而疫調主要要找的是感染源。因此就以做疫調來說，我們是投入了很多才能快速找到這些關鍵因素。
達文西法律事務所 葉奇鑫律師	新聞報導是說實際上衛生局調取這些紀錄出來是沒什麼問題的，但是實際上很少去調，至於社交安全距離的問題是藍芽怎麼有辦法判斷距離？開發者是說靠信號強度辨別，這個信號強度是在作業系統的層面設定，後來 ios 跟 Android 也有去更新系統已開通這個功能。國發會當時看完就發現社交安全距離 APP 比較沒有個資的問題，也符合歐盟的標準，不過因為那時候疫情比較輕微，就沒有進行強力推行。
達文西法律事務所 葉奇鑫律師	1. 而且要知道下載量跟實際還有在使用的數量是不同的，這部分也需要考慮。 2. 簡訊實聯制的措施就是強制的，店員都要確認過有沒有上傳，所以目前以量來看，簡訊實聯制對防疫的貢獻可能是比較高的。
世新大學法律學系 翁逸泓主任	1. 簡訊實聯制有固定發布他們刪除的簡訊則數，但如果要貫徹資料透明，是不是可以一併地公布利用個資人（次）數、使用率、調取次數，讓大家能知道他到底有多大的公共利益，這樣民眾就不會有那麼多的疑問。所以除了公布刪除簡訊的則數，如果能夠更近一步知道我們在目的內跟目的外都被調取了多少，可能會更符合個資法上的透明原則。 2. 再來就是刪除資料的部分，我們防疫的特別條例第七條乃是帝王條款，所以個資法 11 條 3 項比例原則的檢驗，要通過是有難度的，所以我建議未來要做類似簡訊實聯制或其他電信加值應用，或許可以透過動態同意的方式，就可以在裡面做很多事項的告知，讓當事人選擇什麼時候要撤回，因此透過動態同意或許可以解決這個問題。 3. 回到 NHS Contact Tracing APP，其實他跟台灣社交距離 APP 比較像，比較大的差別是 NHS Contact Tracing APP 是官方的而台灣社交距離是非官方的；

本報告之智慧財產權屬於國家通訊傳播委員會

議題二：公共利益	14：50 至 15：20
	但是我們的簡訊實聯制跟 NHS Contact Tracing APP 是完全不一樣的，NHS Contact Tracing APP 可以直接用 APP 去掃實聯制的 QR code，不是分成兩軌。 4. 但我們現在分兩軌，就要確保兩軌都有符合個資法的要求，其實像健保資料庫，在健保署那邊就有一個人工智慧加值應用的要點，雖然這個要點有點奇怪，不過當初在做簡訊實聯制的時候是不是還沒有法規範？這部分可能就是政府的法律規範不明確問題。
中央研究院法律學研究所 邱文聰主任	簡訊實聯制 14 天（應是 28 天）刪除是因為目的已經結束，但為什麼電信業者可以保留大家的足跡超過 14 天（應是 28 天）而沒有刪除？
中華電信大數據處 闕仁斌總監	1. 其實中華電信每天收多少交多少，我們都有回報給主管機關，他們要不要公佈不是我們能控制的，電信業者純粹就是幫忙收取簡訊，提供查詢，在 14 天（應是 28 天）後刪除。因為政府也有預算問題，所以會希望看到電信業者的利用量，而且我們不會想要去利用這些資料，不會去發國難財。 2. 但為什麼軌跡資料可以超過 14 天（應是 28 天）不刪除，大家要先了解電信業者的軌跡資料沒有那麼精準，可能是兩百米乘以兩百米這樣的大小，而且我們本來就有蒐集軌跡資料，這是為了提供電信服務所必要的，不是為了防疫目的。 3. 而其實這些資料中華電信都放在機房裡面，與使用者的合約裡面本來就有像是當事人同意我們做分析或其他利用等等的條款，像是有些資料是預防萬一，因為有些要保存七年之類的，所以我們之所以沒有刪除這些電信資料主要是因為業務上還有服務客戶的需求。
達文西法律事務所 葉奇鑫律師	基地台裡面的資料目的就是為了電信服務，是基於契約目的蒐集，就像是用戶可以跟電信業者反應通訊不好等問題，或是調取通訊紀錄等等，基地台裡面的資訊跟電信服務是息息相關的，至於該保存多久，我認為最長就是電信業者還提供客戶服務的時間，而契約終止等沒有提供服務時就應該要刪除。

本報告之智慧財產權屬於國家通訊傳播委員會

議題三；身分識別	15：45 至 16：15
財團法人資訊工業策進會 宋佩珊主任	其實我們在申辦手機號碼的時候都會做身分認證的確認，所以基本上在做身分識別的服務會是很好的輔佐工具。
台灣走著瞧股份有限公司 柯志強商務經理	1. 在資訊安全跟資料保護上我們很難做到百分之百的防護，比較有可能的是平衡的方法，我認為可以先問客戶想不想取得這個服務，他們才會思考拿他的個資可以換到什麼服務或什麼權利；再來我們才要提出我們會怎麼保護你的個資；最後再向他們證明我們有沒有確實保護個資。 2. 像這次在繳稅的時候，健保卡的雙因子認證很便利，我會先想到用健保卡的後四碼去換這個服務是很值得，再想到政府會如何保護我健保卡後四碼的資料，最後才會思考如果健保卡後四碼洩漏會有什麼後果，而我會覺得這洩漏出去不會有什麼問題。所以用消費者的角度去想，才不會有媽媽覺得冷但你不冷的問題，一直在思考要多嚴格的保護消費者個資，我們應該去思考消費者到底在乎的是什麼。 3. 假設有個服務是提供身分證跟電話號碼可以得到一億元，大家都會同意，所以我們要先去想消費者需要什麼服務，再去想要怎麼保護，不是每一個小小新創的服務都需要非常嚴格的保護。
中央研究院法律學研究所 邱文聰主任	1. 針對愛沙尼亞的 mobile ID 跟 TWID 是不是一樣的事情，其實我不是很確定，因為愛沙尼亞除了要識別以外還需具有身分驗證的功能，像我們剛剛提到的例子，像是疫苗等等，其實不涉及電子簽章的身分驗證，所以必須先確定是談哪個問題。 2. 如果是談到身分識別，大家都知道不需要綁什麼手機或電腦之類的，如果需要身分驗證，才會牽涉到憑證該用什麼方式呈現或要附著在什麼硬體上。 3. 對於比較多元的身分驗證而言，如果是在手機或其它硬體上，我會覺得多元可以的。接下來的議題會是，金融業是否可以拿個資來做身分識別或當作信用資料的提供，我也覺得某程度上是可以接受的，因為這等於是增加了人民的可能性，但如果要提供給像銀行等其他 fintech 業者的話，就比較敏感，銀行有受到金管會的高度監管，比較沒有問題；但如果 fintech 業者能拿到聯徵的資料，他背後又是中資

本報告之智慧財產權屬於國家通訊傳播委員會

議題三；身分識別	15：45 至 16：15
	或等等的情形時，就會有比較大的風險。
中華民國消費者文教基金會 蘇錦霞律師	1. 有關於身分識別的部分，從消費者的角度來看，運用前需要要了解哪些事情是很重要的，像是識別身分的機制是合一的，就是說只要一張卡就可以辨識所有東西，但越便利的東西風險就越高，這部分要跟消費者說清楚。目前的 TWID 是政府機關提供，讓消費者可以申請政府機關的任何服務，這就可以讓消費者了解要承擔的風險。 2. 第二，消費者想了解的是，運用的過程中能不能自願終止或會不會被非自願性的終止，就像是消費者的身分會不會被盜用，或者說手機會不會不見等問題。 3. 最後就是發生狀況時，依照個資法要請求損害賠償是相當困難的，消基會也在 106 年對某家旅行社的個資外洩提出團體訴訟，也被判敗訴，個資法的舉證責任不像消費者保護法第 7 條有舉證責任倒置的規定，所以在損害賠償的部分個資法無法讓消費者滿意，業者可能會認為是不是個資法部分隨便做做就好。 4. 所以在身分識別上，希望能在前中後的三階段都讓民眾了解，業者做了哪些東西。
台灣人權促進會 周冠汝專員	1. 講到運用門號來做身分識別，今年有蠻多便利的運用，但當民眾去使用這些識別服務時，要考慮留下來的紀錄能不能被民眾查詢，或是會不會被串起來去做更個人化的東西。 2. 另一個想要提的是比較遠程的風險，過去有蠻多國家的服務都需要手機門號進行驗證，我們會比較擔心這樣的服務推出後會造成更多網站想要採取同樣的實名認證，像有一些網購平台要求手機或身分證字號；還有 PTT 以前是用信箱申請帳號，但現在是一個手機門號搭配一個信箱，我們會想要知道說，當有這樣的服務時，其他服務是不是會想要跟進，到時候消費者會不會之前有其他方式可以選擇，但現在只能用手機來進行身分識別？還是說我們只允許某些服務能夠使用手機來進行身分識別？ 3. 現在也有一些設計是在最初設計時就把隱私跟資安考慮進去了，這麼做就可以預防出問題再修補的可

本報告之智慧財產權屬於國家通訊傳播委員會

議題三；身分識別	15：45 至 16：15
	能性，不過這也可能是為什麼我們會坐在這裡的原因，因為我們都不是做產品的人。
金融監督管理委員會 蔡少懷組長	1. 現在 mobile ID 在沙盒裡面有兩個案子，一個是凱基跟中華電信的數位身分認證，主要是信用卡跟貸款；另一個是現在進行中的阿爾發投顧跟永豐金證券合作，讓開戶時可以用手機認證，這兩個都有取得初步成果。當然後續要全面性推廣的話，可能會涉及銀行業自律規範的規定。 2. 其實在處理身分識別上可能的解方有很多，像是我們最近在推的網路身分識別標準（Fast Identity Online, FIDO）是希望透過生物特徵跟行動裝置來取代密碼，傳統上的密碼很容易被猜到跟外洩，但用生物特徵來說相對上比較難取得，這也是我們一直在推動的。 3. 但數位身分認證在使用上還是有各種的層次，像是在什麼領域用到什麼程度，也是我們常常在思考的問題，像是 mobile ID 跟生物特徵也是，實務上不會讓他們用在所有領域，如果要用在更高風險的地方的話，可能要採取更嚴謹的身分識別，我們現階段都是希望先從風險比較低的交易開始推動，新科技的推廣跟運用還有控管，我們跟業者都會去評估跟控管。
東吳大學法律學系 余啟民副教授	1. 身分識別跟身分驗證的根本問題可能要回到電子簽章法，電子簽章法裡面的數位簽章跟憑證是一樣的，但電子簽章沒有要求憑證，所以生物特徵並不等於是數位簽章，但因為我們的修法過程導致有些公務機關會誤會並且最信賴數位簽章，而認為沒有其他電子簽章。 2. 如果我們去觀察電子簽章的定義，可以知道是「指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。」，其實在國外的條文中沒有「資格」這兩個字，數位簽章是用數學演算法，一定長度的數位資料進行私鑰或公鑰的加密去行成電子簽章，但現在實務上的運用都是從第四條跨越第五條。 3. 今天我們有很多生物識別的東西，他可能已經可以用指紋去身分驗證，不過他只用來做低等級的身分

本報告之智慧財產權屬於國家通訊傳播委員會

議題三；身分識別	15：45 至 16：15
	識別而已，這點可能是因為電子簽章法的迷思。
輔仁大學法律學系 張陳弘助理教授	1. TWID 身分識別談的是消費者要使用這個功能去證明是本人並申請服務，這個是被動識別，但如果當事人沒有要申請服務，但電信業者拿資料去辨識這個人，這就是主動識別，我想搞清楚 TWID 是哪一類別。 2. 譬如說我的臉部驗證，我的手機製造商，也就是蘋果公司可以收到我的資料，但電信業者有辦法蒐集嗎？因為這些都是生物特徵資料，在歐盟 GDPR 上使用生物特徵資料需要符合特別的規則。
中華電信大數據處 闕仁斌總監	1. 愛沙尼亞的行動 EID（Mobile ID）需要特殊的晶片，因為他要存很多個資在裡面，像是生物特徵或其他相關的東西，但是 EID 跟 TWID 兩個強度不一樣，EID 能代表身分證，但我們手機的認證只能證明這個瞬間你拿著這支手機在使用，所以我們才會說他是雙因子的輔助認證，無論是打疫苗還是繳稅，主要認證還是在於健保卡號。 2. 如果要把生物特徵放進去，其實銀行走得比較快，電信事業也很希望能利用生物特徵，但法規上很難突破，但如果偏遠地區能夠利用生物特徵來辨識，會有很大的突破。 3. 至於要以甚麼資訊來認證，業者會去衡量風險，就像是為什麼以前用信箱認證，現在要用手機號碼認證，因為他們會擔心有風險，所以我覺得這個部分是雙方同意就好，因為商業上業者會想要用身分驗證來確保使用者的身分。 4. 而電信業者不會給手機製造商任何資訊，只會幫他確認說這個手機現在被使用者所使用。
財團法人資訊工業 策進會 宋佩珊主任	其實大家最擔心的就是安全性的問題，像是傳輸的過程，透明度的問題等等，這也是未來在應用上的重要問題。

本報告之智慧財產權屬於國家通訊傳播委員會

議題四：金融科技	16：25 至 16：55
財團法人資訊工業策進會 宋佩珊主任	在美國法上面，金融的隱私保護相對我國是比較寬鬆的，像是機構內的資料流動都比較開放，像這樣的交互運用要不要比較寬廣開放，也是一個需要討論的問題。
金融監督管理委員會 蔡少懷組長	1. 對於金融的創新實驗或者金融監理來說，我們比較重視的概念是個資法，也就是資料擁有權，客戶有權力自由利用其擁有之個人資料，就像是繳交電話費的紀錄會成立一個的信用報告，但提供這樣的資料給銀行，是不是會發生銀行的信用等級降低，這其實是有可能的。至於要怎麼保障客戶的安全，也就是要回到資料擁有權的概念，重點在於當事人有權利自行決定是否要提供電信信用報告予銀行，而銀行不能基於當事人沒有提供資料就僅以此理由拒絕核撥貸款，所以就算客戶在電信費的繳交沒有那麼規律，只要客戶不提供相關資料給銀行，也不會影響到銀行的服務。 2. 再來就是資安疑慮部分，最主要的問題是分享的對象是誰，如果是金融機構的話比較沒問題，畢竟他們算是高度監理。 3. 最後是行銷部分，在授信往來的契約書上就已經把行銷列為個資的使用目的了，如何使銀行的行銷對客戶真的有幫助，再來就要考慮如何符合客戶的需求，並且要怎麼讓客戶很方便的拒絕行銷，都是解決問題的可能方法。
中華電信大數據處 闕仁斌總監	1. 剛好這是中華電信推出的服務，先前柯經理有提到，業界在設計新服務時，會考慮這是不是客戶需要的服務，所以會先知道客戶有需要這個服務的動機，不然客戶不會願意讓他的個資被跨領域使用。 2. 對有些沒有信用資料的人來說，他們會需要信用資料，其實電信繳費的資料就可以代表個人，我們就可以透過電信公司用在電信服務的資料，去爭取跨業的貸款服務，這已經算是進展到個資可攜性的應用。 3. 所以我們光是在法務的設計上都花了很多時間，而資料的保護層面，其實在銀行跟電信業都是高度重視個資的地方，我們會鎖 IP，且交易過程都會有 Token 驗證，所以資安對我們來說只是要不要花錢的議題，不過要做好資安確實需要資金去堆疊。

本報告之智慧財產權屬於國家通訊傳播委員會

議題四：金融科技	16：25 至 16：55
台灣走著瞧股份有限公司 柯志強商務經理	1. 這個議題其實是快樂的議題，因為讓金融小白可以多一個選擇，讓他有機會能夠借到錢，但是後面要怎麼確保在資安上可以達到水準，這是很好的問題，我也希望能更全面性的發展。 2. 至於要怎麼更全面的發展，整體來說我們要去鼓勵業者創新，不要因為不會賺錢就被董事會擋下來，因為我們可能藉由這些嘗試而扶植台灣的獨角獸。 3. 最後，我覺得電信業跟金融業是受高度管制的產業，換句話說，他們也是被保護的產業，既然受到保護就要有配合的義務。像我們之前跟銀行合作 open API 的案件，成案了之後我們想要複製這個模式到其他銀行，但其他銀行會跟我們說他們根本不想配合，這就會讓我們窒礙難行，因為我們努力很久的案件就只能在一間銀行落地。但其實我們要的資料根本不是銀行的，他們只是基於自己的立場不配合，這其實是我們希望能立法改進的。
財團法人資訊工業策進會 宋佩珊主任	定期繳款的服務是不是都會當作信用紀錄，會不會對信用制度產生什麼影響？
遠傳電信 江奎徵律師	1. 遠傳電信在做行銷的用途上，都是電信服務內的行銷，比方說資費的促銷方案，其實在行銷用途對電信業者是有限縮，不是什麼東西都可以拿來行銷。 2. （回應身分識別議題）遠傳電信目前針對身分識別的部分，有採用蒐集聲紋的方式，以聲紋的比對來做為客服核資的一種方式，比方說，你的親友可能很熟悉你的基本資料，甚至你的繳費狀況，所以如果只是透過幾個靜態個資、動態個資的問題詢答，就很有可能通過客服的核對資料，而進一步冒名。因此，我們嘗試以聲紋做為核資的一種方式，以確保是客戶本人進線客服。而且我們蒐集的方式，是個別並且很明確的告知客戶我們蒐集聲紋的目的（核資），並取得他們的同意；有使用語音宣告，告知其權利，過程也有錄音。聲紋資料蒐集後，如同所有的客戶個人資料，我們就放在遠傳電信的專屬的伺服器，而且沒有連結到雲端。 3. 以電信業者來說，要服膺資通安全管理法，作為關鍵基礎設施提供者，我們都要向主管機關提資安維

本報告之智慧財產權屬於國家通訊傳播委員會

議題四：金融科技	16：25 至 16：55
	護計畫，所以說在資安部分是能夠讓用戶放心的。
輔仁大學法律學系 張陳弘助理教授	我不太相信繳款紀錄能夠驗證信用，因為都是小額的錢，所以中華電信有搜集其他的電信資料嗎？譬如說會不會看手機綁定了幾張信用卡？手機有哪些要收費的 APP？而你們在告知上是用哪樣的告知方式，是用概括性的還是在驗證信用資料時上利用客戶個資？
中華電信大數據處 闕仁斌總監	1. 中華電信不會去看客戶的個資，也不會去看客戶的簡訊。而哪些資料會讓銀行認定要不要放款，他們會需要繳費資料，還有這些繳費的金額，像是凱基提供的申請書，是用正向表列的方式，你如果同意中華電信提供這些資料來申請貸款，就打勾，我們不會冒險去做這個創新。 2. 不只是消費金融，我們企業金融也在做，我們就有和中華徵信合作，因為銀行最怕貸款給空殼公司，跟我們合作以後，銀行可以去判斷這間公司有沒有裝市內電話，或是裝多久，其實多一個資訊就對銀行來說幫助很大了。 3. 對銀行來說一定會希望把所有資料給他，但國家通訊傳播委員會 NCC 說不能這樣，所以我們不會全部給。
金融監督管理委員會 蔡少懷組長	凱基銀行實驗案之電信信用報告使用授權書所調取的信用報告內容含有個資、往來紀錄、信用資料等等。但如同總監所說，不會有涉及訊息的內容，也就是中華電信提供的僅有客戶跟中華電信往來的交易資料。
台灣人權促進會 周冠汝專員	這個交易紀錄會包含用電信費扣款的 APP 交易紀錄嗎？
中華電信大數據處 闕仁斌總監	那一次的創新是，經過認證後，中華電信會把你的通訊地址跟手機號碼提供給銀行，因為銀行開戶會需要填這些，開戶流程可以從好幾分鐘變成三十秒，所以沒有提供任何交易資料，因為銀行認為客戶跟電信公司申請服務就算交易了。
中華民國消費者文教基金會 蘇錦霞律師	所以繳費資料包含月租費、專案費、小額付款也有嗎？
中華電信大數據處 闕仁斌總監	中華電信不會提供帳單內容，我們只會提供有沒有準時繳費的紀錄。
金融監督管理委員	1. 第一，銀行決定是否放款並不是只依據中華電信給

本報告之智慧財產權屬於國家通訊傳播委員會

議題四：金融科技	16：25 至 16：55
會 蔡少懷組長	的資料，所以銀行只是額外取得中華電信的資料，其他徵授信的資料也要有，中華電信的資料只是補充的作用而非取代。 2. （回應身分識別議題）第二，有關生物辨識的部分，Fido 在設計的時候就有考慮到生物特徵資料之敏感性，因此 Fido 不會把生物識別的資訊傳出去，只會存在設備裡面。 3. 最後就是開放銀行的狀況，英國有 GDPR 的資料可攜權，但我們沒有，所以銀行不配合也沒辦法，這部分我們會努力推動銀行去多多參與開放銀行。
台灣人權促進會 周冠汝專員	1. 當初看到簡報的時候有想到中國芝麻信用，芝麻信用也是站在當事人同意的基礎，只是他要的東西更多，我覺得讓消費者知道我們跟芝麻信用這樣極端的案例不同，其實是很重要的。 2. 前面聽到遠傳電信的行銷只限縮在電信資費裡面的部分，但我曾經在社群平台揭露的資料中看過電信業者、銀行業者上傳我的資料，讓我疑惑行銷的範圍？ 3. 這個部分可能是行銷應用上講求精準行銷，所以很多可能是使用者在不知道的時候被第三方業者轉手取得，不知道有什麼方法能夠處理這種情形？
財團法人資訊工業策進會 宋佩珊主任	我覺得科技能處理這種問題，像是用區塊鏈的不可篡改性來去降低這樣問題的風險。
世新大學法律學系 翁逸泓主任	1. 個資法遠遠落後於現在這個數位時代該有的規範，還有其他落後的是個資法僅僅是做為骨架的基本法，在特別的領域應該要有特別的個資規範，像是歐盟那邊也有相對可能具有域外效力的法規草案，就是通傳領域的 ePrivacy Regulation (proposal)，以後他們變成這種情形時我們就應該要想該如何因應，希望大家能記取教訓提早準備，不要像是 GDPR 的適足性認定一樣如此倉促。 2. NCC 這邊本來有一個數位發展法，但我們現在有數位發展部，所以可能會改成其他規範，最重要的是到時候要把個資保護的主管機關劃分為給數位發展部，或是由一個專責機關負責，讓他能明確化。 3. 再來就是資料可攜權的問題，因為我們沒有這種權

本報告之智慧財產權屬於國家通訊傳播委員會

議題四：金融科技	16：25 至 16：55
	利，銀行也有自己的考量，金管會是高度監管，所以銀行會願意拿出來，而 NCC 也是高度監管，不知道會不會讓電信公司願意把這些東西給新創公司。
達文西法律事務所 葉奇鑫律師	其實溝通很重要，但是溝通很難，要跟一般的消費者溝通其實是更困難的，再來就是個資法本身有一條很遠的路要走，也就是需要單一獨立的主管機關。從世界各國的經驗來看，只要成立後他都會罰得很重，而且他也具有足夠的專業性。

本報告之智慧財產權屬於國家通訊傳播委員會

附錄4：110 年 8 月 4 日座談會（二）會議紀錄

110 年度電信事業運用數據資料提供創新應用服務治理模式

座談會（二）

一、 時間：110 年 8 月 4 日下午 14:00 至 17:00

二、 地點：財團法人資訊工業策進會科技法律研究所行遠講堂

三、 與會人員：詳參簽到表

四、 會議記錄：

議題一： 電信事業加值利用之障礙	14：20 至 14：50
台灣大哥大 與會代表人	1. 我們很認同簡報所提出的案例，但提到對政府的小建議，當看到了口罩實名制後，我會想到報關進貨物或繳稅等服務，希望政府都可以讓民眾進行一次性的身分驗證，讓每一次使用時可以更簡便的進行認證，可能會比較現在好一些。 2. 如果是其他的類別，我們希望能有更多元的發展，在這方面的應用只要在安全且沒有疑慮、且知道自身個資會被用在何處的情形下，我覺得是沒什麼問題的。
亞太電信 與會代表人	1. 對於我們電信事業而言，傳統的電信服務對大家而言只是日常，已經不再具有價值，而在進入 5G 後，會發很多物聯網跟加值利用的服務，這反而是由電信業來主導這件事。 2. 這時會面對很多問題，第一個部分，電信事業每次想到新的加值服務時，都會遇到一個問題，就是我們要怎麼徵求客戶的同意，有很多加值服務都因為這個關卡而胎死腹中。 3. 第二，電信業者擁有的個資會產生問題，也就是業者能將這些個資運用到什麼程度？這部分的規範比較沒那麼具體，我們會希望有規範能夠清楚規定業

本報告之智慧財產權屬於國家通訊傳播委員會

議題一： 電信事業加值利用之障礙	14：20 至 14：50
	者可以針對什麼目的運用到什麼程度。
達文西法律事務所 葉奇鑫律師	上一場中華電信也有表示取得消費者同意的成本是很高的，而電信業者取得消費者同意最重要的關卡就是申辦門號的時候，也就是臨櫃辦理時，這時候蒐集個資會需要有各別的同意，像中華電信之前只有一成民眾會在辦理時另外勾選同意，另外的九成沒勾選後來發現很多時候是因為門市員工告知民眾可以不用勾選。
域動行銷 與會代表人	1. 市場上電信數據使用在廣告投放上，以中華電信跟台灣大哥大較為成熟。先不論電信業如何以數據做加值服務，國外業者 Google、臉書等都以我國民眾的數據來做廣告加值服務，為什麼政府沒有完善個資保護法令、統一的數據運用標準規則？在同一個市場中，部分廠商可使用數據加值運用，部分廠商卻不被允許？ 2. 所以我想問的是，在數據加值服務上，企業當然應該要顧及消費者感受跟做好資安保護，但相關法令是否能有明確規範？這幾年執行數據服務的業務下來，許多新型態的服務，感受政府只規範本土企業，我們會覺得為什麼其他國家可以做？但我們不能做？ 3. 針對問卷部分，難道 1 千多位填答者，都很清楚個資跟資安規則嗎？相信很多人都沒辦法理解資安保護了哪些事情。這也是為何，我國許多數位行銷業者，有時候除了我國的法令規定以外，也只能去參考 Google(國外民間企業)的資安規定。 4. 至於希望政府幫忙的地方，就是能有清楚規範，不是像現在我們遇到問題一直去請教政府說明。例如我們看到國外有做的事情(新服務)，我們去問政府我們能否這樣做，來回多次，也無法說清楚，這就是在快速變化數位時代，我國業者都只能在後方苦苦追趕的原因。
達文西法律事務所 葉奇鑫律師	執行長有講清楚業者的心聲，但這也不是我國才有這個問題，Google 跟臉書等都常常在其他國家被處罰。
政治大學法學院 劉定基副教授	1. 在問卷上有條件支持跟完全支持的比例是蠻高的，所以問題的關鍵應該是說在什麼情形下是可以去利

本報告之智慧財產權屬於國家通訊傳播委員會

議題一： 電信事業加值利用之障礙	14：20 至 14：50
	用電信資料，看了問卷後我整理了兩個方向： 2. 擔心的人主要擔心的是兩件事情，一件是目的外利用，第二件則是這些填答者對業者沒有太大的信心，或是對監理的能量沒有太大的信心，所以他們才會希望要保證將來屆期能刪除或說明如何做好資安措施。 3. 所以要解決加值利用的問題可能兩方面都要處理，首先要先提升民眾對業者的信心，我覺得不需要質疑民眾對法律跟資安認知的程度，因為這個要求有點高，而對大部分人民而言，這是感覺跟信賴的問題，而不是法律或技術的問題。所以要怎麼利用告知或措施讓民眾相信，這部分是比較重要的，當然監理部分要怎麼加強也很重要，而加強不一定是處罰，而是行政機關可以給出更清楚的指示，讓業者能做出清楚的判斷。 4. 就同意的部分，我覺得同意是比較麻煩的事情，但其實同意這件事情在個資法上是有些彈性的，像是我跟葉律師討論過這個問題，葉律師以前是採取比較嚴格的見解。但如果我們有共識認為線上取得數位化同意不用採取那麼高的標準，這時候電信業者在取得同意上是比較具有優勢的，因為電信業者有當事人即時聯絡的方式，可能是電話號碼或電子郵件，而除了首次接觸以外，每個月還有定期聯繫的機會，從這幾個面向來看，我會傾向電信業者能更具體的描述這個難題，譬如說客戶多所以成本高這類型的，這樣在法律的修正或是法律的誤解上能更清楚的釐清。
東海大學法律學系 范姜真媺教授	1. 看到問卷結果的感想是其實在日本也一樣，人民對電信業者信賴度的問題是非常重要的，因為如果民眾不信任，可能會給出假的資料，反而會造成資料運用上不正確之結果。所以我也覺得信賴度很重要，信賴度的建立其中一項就是透明化，對於業者如何取得資料？取得哪些？利用目的為何？提供給了誰？對民眾有什麼風險？這些都是經透明化過程非常重要須實現的，資訊生命週期之軌跡也同樣必須

本報告之智慧財產權屬於國家通訊傳播委員會

議題一： 電信事業加值利用之障礙	14：20 至 14：50
	有完整之紀錄，而透明化的這塊我們可能沒做的那麼好。 2. 在日本，即使是匿名化以後的資料，只要你有提供給他人，都必須留下紀錄，而且要讓當事人隨時可以查詢，所以我自己的感想是，我國在透明化這塊比較沒有落實，因為民眾對此常常一無所知，這部分是我覺得可以加強的。 3. 再來就是資安的部分，我覺得隱私影響評估屬於資安之一部份，在建立系統獲取資料，到底有沒有先做影響評估，有沒有確認可能發生的風險？可能採取之的補救措施為何？在歐盟的規定中是一定要做的，但我們個資法之規定中沒有明確此部分之義務。評估之實行及結果必須公告對民眾說明，這也是一種建立信賴度的方式。 4. 我也會懷疑我的個資被拿到哪裡用，到底簡訊實聯制的資料 28 天後有沒有銷毀，銷毀方法為何，是誰在監督，有落實建議在官網公開。
東海大學法律學系 范姜真媺教授	1. 其實我們很多個資蒐集是跨行業的蒐集跟利用，我會覺得可不可以跟有關的主管機關確認關於跨行業個資蒐集利用的規範要怎麼做，發現政府機關都各做各的，像金管會對主管之金融機關控管就是最嚴格的；再參考日本的做法，他們是先確立整體政府政策，然後所有相關的政府機關必須一起研議討論具體之方向討論，再由各主管機關定出各自之指導原則，這我國嘗試各主管機關各自解釋法令、各自為政欠缺整體性之政策方向及機關間之橫向聯繫，所以跨領域之業者常會無所適從，甚至不知主管機關為何。 2. 而其實國外業者也很常被處罰，像是 Amazon 被歐盟罰，臉書也常常被罰，所以國外業者的做法也不是真的都是對的，更未必不受管制。 3. 再來同意的部分，目的外利用的部分性質上是簽訂另一個蒐集處理利用的契約，這部分日本，在現在資料銀行（Databank）進行實驗運行過程中，當事人同意都是在線上同意蒐集，他們詳列提供給第三人

本報告之智慧財產權屬於國家通訊傳播委員會

議題一： 電信事業加值利用之障礙	14：20 至 14：50
	之名單、條件及回饋內容當事人選擇，資料銀行非常清楚告知當事人，讓當事人下載 APP 後即可在手機或電腦上操作同意，亦可撤回同意。這個試運行結果還沒出來，現在先提供給大家做參考。
達文西法律事務所 葉奇鑫律師	像是歐盟有對透明性這點寫出了指引，但我們還沒有，所以國發會委員都希望能先有一個獨立的主管機關，有獨立主管機關就可以進行管理，行政院也有說這是他們的目標，但業者也不一定會喜歡，因為獨立主管機關的標準可能會更嚴格，不過相對的也會非常清楚。
開放文化基金會 李柏鋒董事長	1. 我完全認同要解決同意的問題，我也覺得需要獨立的主管機關，因為跨部會的事情就需要有統一的管理，像是拿健保卡買口罩是經濟部還是哪個單位要管？ 2. 至於獨立主管機關是否會更嚴格，我覺得倒是還好，因為委員會的組成一定有業界代表跟人權團體，像台權會就會關注健保資料庫的加值利用問題，這部分健保局就也一直在躲避這個問題，直接提供給學術界研究，但這一定是違反 GDPR 的規定，我們也反映過很多次，提過異議跟訴訟，也提出釋憲了。結果現在健保署署長說，為了回應大家，會在健保的 APP 中增設供民眾同意，這表示健保署也有遇到問題，我猜想可能是做研究時遇到其他國家民眾拒絕我國健保署利用他們個資進行研究，之後才有改進。 3. 所以知情同意是很基本的事情，我也認為有點麻煩，但還是必須要做，而我也同意學者說的，電信業者在諮詢同意上是相對容易的。 4. 單一主管機關會比較好，這樣才能畫出清楚的界線，當然我們也不是要阻止運用，舉個例子，其實很多民眾想拿到自己的健保資料，所以健保局就轉了方向作出健康護照，舉這個例子是想表示我們也是有鼓勵利用，只是是不同的方向，像是先尊重每個人，讓每個人能很清楚的得到自己的資料，之後就會對業者有比較好的信任。
達文西法律事務所 葉奇鑫律師	民間團體對於個資的要求跟監督，我們也認為是很必要的建議。

本報告之智慧財產權屬於國家通訊傳播委員會

議題一： 電信事業加值利用之障礙	14：20 至 14：50
中華電信股份有限公司法律事務處 陳人傑主任 （書面意見）	1. 電信業者對於電信資料的使用，會先區分是否為個人資料及非個人資料，對於個人資料則依據個資法的規定處理，如對於用戶的行銷需事先取得用戶的同意才能進行，但與客戶權益通知事項有時候會不易區分，使部分較為敏感的用戶有認為電信業者是在進行行銷行為，這部分較容易引起爭議。 2. 由於目前用戶的個資保護意識高漲，所以要進行精準行銷的難度很高，通常都會以提供優惠折扣等方式吸引用戶申辦新的加值應用服務。若通傳會能在相關法規上同意給予第一次行銷的 Opt-out 機制(個資法第 20 條第 2 項參照)，或許可以有效改善目前此一情形。
台灣之星電信股份有限公司 李梅芬副理 （書面意見）	目前因法規並未明確規劃可運用的程度及範圍，這塊對電信業者算是模糊地帶，在創新加值應用上會顯得綁手綁腳，因此我們會很希望有個監理主管機關針對這部分有更詳細的解釋，並且也能站在電信業者商業模式的立場來思考如何監管比較妥當，也許是某些程度上的開放使用，而非全面禁止，這樣也可以避免扼殺創新加值應用。

議題二：公共利益	15：00 至 15：30
達文西法律事務所 葉奇鑫律師	1. 確實目前法規有很多檢討的空間，檢警爭議我們是做為特例帶出目的外利用的議題，原本衛福部保證簡訊實聯制的資料不能被目的外利用，但檢方那邊的意見可能是：在犯罪偵查時本來就可以調資料，為什麼行政機關可以阻礙我們的犯罪偵查呢？衛福部沒有權利去禁止行政機關調取這個資料。像是英國就用全部匿名化的方式去處理這個問題，但缺點就是沒辦法把資料拿來作疫調。
東海大學法律學系 范姜真媺教授	1. 其實公共利益是典型的不確定法律概念，當然 GDPR 裡也有公共利益的要件，但是必須描述是什麼具體的公共利益，例如國民健康、國防等等，所以業者必須要告訴民眾是為了什麼的公共利益，我們才能判斷是否符合比例原則。 2. 日本也有公共利益的問題，但他們要求要清楚說明

本報告之智慧財產權屬於國家通訊傳播委員會

議題二：公共利益	15：00 至 15：30
	公共利益是什麼，才能判斷比例原則，所以我看到公共利益時有想到，不用去定義什麼是公共利益，因為這個問題基本上是無解的，但當我們進行公共利益判斷時流程是很重要的，要先說清楚公共利益是什麼，再進行比例原則的判斷。所以我不是完全不接受公共利益，但一定要說明具體內容是什麼，然後手段必須是最小侵害的。 3. 針對檢調的爭議，我會覺得這沒辦法說服我，因為你有其他不侵犯人民隱私的手段可以使用，調取簡訊實聯制的資料不是最後的手段。 4. 我也提過，個資一旦洩漏就無法回復原狀，這也是我們要做影響評估的原因，這跟環評很像，希望能防患於未然，所以不要等損害發生後再用賠償的方式處理，這已經來不及了，寧願在前端就控制好。 5. 至於匿名化的部分，英國的 GDPR 在脫歐後應該是沒有改變，所以我不太確定他們的匿名化是做到什麼程度，所以要怎麼確定能去識別化這仍然是個大問題，我們也沒有能明確解決的方法，因為對業者而言他一定會有很原始的資料在他那邊，你不確定他會怎麼去利用。匿名化的部分我們也希望能講清楚，因為現在規定的不夠清楚，不知道是要往假名化還是匿名化發展。 6. 數位落差部分也是很重要的問題，像是現在的實聯制，很多老年人會比較手足無措，這也可能涉及人權問題，這要去特別注意。日本他沒有採簡訊實聯制類型的作法是因為他認為低於全國人口的六成數量下載 APP 是沒用的，所以有效性也是個問題，同時還有侵害隱私權的擔憂。
達文西法律事務所 葉奇鑫律師	上一場台權會有提供資訊，社交安全距離 APP 大概有 400 萬的下載量，我們也知道下載跟還有在用的人是有差距的，所以數量也是比較少。至於這個 APP 有沒有去識別化，就國發會觀察歐盟的指引，覺得是不太可能恢復的，所以社交距離 APP 的部分在個資法上是沒有太大的問題。
政治大學法學院 劉定基副教授	1. 公共利益這點我會支持要再具體化一點，因為不可能什麼東西都用公共利益，防疫是否是公共利益，我可以支持這一點，但就算防疫是公共利益，也是

本報告之智慧財產權屬於國家通訊傳播委員會

議題二：公共利益	15：00 至 15：30
	要考慮特定的措施是否能達到這個公共利益，所以不代表在公共利益的帽子下可以正當化所有措施。 2. 地方衛生機關及中央副指揮官都有承認實聯制沒有太大幫助，只能用來作為輔助的判斷工具，所以如果實聯制沒辦法達到所要保護的公共利益，剩下的問題也就不用談了。 3. 其實簡報中有提到英國 NHS APP，他在推出之前有做非常詳細的個人資料保護影響評估，那時英國的疫情比我國嚴重非常多，英國政府也沒有急著上架，仍然依據法律需求做出影響評估。所以在英國的例子裡面，我們可以知道英國接受公共利益作為理由，也接受新科技，但有沒有經過妥當的評估跟利益權衡是很重要的事情。 4. 至於 NHS APP 事後的同意部分，可以在網路上看到簡單版跟詳細版的說明，所以回到剛剛的檢警爭議，如果你有做很完整的影響評估，或是有很好的設計，你就不會讓人家用通保法調通聯或電信紀錄，這時就不會有問題的。不過這個風險就沒有在簡訊實聯制的設計上事前被評估出來，因為第一個他不是匿名，第二是他被跟電信資料放在一起。 5. 但還是要強調，如果這個做法沒辦法實踐公共利益，後面的問題都不重要了。
達文西法律事務所 葉奇鑫律師	這也是一個問題，大家都覺得這個用途不大，但最初其實大家是用手寫，而掃 QR code 這點，除了比較方便以外，也不會造成個資外洩。
域動行銷 與會代表人	1. 就我個人在使用上，不會去判斷是公共利益?商業行為?而是考量我的需求、防疫保障。個資安全？就交給負責單位去把關。我也同意范姜老師「個資只要洩漏就不可逆」。公共利益很重要，但問題是誰來判斷公共利益？所以不論是公共利益或是商業發展，我希望還是能有一個專責主管機關把這些事情講清楚。 2. 舉個例子，如果把檢警爭議案件當成是商業行為，這一定會被算是個資保護法的「目的外利用」，但這可能保護了也服務了更多的群眾，那算不算是公共利益呢？我覺得任何商業運用上，要用什麼立場來看，只是因為今天的主題是個資，所以我們特別把

本報告之智慧財產權屬於國家通訊傳播委員會

議題二：公共利益	15：00 至 15：30
	個資問題放大檢驗。 3. 對於健保資料庫的使用不會被處罰，葉律師有提到是因為個資法的規定不會處罰行政機關，這就有點像是球員兼裁判，如果健保局是民間企業，他的收入(客戶)都是企業與民眾的繳費。而當真正的企業使用相同方式時，就可能會變成是被處罰的商業行為利用，對於業者會像是啞巴吃黃蓮。 4. 當然范姜老師說的個資洩漏不可逆是非常重要的，所以我們還是希望有專責的主管機關，即使管的比較嚴，但講清楚，對企業來說是相當重要的。
亞太電信 與會代表人	1. 其實亞太電信是依照 NCC 的交辦來快速達成，而我們不能判斷有沒有實踐公共利益，因為公共利益是我們上級主管機關來判斷的。 2. 像是對簡訊實聯制而言，其實電信公司只會得到你的手機號碼發了一封簡訊到 1922，不會得到場所的代碼，而我們公司有成立一個專們的小組去做這件事情，所以並不是每個人都會接觸這件事情。而電信資料到達某個節點時，這些資料就會被濾掉，不會出現在帳單的任何資訊上，這是目前我們公司的做法。所以 NCC 來督導我們刪除的紀錄時，我們就能很清楚地去說明。 3. 回到范姜老師透明化的問題，我也不確定我們這樣的解釋算不算透明化，也就是透明化要到怎樣的程度？
東海大學法律學系 范姜真嫩教授	請問簡訊實聯制的成本由誰負擔？
亞太電信 與會代表人	一開始的時候我們依電信公司的用戶數，每個電信公司認捐幾則簡訊，再由政府編列預算。
台灣大哥大 與會代表人	其實相對應的做法每家電信業者差異不大，電信公司都是配合 NCC，目前為止我們一定都是盡量配合。
達文西法律事務所 葉奇鑫律師	其實對於 CDC 而言，五大電信業者也不太會理會 CDC 的指令，所以任務編組上才會由 NCC 來負責這塊。
中華電信股份有限公司法律事務處 陳人傑主任 （書面意見）	1. 目前 NCC 均有不定期查核各行動業者在簡訊實聯制的資料安全及刪除機制。電信業者並定期回報執行情形，建議 NCC 應可定期公布目前執行情形以化解民眾疑慮。 2. 另據了解法務部將行文各行動電信業者在檢警要調

本報告之智慧財產權屬於國家通訊傳播委員會

議題二：公共利益	15：00 至 15：30
	閱 1922 簡訊時，得不予提供。然而電信業者在配合政府進行通訊監察工作上，係由法務部所屬機關設置相關通訊監察設備及進行特定用戶的監聽或監看簡訊時，電信業者並不知悉所屬機關監看的內容為何，因此要如何配合執行尚須技術評估。電信業者希望能有較為明確的法規範得以遵循。
台灣之星電信股份有限公司 李梅芬副理 （書面意見）	1. 在公共利益上，電信業者絕對是全面配合。 2. 以口罩實名制、簡訊實聯制、行動報稅、健保快易通 APP 支援預約疫苗為例，電信業者都是收到行政機關的要求後在期望時程內完成相關服務開發上線；但對電信業者而言，若收到警調機關來函也必須配合提供相關資訊，這就導致電信業者會很困擾，因為一方面我們必須配合政府政策，但另一方面我們又不能拒絕警調機關來函調查，因為主導權都不是在電信業者身上，所以建議可能在相關公共利益服務需求推出前，主管機關儘可能先設想到後續在資料安全的管理風險會比較好，要不然民眾在不瞭解全貌的狀況下，對於電信業者的疑慮就會更大，之後對基於公共利益的相關服務都會質疑。

議題三：商業應用	15：55 至 16：25
中華黃頁 與會代表人	我比較想要知道的是電信的資料可以如何利用在廣告行銷上，然後如何處理資安的問題？
亞太電信 與會代表人	前述韓國 BigSight 的應用其實有點像是用基地台蒐集位置資訊，有點像 location base 的服務，目前其實國外有在做了，但現在國內好像是不能做的，否則電信業者早就跟著做了，因為這對電信業來說是很好的數據。
達文西法律事務所 葉奇鑫律師	我的理解是，假設我們現在要在樓下開咖啡廳，我們就可以跟電信業者詢問人流的狀況，平均年紀，男女比例等等，所以電信業者提供店家的資料是不含個資的。
亞太電信 與會代表人	1. 基本上我們公司沒有在做這樣的事情，但為了公共利益的話我們有接觸，但民間企業來要這些資料時我們不會提供，政府來要我們才會給，所以電信業最大的困境是，電信業有很多資料但這些資料都不能用，所以對我們而言，就只能繼續做電信業。 2. 當然電信業者的資安作為，目前是有資安法，電信管理法對資安也有要求，這一塊電信業都有跟隨國

本報告之智慧財產權屬於國家通訊傳播委員會

議題三：商業應用	15：55 至 16：25
	家的腳步去進行。 3. 至於行銷的部分我們申辦時都會讓客戶去勾選是否願意讓我們進行行銷，針對行銷簡訊的部分，電信業者可能都有固定的處理模式。 4. 最大的困境應該是我們有很多資料卻都不能拿來用。
台灣大哥大 與會代表人	1. 就資安的這塊，假設未來可以做使用的話，我們希望能做到的是像教授提到的盡量透明化，逐步創造客戶的信賴感。 2. 將來如果有機會提供類似服務，回饋是沒問題的，至於要怎麼回饋，這就是可以去設計的。 3. 至於行銷簡訊的部分，現在除了簡訊以外可能還有LINE，還有實體的信件，而實務上要怎麼解決，可能是行銷方式要進步，讓客戶不要覺得被打擾 4. 像是我也常常看到臉書廣告，我也去購買了，但其實我沒有不開心，我反而買到了滿意的商品，所以可能跟廣告內容跟行銷的標的有關，這也是業者要解決的問題。
東海大學法律學系 范姜真媺教授	1. 我很難想像韓國 BigSight 的作用方式，我知道基地台可以分析人流，但我很難想像要怎麼分辨出常住人口等人口的類別，我當初還以為是監視攝影器，因為日本的超市有利用監視攝影器去監測人流，什麼時候的人流最多，跟年齡層等等，這些資料會被數據化，而原始的攝影紀錄就銷毀，不過他們有嚴格的規定，像是不能清楚的紀錄臉孔，只能大概知道性別年齡等等。 2. 我覺得這方面在我國比較難做，因為大法官解釋有說明電信公司蒐集的資料有哪些是不能利用等等。 3. 至於回饋的部分其實很有意思，因為日本的資料信託銀行有提到回饋的議題，這有一定的操作過程，像是當事人會先去告知資料銀行有哪些資料願意被蒐集，再讓廠商來申請，信託銀行也會將廠商跟其蒐集目的都告知當事人，信託銀行會跟廠商訂約，這個約是相當嚴格的，因為如果有問題的話銀行要負連帶責任。至於廠商的回饋主要是提供 coupon，或是促銷活動的折扣或紅利點數，大概就是這樣而已，這些對我而言有多少的吸引力是個問題。這部

本報告之智慧財產權屬於國家通訊傳播委員會

議題三：商業應用	15：55 至 16：25
	分還是在實驗階段，是由民間發起的，政府只是提供指引，還不確定結果會如何，日本的電信公司 NTT 也有一個資料銀行的計劃案，這部分還不確定詳細的內容是什麼。 4. 這就是因為要每個人清楚自己的資料要給誰用是相對困難的，所以委託資料銀行來幫忙管理，所以他會叫做信託，但他一定是架構在當事人同意之上。
域動行銷 與會代表人	1. 針對 BigSight 的商業模式，我舉個例，譬如說 Google map，我們可以看到附近的地點，但他同時也會推薦附近的商家及景點，這是目的內的利用還是目的外的利用？Google map 是地圖，但後面拿 location base 來做廣告媒合或是需求推薦，這樣算不算是目的外利用？ 2. 其實 Google 跟 FB 都不是媒體，只是平台，媒體會對時事發表評論，在平台上，所有使用者(我們)，都變成「自媒體」，所以才能取得我們的資料。 3. 2015 年時為完成數據行銷服務，曾去請教什麼算個資？他說只要能辨別出單一個人就算個資。譬如說某區域內只有一個人拿 Apple 的手機，雖只是要辨識手機型號，這就算是個資。我提到沒有手機號碼辨識，但屬於特定物品的辨識，也算個資。意思是如果這個區域能辨識出單一個人，都算個資。 4. 政府想推廣智慧交通，要做人流的計算，也常要求電信業者提供數據資料，另像跨年時台北市政府跟中央都會跟電信業要人流檢測資料，來做運輸規劃安排。這都是由手機號碼為原始資料去判斷位置推測人流。而原始資料只有手機，統計運用時的資料就轉換為人數&人潮軌跡的資訊而已。 5. 對電信業者來說，會從手機源頭利用手機號碼進行辨識，但不提供號碼，只將一群特定興趣的人，像是幾十萬有相同興趣的人，打包成一整包，接下來就會對這些人進行編碼加密，如要針對這些人投放廣告，還得架設一套系統在電信業者的機房才能運用這數據。 6. 電信數據、發票數據，對於廣告行銷服務上屬於第三方數據，現在趨勢已進步到發展廣告主在電商上的第一方數據運用，也就是將去除個資後的消費者

本報告之智慧財產權屬於國家通訊傳播委員會

議題三：商業應用	15：55 至 16：25
	購買紀錄、登入時間等，與站外的興趣行為，整合到顧客資料管理平台，進行商品推薦的廣告媒合的服務。 7. 第三方的電信數據很重要，但近期第一方數據更重要，雖然量少但是更珍貴，因為他是明確的實際行為，而且能反映當事人的偏好，在服務上可以達到更符合他需求的商品推薦服務。 8. 至於人流系統，不會知道這個人是誰，原始判讀是手機號碼，但轉換為加密編碼，單純判斷的位置，譬如早上出現在信義區，但晚上在蘆洲，系統會初步判斷上班地點在信義區，而居住地點在蘆洲，這也是人潮分析平台在做的事情。這些數據資料可用在更合適的廣告推薦，甚至可以幫忙縮短交通時間，我想這些都是立意良善的。 9. 過去數年「大數據」是大家探討的主題，最近常被討論的是 AI，但 AI 的基礎就是大數據，如果沒有資料導入的話，就沒有 AI 演算。而我們還在針對大數據的資料能否運用探討，相較國際腳步真的慢了許多。
財團法人資訊工業策進會 科技法律研究所 孫鈺婷專案經理	其實到最後這些資料都已經不是個資了吧？
開放文化基金會 李柏鋒董事長	1. 其實有很多資料不能用的情形跟健保資料庫是很像的，因為隨便使用會侵害大家的隱私，而為什麼人數少也有隱私問題，這是最小統計區的概念，譬如說你有罕見疾病，全台灣只有一個人有，你就可以辨識出他，這個最小統計區要怎麼認定，可能要主管機關坐下來談。 2. 我也認同主管機關要對國內外業者都要平等的開罰，我有查詢臉書跟 Google 的隱私設定，其實他們都有符合 GDPR 的規定，譬如說可以刪除自己的資料，這部分我們國內廠商還是做的不夠好，像 Google 就可以很輕易的刪除這些個人資料。 3. 前面有提到行銷簡訊可以關掉，但是其實中華電信有警告我，如果關閉的話可能無法接到國外的兩階段認證，這部分不知道是誰的問題。

本報告之智慧財產權屬於國家通訊傳播委員會

議題三：商業應用	15：55 至 16：25
	4. 至於簡訊實聯制的問題，先講到社交安全距離 APP，如果他是每 15 分鐘更新亂碼，這部分比較沒有個資的問題，社交安全距離 APP 也有公布原始碼，但比較大的缺點是只要是接觸兩分鐘就算接觸了。不過我認為社交距離 APP 是目前我國所有接觸者追蹤(contact tracing)的 APP 裡面最沒有個資疑慮的。 5. 而簡訊實聯制的問題很大，行政院一直強調的是實際聯絡到的機制，所以理論上來說可以只填手機，或是只填 email 也可以，我自己是都填紙本的資料，而雖然紙本有疑慮，我們可以透過填不同資料（手機、家裡電話、郵件）來防止資料被串連，我也遇過小七的店員說這樣不行，但我有跟他說他們是錯的。電信公司雖然只保留商家代碼，但這個代碼其實有分公司的制度，所以假設只要拍一個小七的 QR code 之後，我就知道前面的代碼是什麼，假設資料外洩，就可以確認哪些人要去過小七。 6. 主要的問題是這個資料是明碼的存在各電信公司的資料庫，在德國他們是加密在國家的資料庫中，這部分來說，把簡訊拉出來集中存放其實是技術問題，是資安的問題，不是隱私的問題。如果是隱私問題，不管這個資料存在哪裡，只要交出去了，就會侵害當事人的個人資料自主權，只是因為有其他法律有特別規定，所以不會有違反個資法的情形。 7. 所以我覺得電信事業要跟 Google 一樣抵抗政府機構來要求提供資料，這樣我們才會信任電信公司，像我就比較信任 Google，而不是電信公司，我覺得電信業者可以提出報告，報告哪些單位來調資料最多等等，這樣我們就可以往資料治理的大國邁進。
域動行銷 與會代表人	1. 很多人都很信任 Google，其實他有兩個系統，一個是 Android 一個是 Google 的 map APP，我也承認 Google 在資安上是越做越好的，但誰能保證在 Google Map 關掉使用者的軌跡，Android 就沒蒐集呢？如果把本身手機的定位全都關掉了，手機上有很多的功能會無法使用。 2. 另一個是信任度問題，業者給你選項可將資料刪除，但雲端上是不是真的有被刪除？ 3. 個資的使用或利用的選擇權上，Android、IOS、各種

本報告之智慧財產權屬於國家通訊傳播委員會

議題三：商業應用	15：55 至 16：25
	APP 確實有讓我們自己選擇是否同意提供相關數據，但如果你不勾選同意，會有很多服務無法使用，那這算不算強迫？ 4. Apple 也曾經承認 ios 系統有偷錄 iphone 使用者的所有對話，這算不算是資料竊取濫用？有沒有資安問題？為什麼大家仍然會比較信任 Google 跟 Apple? 這信任度的問題，也就是簡訊實聯制沒有處理好的事項。
開放文化基金會 李柏鋒董事長	1. 我以前就把 Android 系統的定位都關掉了，其實 Google 也犯很多錯，像是之前利用街景車去掃描 Wi-fi 的 ID，這部分也有被歐盟裁罰。 2. 我想要澄清的是，我希望大家一起監督 Google，我只是相對信任 Google 而已，像是我很多法律界的朋友，他們手機是用刷機的，也是不信任 Google 的體現。 3. 所以我覺得要大家一起監督 Google，讓我國網路業者有相對公平的環境。
中華電信法律股份有限公司法律事務處 陳人傑主任 （書面意見）	1. 目前在與第三方合作的電信加值服務上，基於個資法的要求均需事先取得當事人的同意才得進行。 2. 若要進行與位置資訊有關的加值利用，過去通傳會並未允許行動電信業者得以與第三方合作進行位置資訊的行銷，但據了解電信業者都希望能在事先取得當事人同意的前提下能夠提供此一服務。個人建議在法規上得以比照歐盟 2002/58/EC 指令（隱私及電子通訊指令）第 9 條，在告知後取得當事人同意。若經同意提供此一加值服務，得以與參與的店家合作規劃提供回饋機制，以建立三方共贏的商業模式，這部分應該可以考慮。 3. 在上述 2.的機制下，用戶的位置資訊等個資可以不提供予合作的第三方業者，只要第三方業者得以及時提供其行銷資訊予各行動電信業者，對於個資流通的管控部分電信業者應可處理。
台灣之星電信股份有限公司 李梅芬副理 （書面意見）	以各大電信業者與臺灣網路認證股份有限公司合作的 Mobile ID 身分驗證為例，電信公司雖然開放 SP(Service Provider)可以輸入客戶資料來與電信業者客戶資料比對，但這個前提是電信業者不會吐任何額外的客戶資料給 SP，電信業者僅會就客戶資料是否一致來回應身分驗

本報告之智慧財產權屬於國家通訊傳播委員會

議題三：商業應用	15：55 至 16：25
	證是否通過。目前各電信業者其實對個資都非常重視，但因為民眾不瞭解其中運作，可能就會提出他不希望自己的資料被拿來做身分驗證或是利用。

議題四：交通運輸	16：35 至 17：05
內政部統計處 賴威宇專員	1. 我們本身是電信資料的使用者，有一則新聞說台北市的日間人口比夜間多了七十萬人，這怎麼知道的？其實就是用電信資料去做常住人口的推估，剛剛范姜老師有提到政府機關會舉著公共利益的大旗會做這個事情，假設我們能保證不會對個資造成侵害，是不是就可以被接受？ 2. 譬如說內政部以前很多政策都會依據戶籍資料做資源配置，但其實戶籍資料並非完全準確的，所以我們必須要有能反映日間活動的人口數據，才能推行更正確的政策。 3. 所以我們要討論的是如何讓資料進行更好的利用，我們去年跟三大電信業者合作，蒐集使用者白天跟晚上最常出現的地點，還有最小統計區有多少人，這就可以輔助政府做更精準的統計，讓我們可以知道哪些地方聚集太多人？消防栓要擺在哪裡？所以我們宜在確保個資無虞的前提下，做更多的發展應用。
東海大學法律學系 范姜真嫩教授	1. 其實個資法有關於第 16 條 1 項 5 款的規定，統計資料是可以用的，但主要問題是出在個資法沒有盪民間可以利用這些資料。 2. 但其實還有一個重點在於去識別化要怎麼做，這也是個資法的致命傷，始終是不清不楚的地方，如果有政府能講清楚去識別化究竟是什麼，這一切都會變得比較清楚。 3. 其實人數的統計不會有什麼個資問題，但如果說可以勾勒出一個人的生活軌跡時，這個就會是個資了。 4. 至於去識別化在日本的作法，日本在法律上規定在業者去識別化之後提供給利用者時，利用者不能將其再識別，日本是利用法律義務的規定去強制利用者不能回復原狀。
亞太電信 與會代表人	1. 像是交通的應用，以 ETC 為例，在 ETC 剛開始的時候很多人都不裝，原因大概就是隱私問題，後來

本報告之智慧財產權屬於國家通訊傳播委員會

議題四：交通運輸	16：35 至 17：05
	也有其他爭議，像是要不要抓超速，這個時候 ETC 保證不會提供警察機關去偵查交通違規。 2. 電信業者在位置資訊的事情上，我們有目的內的應用，就是計算基地台是否雍塞，因為我們要去算基地台夠不夠，而我們也盡可能不要處理個人的位置資訊。 3. 至於大家都有提到的去識別化問題，其實我們會希望能有第三方公正單位去識別化之後交給電信業者，這樣我們就能夠免除責任，因為可以確認我們無法還原，所以我認為去識別化的工作可以交給公正的單位，對我們來說保障比較大。
域動行銷 與會代表人	在商業運用上很多事情是從交通而來的，因為交通一直需要改善，像是中華電信在桃園捷運這一塊就希望能發展智慧交通，所以這邊的網路線都是中華電信架設的，才會從這邊延伸要怎麼運用的問題。
開放文化基金會 李柏鋒董事長	1. ETC 的問題其實也蠻嚴重的，很多紅綠燈上面有個方形天線，可以掃 ETC tag 的資料，這就是為什麼我們裝 ETC 會被警方查資料，當然美其名是為了交通控管。 2. 至於民眾可不可以去查，有被哪些 ETC 門架或紅綠燈上的方形天線記錄位置，可不可以請求刪掉？我其實也願意付錢去查，這部分搞不好可以進行商業化。 3. 警方如果有疑慮，可以透過立法決定，來討論說哪些人的哪些資料可以儲存多久，像是 GPS 的功能可以關起來，但是 Wi-Fi 也會紀錄位置資訊，所以我們需要第三方來認證，需要獨立主管機關來處理這些問題， 4. 我完全理解 Google 有不公平競爭，但這部分就是要提證據，大家好好討論。
域動行銷 與會代表人	1. 電信業者的市內電話、國際電話、手機電話，越來越少人使用。另外 OTT 都是架在電信業者的網路線路上賺錢，現在若只是網路郵差的收入，不讓電信業者多發展加值服務，是很難生存的。 2. 現在國外網路服務企業，需要付線路費給我國的電信業者，但未來低空衛星架設好後，我國業者還能收到網路線路費用嗎？

本報告之智慧財產權屬於國家通訊傳播委員會

議題四：交通運輸	16：35 至 17：05
	3. 所以我的建議是希望能有明確規範，讓加值應用成長，才能有機會永續發展。
中華電信股份有限公司法律事務處 陳人傑主任 （書面意見）	1. 在有關交通傳輸的應用部分，目前已有電信業者與各地方縣市政府合作進行有關智慧城市及智慧交通運輸的合作，對於相關車流資訊均進行匿名化的處理。在有關路口監視器的部分則由合作的地方縣市政府取得及管理相關錄影資訊，電信業者僅協助提供網路的設置，無掌握相關的資料可為處理。 2. 在旅遊人潮警示部分，行動電信業者只有提供相關景點區域的數量，以供判斷是否有人潮過多的情形，不涉及用戶個資的提供。 3. 若有受政府機關委託蒐集、處理或利用個資的情形，則依據個資法第 4 條規定辦理。電信業者不得對這些個資為其他目的的利用。
台灣之星電信股份有限公司 李梅芬副理 （書面意見）	1. 這跟街道上要不要裝設監視機的議題很類似。回到初衷，如果民眾希望能夠享受到交通運輸應用服務帶來的便利，相對就必須提供自己本身的位置資訊供電信業者或第三方分析，做為交通改善優化的依據，那這可能又是公共利益，但如果願意參與的民眾少，那這個分析也會失準，這都會造成兩難。 2. 所以我們還是建議在任何服務的推出前，要有相關的對策，當然不可能百分百，但至少在有疑慮的部分能夠讓民眾先釐清，避免造成應用服務推出後衍生的爭議，甚至讓本來的目的都失焦。

本報告之智慧財產權屬於國家通訊傳播委員會

附錄5：110 年 10 月 13 日座談會簡報

電信事業運用數據資料提供創新應用服務治理模式研究建議與解決方案座談會

資策會科法所、達文西法律事務所
2021/10/13

stli 科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

資訊工業策進會 Institute for Information Industry

座談會議程



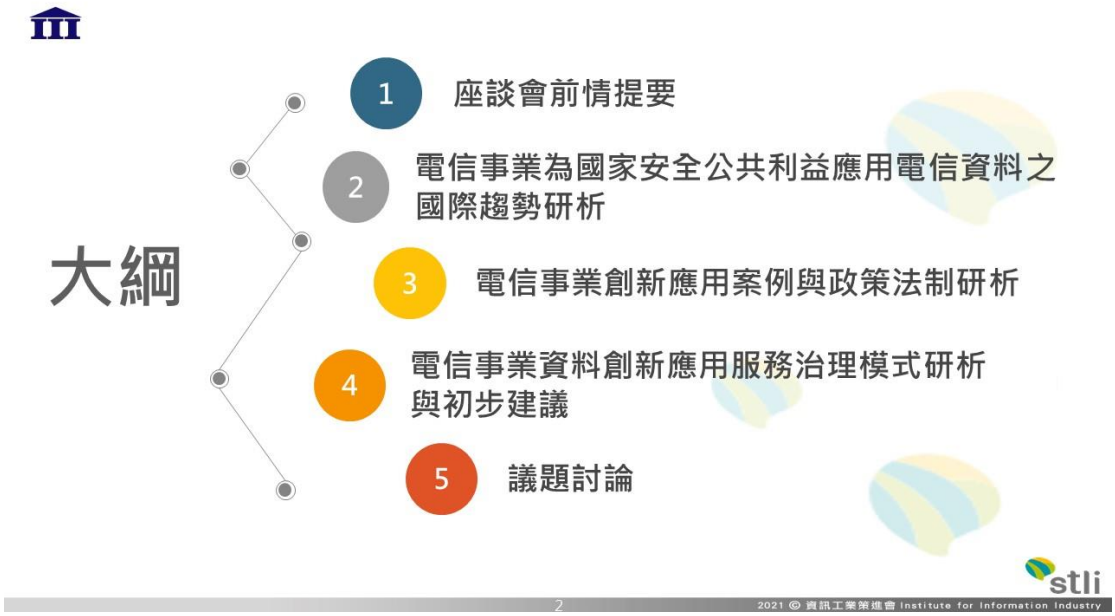
時間：2021年10月13日（三）14:00-17:00
地點：科法所行遠講堂

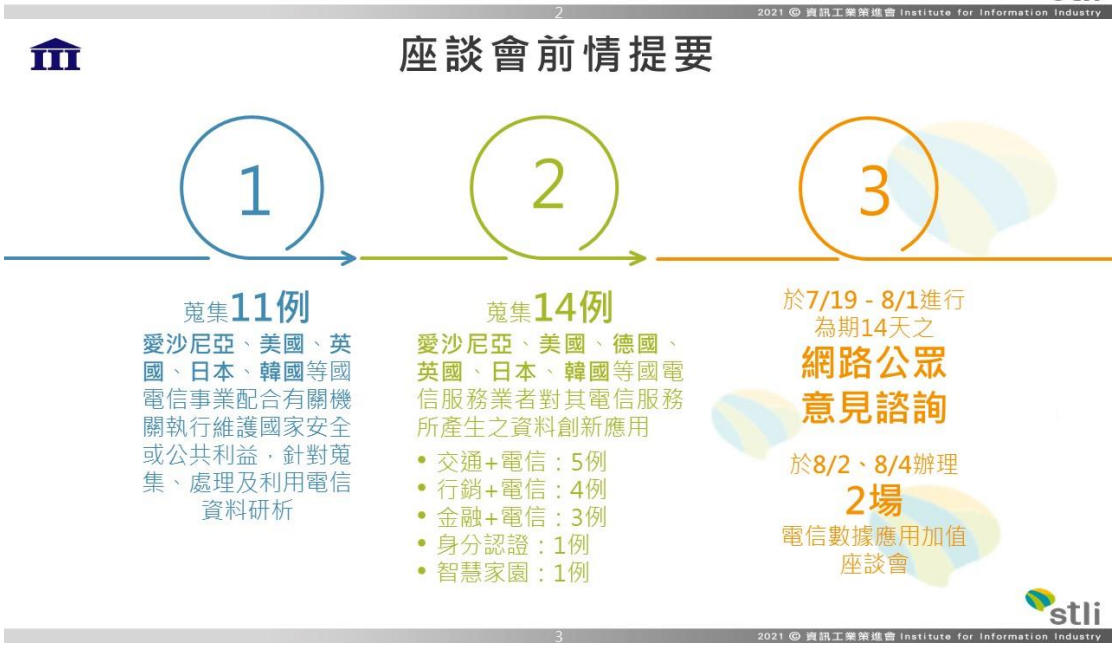
時間	議程內容	主持人/主講人
13：30~14：00	報到	
14：00~14：05	開場致詞	張乃文 副主任 （資策會科法所）
14：05~14：25	引言簡報及議題說明	孫鈺婷 專案經理 （資策會科法所）
14：25~17：00	與會學者專家綜合討論	張乃文 副主任 （資策會科法所） 王慕民 律師 （達文西個資暨高科技法律事務所）
17：00	賦歸	

stli

2021 © 資訊工業策進會 Institute for Information Industry

本報告之智慧財產權屬於國家通訊傳播委員會



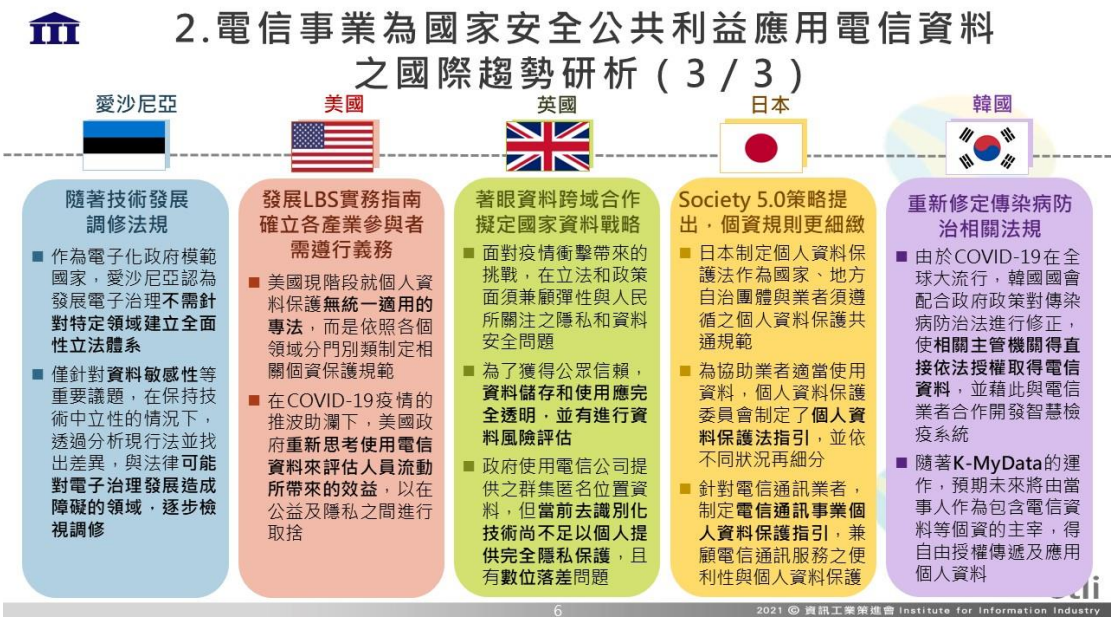


本報告之智慧財產權屬於國家通訊傳播委員會



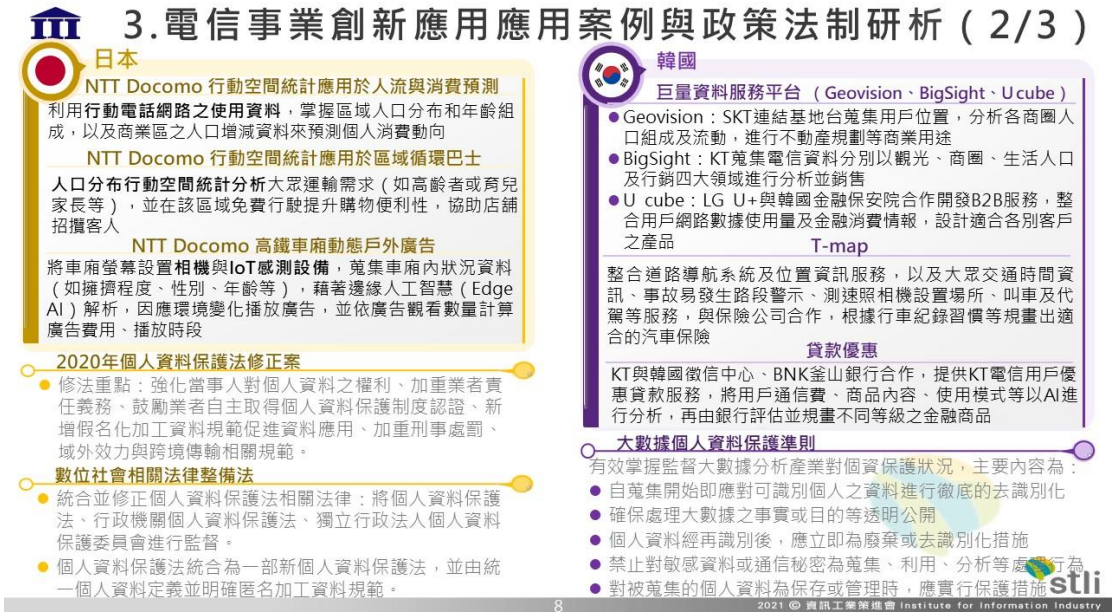


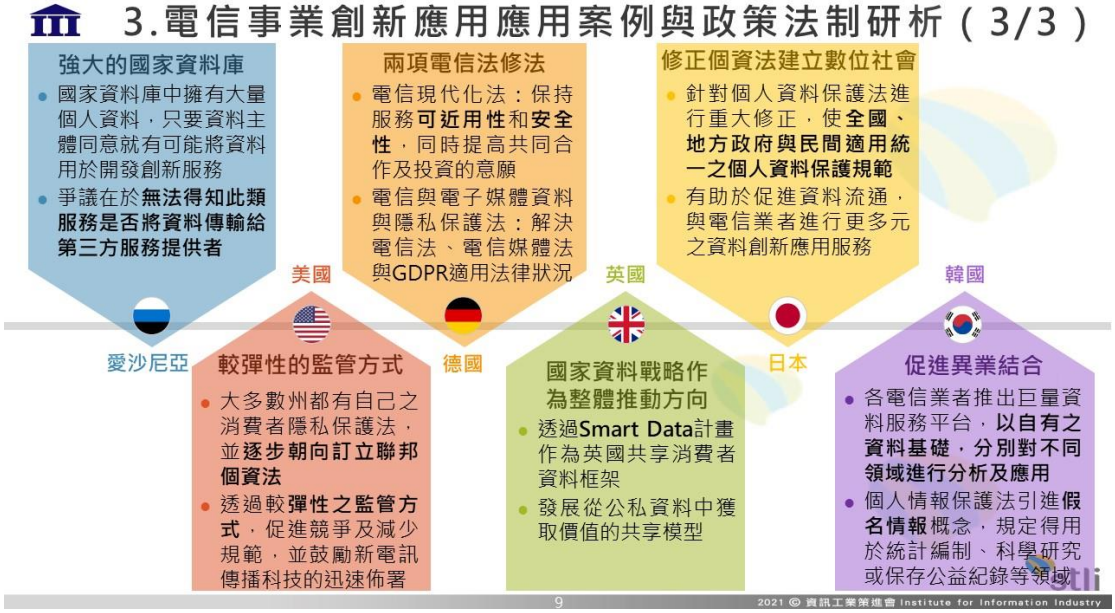
本報告之智慧財產權屬於國家通訊傳播委員會





本報告之智慧財產權屬於國家通訊傳播委員會

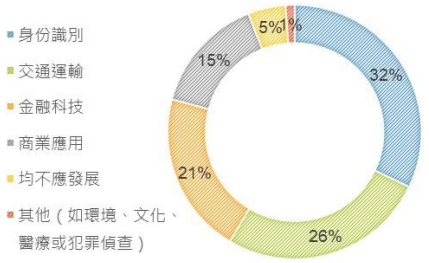




本報告之智慧財產權屬於國家通訊傳播委員會

4.電信事業資料創新應用服務治理模式研析與初步建議（1/2）

電信業者應優先發展創新服務領域



電信業者推動創新服務中，民眾最在意之個資保護議題為：

- 若需要創新利用本人資料，有無事先經過**本人同意**？
- 電信資料是否會**提供第三方**？
- 如何更便利地**行使個人資料相關權利**？
- 資料的**安全**性？
- 有無事先進行**隱私風險評估**？

根據前次座談會之討論，探討目前現行個資法困境：

- 現行個資法規定不足夠，如**去識別化規範不甚清楚**，也**沒有個資保護專責機關**，若電信事業發展加值應用容易產生爭議
- 座談會中眾與會者對個資法應盡速修法共識整理如下：
  - **訂定去識別化標準**：針對資料進行去識別化業者，及接受去識別化資料業者，課以不得再將該資料回復再識別之義務
  - **強化當事人權利行使**：以加州消費者保護法CCPA為例，不要求蒐集者取得當事人同意，而是強化當事人權利，讓當事人權利能更便利行使
  - **設置個資保護專責機關**：加強個資保護之監理能量，尤其在跨行業個資蒐集、處理及利用上能統一規範，以免個別主管機關規範有所歧異而產生爭議
  - **隱私衝擊評估**：事前找出可能發生之風險及可能補救措施外，並建立民眾信賴度
  - **建立透明化之要求**：資料生命週期亦應該公開，讓民眾能瞭解提供出去之個資狀態為何

2021 © 資訊工業策進會 Institute for Information Industry

4.電信事業資料創新應用服務治理模式研析與初步建議：座談會重點摘要（2/2）

議題	討論重點
電信事業加值利用之障礙	業者就當事人**同意及去識別化**之困難及期待
	加值利用之風險
	我國推動加值利用之體制問題
公共利益	**公共利益之目的外利用**透明化
	防疫相關應用之技術及制度設計
身分識別	身分識別應用之**風險**考量
	民眾對身分識別應用之**顧慮**
	管理身分識別應用相關**技術**之制度設計
商業應用	業者**推廣**商業應用之困難
	未來推動商業應用可能之**機制設計**
交通運輸	交通運輸相關資料之**可能用途**
	業者對未來交通運輸應用之**期待**
	交通運輸應用之**制度設計**

2021 © 資訊工業策進會 Institute for Information Industry

本報告之智慧財產權屬於國家通訊傳播委員會

5.議題討論（1/3）

1 基於國家安全與公共利益下，在我國具有推動優勢的電信數據資料類型為何？透過何種機制比較容易推行？

愛沙尼亞	行動定位資料（MPD）即時追蹤行動定位資料，評估各區域風險，並妥適地進行資源規劃
英國	電信行動位置資料分析去識別化、群集資料了解疫情期間人們移動和行為模式
美國	電信法及無線通訊及公共安全法規範電信業者公開用戶位置資訊須經同意、LBS開發布署指南
日本	KDDI人口動態分析支援國家對災害因應、NTT Docomo人口流動統計服務，支援防災與社會產業調查
韓國	修正傳染病防治暨管理相關法律，明文要求電信業者為防止疫情傳染並擴散，應提供使用者位置資訊

歐洲資料治理規則草案（Data Governance Act, DGA）資料利他主義（data altruism）：

- DGA第4章促進個人或公司出於公共利益自願提供資料，資料利他組織需註冊為「歐盟認可的資料利他組織」（data altruism organisation recognised in the Union），增進社會對該等組織營運的信賴
- 為促進基於資料利他主義的資料蒐集，訂定「共通歐洲資料利他同意書」（common European data altruism consent form），降低取得當事人同意成本，促進資料可攜性

2020/8 英國Ofcom Open Communication公開意見徵詢，使消費者能將通訊資料與獲授權第三方簡單安全地共享。規劃共享兩大類資料：

- 範圍包含市話（landline）、固網、行網與付費電視（pay TV services）的獨立和套餐（standalone and bundled）服務
  - **消費者資料（customer data）**：如消費者姓名、地址、資費、服務合約相關資訊、使用經驗等
  - **產品資料（product data）**：產品詳細資訊（合約內容、費用、加值服務）速度、服務品質（覆蓋率、可用性等）以及消費者的總體客戶體驗詳細資料等

2021/7 Ofcom諮詢結果：針對資料類型建議應訂定標準，以確定開放何種資料

- 共享的資料應與客戶決策相關、不同提供者資料應相容（comparable）、業者提供資料前考量提供成本或難度

2021 © 資訊工業策進會 Institute for Information Industry

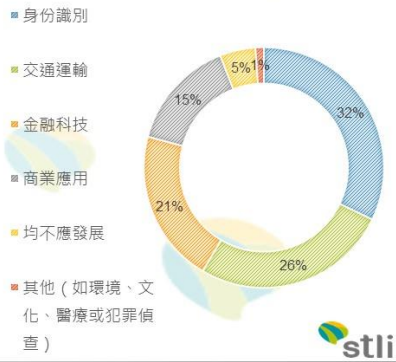
5.議題討論（2/3）

2 在商業資料創新應用領域，具有推動優勢的電信數據資料類型為何？透過何種機制比較容易推行？

- 身分識別、交通、金融（貸款、保險）、零售、旅遊應用、廣告行銷、智慧家庭、人流與消費預測...

國家	應用案例
愛沙尼亞	• 交通應用：Telia M-Praking • 城市規劃、交通、零售、旅遊應用：Telia之人口流動分析（Telia Crowd Insights）
美國	• 廣告行銷：T-Mobile推出個人化廣告推播
德國	• 智慧家庭：德國電信開發智慧家園求救系統
英國	• 身分認證：EE電信公司數位身分平台（Digital Identity platform），防止欺詐並促進客戶交易安全 • 交通應用：EE電信與Atkins於M25公路之電信與交通大數據應用
日本	• 人流與消費預測廣告行銷、大眾運輸：NTT Docomo行動空間統計
韓國	• 商圈人流分析：SKT成立Geovision平台 • 觀光、商圈、人口及行銷：KT設立BigSight平台 • 巨量資料分析：LG U+企業資源規劃系統 • 交通保險服務：SKT電訊T-map整合導航系統及位置資訊服務 • 金融貸款服務：KT與BNK集團合作推出貸款優惠

電信業者應優先發展創新服務領域



2021 © 資訊工業策進會 Institute for Information Industry

本報告之智慧財產權屬於國家通訊傳播委員會

5.議題討論（3/3）

3 業者應用時面臨問題整理如下，是否還有其他問題或風險需要考量，以促進電信數據資料應用？

- 缺乏共享動力
- 對於資料缺乏了解
- 商業、道德和聲譽風險、法律和監管風險
- 資料近用/共享的成本
- 錯失為公共利益應用資料的機會

4 解決方案建議：基於民眾需求推動電信資料應用，政府機關間可行的分責合作模式為何？

短期規劃

建立網路公眾意見諮詢平台

中期規劃

- **規範面：**
  - 指引訂定
    - 強化當事人權利行使（動態同意）、隱私衝擊評估、透明化要求、去識別化標準（CNS29100-2）
  - 定型化契約明文取得當事人同意

長期規劃

- **政策面：**
  - 政府橫向溝通以利決策，借鏡金管會開放銀行、國發會，未來數發部資料治理權責
  - 資料沙盒模式（借鏡英國ICO）、發展電信領域資料中介機制（歐盟資料治理規則草案）、資料銀行...

stli

2021 © 資訊工業策進會 Institute for Information Industry

Thank you

stli

2021 © 資訊工業策進會 Institute for Information Industry

本報告之智慧財產權屬於國家通訊傳播委員會

附錄

- 可能阻礙資料共享問題與資料中介應用對應座談會討論

2021 © 資訊工業策進會 Institute for Information Industry

可能阻礙資料共享議題與資料中介應用對應座談會討論

議題	說明	資料中介的潛在作用	座談會討論對應
缺乏共享動力	資料提供者沒有足夠動力共享或提供資料	付費模式（pay to play），如組織近用資料集的前提是該組織也貢獻資料	• 業者推廣商業應用之困難 • 民眾對身分識別應用之顧慮
對於資料缺乏了解	資料提供者可能對其資料潛在用途缺乏了解，而資料使用者則不了解哪些資料可用與如何用	容易找到特定資料集，使資料提供者能發揮資料價值，資料使用者可以促進潛在應用	• 交通運輸相關資料之可能用途 • 未來推動商業應用可能之機制設計
商業、道德和聲譽風險	失去競爭優勢風險、破壞他人信任的資料使用而遭受聲譽損害，或允許在道德上有問題的資料使用	向資料主體和持有人保證，資料只能由經核准的組織出於特定目的近用	• 加值利用之風險 • 身分識別應用之風險考量
法律和監管風險	違反資料保護、智慧財產權或監管要求或相關風險也可能會阻止共享	提供法律專業知識和共通資料標準，以促進合法資料共享	• 業者就當事人同意及去識別化之困難及期待 • 我國推動加值利用之體制問題
資料共享成本	缺乏資料共享所需的共同基礎建設和技術，且建置成本可能過高	提供資料共享環境，包括應用隱私增強技術等（privacy-enhancing technologies	• 業者對未來交通運輸應用之期待 • 管理身分識別應用相關技術之制度設計 • 交通運輸應用之制度設計
錯失為公共利益應用資料的機會	資料共享可能帶來經濟和社會效益	在受信任的研究環境中對敏感資料安全近用，為公共利益而進行研究	• 公共利益之目的外利用透明化 • 防疫相關應用之技術及制度設計

參考英國資料倫理與創新中心（Centre for Data Ethics and Innovation, CDEI）報告Unlocking the value of data: Exploring the role of data intermediaries (22 July 2021)

2021 © 資訊工業策進會 Institute for Information Industry

本報告之智慧財產權屬於國家通訊傳播委員會

附錄6：日本電信通訊事業個人資料保護指引

（2017 年總務省公告第 152 號）

最終修正 2017 年 9 月 14 日總務省公告第 297 號

第一章　總則

（目的）

第一條　本指引鑒於電信事業的公共性及高度資訊化通訊社會的進展所帶來的個人資料之利用顯著擴大的情形，攸關屬於通訊的秘密事項及其他個人資料正確處理，藉由規定電信事業業者所應該遵守的基本事項，除了謀求提升電信勞務的便利性之外，同時也以保護使用者的權益為目的。

（適用對象）

第二條　本指引的規定，攸關個人資料的正確處理，規定、解釋及運用電信事業業者所應遵守之基本事項的內容。

2　電信事業業者除了遵守保護個人資料之相關法律（以下簡稱「法律」。）的規定及有關秘密通訊的電信事業法（1984 年法律第八十六號）第四條及其他相關規定之外，也必須依照本指引的規定正確處理個人資料。

3　電信事業業者除了遵守第三章所規定之各種資料、第二章所規定之個人資料處理相關共通原則之外，也必須依照第三章的規定正確處理。

（定義）

第三條　在本指引中所使用的用語，除了根據在法律第二條中所使用的用語範例之外，下列各款所揭示之用語的意義，根據該各款規定的內容而定。

一　電信事業業者係指從事電信事業（係指電信事業法第二條第四款規定的電信事業。）的業者。

二　電信勞務係指電信事業法第二條第三款規定的電信勞務。

三　電信服務係指電信事業業者在業務上所提供的電信勞務及伴隨勞務的服務。

四　使用者係指使用電信勞務的用戶。

五　簽約用戶係指與電信事業業者之間簽訂接受提供電信勞務契約的用戶。

第二章　個人資料處理相關共通原則

（具體指定使用目的）

第四條　電信事業業者在處理個人資料的時候，必須盡可能具體指定其使用目的（以下簡稱「使用目的」。）。

本報告之智慧財產權屬於國家通訊傳播委員會

2　電信事業業者在變更使用目的的情形時，必須與變更前的使用目的有相關性且不得超過可被認可的合理範圍。

3　根據第一項之指定的使用目的，必須努力避免超過為了提供電信服務的必要範圍。

（根據使用目的的限制）

第五條　電信事業業者沒有事先取得本人同意，根據前條之規定，超過達成指定使用目的的必要範圍，因此不得處理個人資料。

2　電信事業業者由於整併及其他事由，從其他個人資料處理事業業者以繼承事業的方式連帶取得個人資料的情形時，沒有事先取得本人同意，超過繼承前達成該個人資料之使用目的的必要範圍，因此不得處理該個人資料。

3　前二項的規定關於下列所揭示之情形時，不適用。

一　根據法令的情形時

二　有必要為了保護人的生命、身體或財產的情形，取得本人同意有所困難時。

三　有必要特別為了提升公共衛生或推動兒童健全養育的情形，取得本人同意有所困難時。

四　有必要協助國家機關或地方公共團體或受其委託者執行法令所規定之事務的情形，基於取得本人同意有可能對執行該事務造成阻礙的疑慮時。

4　無關前三項的規定，電信事業業者除了有使用者同意的情形及其他有否定違法理由的情形時之外，不得使用涉及秘密通訊的個人資料。

（取得的限制）

第六條　電信事業業者對於個人資料的取得，必須努力限制於為了提供電信服務所必要的情形時。

（正確取得）

第七條　電信事業業者不得利用謊言及其他非法手段取得個人資料。

2　電信事業業者除了下列所揭示之情形之外，沒有事先取得本人同意，不得取得需特別考量的個人資料。

一　根據法令的情形時

二　有必要為了保護人的生命、身體或財產的情形，取得本人同意有所困難時。

三　有必要特別為了提升公共衛生或推動兒童健全養育的情形，取得本人同意有所困難時。

四　有必要協助國家機關或地方公共團體或受其委託者執行法令所規定

本報告之智慧財產權屬於國家通訊傳播委員會

之事務的情形時，基於取得本人同意有可能對執行該事務造成阻礙的疑慮時。

五　經由本人、國家機關、地方公共團體、法律第七十六條第一項各款所揭示者、外國政府、外國的政府機關、外國的地方公共團體、國際機構或在國外相當於法律第七十六條第一項各款所揭示者公開該需特別考量的個人資料的情形時

六　藉由目視或拍攝本人，取得其外形上明顯的需特別考量的個人資料的情形時

七　於第十五條第十項各款所揭示之情形，接受個人資料之需特別考量的個人資料的提供時。

3　無關前項的規定，電信事業業者除了有使用者之同意的情形時有及其他否定違法理由的情形時之外，不得取得秘密通訊相關之個人資料。

（有關取得時的使用目的之通知等）

第八條　電信事業業者取得個人資料時，除了事先公告其使用目的的情形之外，必須迅速將其使用目的通知本人或公告。

2　無關前項的規定，電信事業業者與本人之間，伴隨著契約的簽訂，取得在契約書及其他文件（包含電磁記錄。以下同。）中所記載之個人資料的情形時及取得本人直接記載於文件之該本人個人資料的情形時，必須事先對本人清楚表明其使用目的。但是有必要為了保護人的生命、身體或財產等緊急情況的情形時，則不在此限。

3　電信事業業者在變更使用目的的情形時，必須針對被變更的使用目的，通知本人或公告。

4　前三項的規定不適用關於下列所揭示的情形時。

一　經由通知本人或公告使用目的，可能會有損及本人或第三方的生命、身體、財產及其他權益之疑慮的情形時

二　經由通知本人或公告使用目的，可能會有損及該電信事業業者的權利或正當利益之疑慮的情形時

三　國家機關或地方公共團體執行法令所規定之事務有必要協助的情形時，經由通知本人或公告使用目的，有可能對執行該事務造成阻礙的疑慮時。

四　從取得狀況來看，被認為使用目的顯而易見的情形時

（確保正確性）

第九條　電信事業業者在達成使用目的的必要範圍內，必須努力保持個人資料正確且最新的內容。

本報告之智慧財產權屬於國家通訊傳播委員會

（保存期間等）

第十條　電信事業業者處理個人資料（秘密通訊相關內容除外。以下於本條中亦同。）時，在使用目的之必要範圍內訂定保存期間，經過該保存期間後或沒有必要再使用之後，必須努力立即消除該個人資料。但是下列所揭示之情形時則不在此限。

一　根據法令的規定，必須保存時。

二　有本人同意時。

三　電信事業業者在執行自己的業務之必要限度內，保存個人資料的情形時，針對沒有消除的該個人資料，具有相對應之理由時。

四　除了前三款所揭示的情形之外，針對沒有消除的該個人資料，具有特別的理由時。

2　電信事業業者除了有使用者同意的情形時及其他具有否定違法理由的情形之外，不得保存秘密通訊相關個人資料，即使是允許保存的情形時，在達成使用目的之後，也必須迅速消除其個人資料。

（安全管理措施）

第十一條　電信事業業者為了防止其處理的個人資料或秘密通訊相關個人資料（以下簡稱「個人資料等」。）洩漏、遺失或毀損及其他個人資料等的安全管理，必須採取必要且適當的措施（以下簡稱「安全管理措施」。）。

（從業人員及受託人的監督）

第十二條　電信事業業者使其從業人員（含派遣員工。以下同。）處理個人資料等的時候，為了謀求該個人資料等的安全管理，必須對該從業人員進行必要且適當的監督。

2　電信事業業者為了實施安全管理措施及其他確保個人資料等的正確處理，對其從業人員，必須努力實施必要的教育訓練。

3　電信事業業者將個人資料等的處理全部或部分委託的情形時，為謀求被委託處理之個人資料等的安全管理，必須對受委託者進行必要且適當的監督。

（保護個人資料管理者）

第十三條　電信事業業者必須努力設置保護個人資料管理者（係指該電信事業業者處理個人資料等的相關負責人。）、制定遵守本指引的內部規章、建置審查體制及該電信事業業者進行處理個人資料等的監督。

（隱私權政策）

第十四條　電信事業業者務必適當公告隱私權政策（係指該電信事業業者在推動保護個人資料方面的想法及方針。）。

本報告之智慧財產權屬於國家通訊傳播委員會

2　電信事業業者提供應用程式軟體（以下簡稱「應用程式」。）的情形時，應該適當公告關於利用該應用程式取得資料等規定明確且適當的隱私權政策。

3　電信事業業者經營提供應用程式網站的情形時，該網站對提供應用程式的業者，應該敦促該業者適當公告關於利用該應用程式取得資料等規定明確且適當的隱私權政策。

（限制向第三方提供）

第十五條　電信事業業者除了下列所揭示的情形之外，沒有事先取得本人同意，不得向第三方提供個人資料。

一　根據法令的情形時

二　有必要為了保護人的生命、身體或財產的情形，取得本人同意有所困難時。

三　有必要特別為了提升公共衛生或推動兒童健全養育的情形，取得本人同意有所困難時。

四　有必要協助國家機關或地方公共團體或受其委託者執行法令所規定之事務的情形時，基於取得本人同意有可能對執行該事務造成阻礙的疑慮時。

2　有關電信事業業者向第三方提供個人資料（需特別考量的個人資料除外。以下於本項中亦同。），因應本人的要求，停止向第三方提供可供辨識本人之個人資料的情形時，針對下列所揭示之事項，事先通知本人，或置於本人可以容易得知的狀態下，同時根據法律第 23 條第 2 項的規定，向保護個人資料委員會申報時，無關前項的規定，可以向第三方提供該個人資料。

一　必須以向第三方提供為使用目的。

二　向第三方提供之個人資料的項目

三　向第三方提供的方法

四　因應本人的要求，務必停止提供可供辨識該本人之個人資料給第三方。

五　受理本人要求的方法

3　電信事業業者變更前項第二款、第三款或第五款所揭示之事項的情形時，必須針對變更的內容，事先通知本人或置於本人容易得知的狀態，同時向保護個人資料委員會申報。

4　根據前二項的規定，通知或置於容易得知狀態的措施，必須根據下列所揭示之內容執行。

本報告之智慧財產權屬於國家通訊傳播委員會

一　根據向第三方提供的個人資料，被辨識的本人（於次款中簡稱「本人」。）要求停止該提供必須預設必要的期間。

二　必須根據本人確實認知第二項各款所揭示之事項，適當且合理的方法。

5　根據第二項或第三項的規定，必須經由下列所揭示之其中之一的方法進行申報。

一　根據保護個人資料委員會所規定的內容，使用電子資料處理組織（係指保護個人資料委員會所使用的電腦與進行申報者所使用的電腦利用電信迴路連線的電子資料處理組織。）的方法

二　提出記錄根據保護個人資料之相關法律實施規則（二○一六年保護個人資料委員會規則第三號。以下簡稱「規則」。）附件表格第一之申報書及應該記載於該申報書之事項的光碟（包含利用類似的方法，可以確實記錄所定事項的物品。以下簡稱「光碟等」。）的方法

6　電信事業業者經由代理人，根據第二項或第三項的規定進行申報的情形時，必須依照規則附件表格第二向保護個人資料委員會書面提出證明其權限的文件。

7　位於外國（係指本國境外之國家或地區。以下同。）的電信事業業者，根據第二項或第三項的規定進行申報的情形時，在國內有住址者，有關該申報的一切行為，必須規定具有代理該電信事業業者權限的內容。這種情形時，該電信事業業者於該申報的同時，該電信事業業者必須向保護個人資料委員會提出書面文件（包含使用日語的譯文。），證明有關該申報的一切行為，賦予國內有住址者代理該電信事業業者的權限。

8　無關前各項的規定，電信事業業者，除了有使用者同意的情形及其他有否定違法理由的情形之外，不得向第三方提供涉及秘密通訊的個人資料。

9　電信事業業者根據法律第二十三條第四項的規定公告之後，必須立即利用網路及其他適當的方法，公告第二項所揭示之事項（同項第二款、第三款或第五款所揭示之事項有所變更時，變更後該各款所揭示之事項）的內容。

10　於下列所揭示之情形時，該接受個人資料提供者，有關第一項到第七項及前項之規定的適用上，不被視為是第三方。

一　電信事業業者在達成使用目的的必要範圍內，伴隨將全部或部分個人資料委託處理，提供該個人資料的情形時

二　由於整併及其他事由，繼承事業連帶提供個人資料的情形時

三　與特定業者之間共享使用之個人資料，向該特定業者提供的情形

本報告之智慧財產權屬於國家通訊傳播委員會

時，關於其宗旨以及共享使用個人資料的項目、共享使用者的範圍、使用者的使用目的及負有管理該個人資料之負有責任者的姓名或名稱，事先通知本人或置於本人容易得知的狀態時。

11 電信事業業者針對前項第三款所規定之使用者的使用目的或個人資料的管理變更負有責任者之姓名或名稱的情形時，針對變更的內容，必須事先通知本人或置於本人容易得知的狀態。

（對位於國外第三方之提供的限制）

第十六條 電信事業業者向位於外國的第三方（關於個人資料的處理，根據法律第四章第一節的規定，個人資料處理事業業者有必要為了持續性採用相當於應該採取之措施的措施而言，建置符合次項所規定之標準的體制除外。以下於本條中亦同。）提供個人資料的情形時，除了前條第一項各款所揭示的情形之外，必須事先取得向位於外國之第三方提供的本人同意。在這種情形時，不適用同條（同條第八項除外。）的規定。

2 關於個人資料的處理，根據法律第四章第一節的規定，個人資料處理事業業者為了持續性採用相當於應該採取之措施的措施，規定必要措施的標準，務必符合下列各款其中之一。

一 在電信事業業者與接受個人資料提供者之間，關於該接受提供者的該個人資料處理，務必使用適當且合理的方法，以確保執行依照法律第四章第一節規定之宗旨的措施。

二 接受個人資料提供者務必接受根據個人資料處理之相關國際性組織的審核。

（涉及第三方提供之記錄的製作等）

第十七條 電信事業業者向第三方（法律第二條第五項各款所揭示者除外。以下於本條及次條中亦同。）提供個人資料時，藉由使用文件、電磁記錄或微縮膠卷製作的方法，配合下列各款所揭示之情形分類，必須分別製作適用該各款所規定之事項的相關記錄。但是該個人資料的提供適用第十五條第一項各款或第十項各款其中之一（根據前條規定之個人資料的提供，第十五條第一項各款的其中之一）的情形時，則不在此限。

一 根據第十五條第二項的規定，向第三方提供個人資料的情形時下列A到D所揭示之事項

A 提供該個人資料的年月日

B 該第三方的姓名或名稱以及其他足以指定該第三方的事項（對不特定多數人提供時，其要旨）

C 根據該個人資料，足以辨識本人的姓名及其他具體指定該本人

本報告之智慧財產權屬於國家通訊傳播委員會

的事項

D　該個人資料的項目

二　根據第十五條第一項或前條之規定，向第三方提供個人資料的情形時下列 A 及 B 所揭示之事項

A　取得第十五條第一項或前條之本人同意的要旨

B　前款 B 到 D 所揭示之事項

2　前項各款所規定之事項中，有關根據前項、次項及第四項所規定的方法，記錄於已經製成之前項記錄（僅限保存該記錄之情形時的內容。）中的事項與內容相同的內容，可以省略前項之該事項的記錄。

3　每次向第三方提供個人資料時，都必須迅速製作第一項的記錄。但是對該第三方持續性或反覆提供個人資料（根據第十五條第二項規定之提供除外。以下於本項中亦同。）時，或確實預計對該第三方持續性或反覆提供個人資料時的記錄，可以統一製作。

4　無關前項的規定，根據第十五條第一項或前條之規定，涉及對本人提供物品或勞務，向第三方提供關於本人之個人資料的情形時，有關該提供所製作之契約書及其他書面文件中記載第 1 項各款所規定之事項，根據該書面文件，可以代替第一項之該事項相關的記錄。

5　電信事業業者必須從製作第一項之記錄的當天開始，配合下列各款所揭示情形時的分類，分別規定該各款的保存期間。

一　根據前項所規定的方法製作記錄的情形時從最後提供該記錄相關個人資料之日算起、經過一年當日的期間

二　根據第三項但書所規定的方法製作記錄的情形時從最後提供該記錄相關個人資料之日算起，經過三年當日的期間

三　前二款以外的情形時三年

（接受第三方提供時的確認等）

第十八條　電信事業業者從第三方接受個人資料之提供時，必須配合下列各款所揭示之事項，分別根據該各款所規定之方法進行確認。但是該個人資料的提供適用第十五條第一項各款或第十項各款其中之一的情形時，則不在此限。

一　該第三方的姓名或名稱及住址以及法人時，其代表人（非法人團體但有規定代表人或管理人者，其代表人或管理人）的姓名（適用第三款所揭示之事項者除外。）從提供該個人資料之該第三方取得聲明的方法及其他適當的方法

二　經由該第三方取得該個人資料的過程（適用次款所揭示之事項者除

本報告之智慧財產權屬於國家通訊傳播委員會

外。）從提供該個人資料之該第三方取得顯示經由該第三方取得該個人資料之過程的契約書及提示其他書面文件的方法及其他適當的方法

三　從該第三方接受其他個人資料之提供時，已經經由前二款所規定的方法進行確認（關於該確認，僅限依照第三項、第五項及第六項所規定的方法，製作及保存記錄的情形時。）的事項進行確認該事項的內容與該提供相關之前二款所揭示之事項的內容相同的方法

2　電信事業業者根據同項的規定進行確認的情形時，前項的第三方對該電信事業業者，不得偽造有關該確認的事項。

3　電信事業業者根據第一項的規定進行確認時，藉由使用文件、電磁記錄或微縮膠卷製作的方法，配合下列各款所揭示之情形分類，必須分別製作該各款所規定之事項的相關記錄。

一　根據法律第二十三條第二項的規定，從個人資料處理事業業者接受個人資料之提供的情形時下列 A 到 E 所揭示之事項

A　接受個人資料之提供的年月日

B　第一項各款所揭示之事項

C　根據該個人資料，足以辨識本人的姓名及其他具體指定該本人的事項

D　該個人資料的項目

E　根據法律第二十三條第四項之規定，公告的要旨

二　根據法律第二十三條第一項或法律第二十四條之規定，從個人資料處理事業業者接受個人資料之提供的情形時下列 A 及 B 所揭示之事項

A　法律第二十三條第一項各款所列出以外的部分或法律第二十四條取得本人同意的要旨

B　前款 B 到 D 所揭示之事項

三　從第三方（適用個人資料處理事業業者除外。）接受個人資料之提供的情形時第一款 B 到 D 所揭示之事項

4　前項各款所規定之事項中，有關根據前項、次項及第六項所規定的方法已經製作之前項的記錄（僅限保存該記錄之情形時的內容。）中所記錄的事項與內容相同的內容，可以省略同項之該事項的記錄。

5　每次從第三方接受個人資料之提供時，都必須迅速製作第三項的記錄。但是從該第三方持續性或反覆接受個人資料之提供（根據第十五條第二項規定之提供除外。以下於本條中亦同。）時，或確實預計從該第三方持續性

本報告之智慧財產權屬於國家通訊傳播委員會

或反覆接受個人資料之提供時的記錄，可以統一製作。

6　無關前項的規定，涉及對本人提供物品或勞務，從第三方接受關於該本人之個人資料之提供的情形時，有關該提供所製作之契約書及其他書面文件中記載第 3 項各款所規定之事項時，根據該書面文件，可以代替同項之該事項相關的記錄。

7　電信事業業者必須從製作第三項之記錄的當天開始，配合下列各款所揭示之情形分類，分別規定該各款的保存期間。

一　根據前項所規定的方法製作記錄的情形時從最後接受該記錄相關個人資料的提供之日算起，經過一年當日的期間

二　根據第五項但書所規定的方法製作記錄的情形時從最後接受該記錄相關個人資料的提供之日算起，經過三年當日的期間

三　前二款以外的情形時三年

（持有個人資料之相關事項的公告等）

第十九條　電信事業業者必須將持有個人資料，針對下列所揭示之事項，置於本人可以得知之狀態（包含回應本人的要求，即時回答的情形時。）。

一　該電信事業業者的姓名或名稱

二　全部持有個人資料的使用目的（適用從第八條第四項第一款到第三款的情形時除外。）

三　根據次項規定的要求或回應根據次條第一項、第二十一條第一項或第二十二條第一項或第三項規定之要求的手續（根據第二十五條第二項的規定，決定手續費金額時，包含該手續費的金額。）

四　該電信事業業者所進行之持有個人資料處理相關客訴的投訴單位

五　該電信事業業者為認證保護個人資料團體之對象事業業者的情形時，該認證保護個人資料團體的名稱及解決客訴的投訴單位

2　電信事業業者經由本人要求通知可以辨識該本人之持有個人資料的使用目的時，必須立即將此通知本人。但是適用下列各款其中之一的情形時，則不在此限。

一　根據前項的規定，可以辨識該本人之持有個人資料的使用目的明確的情形時

二　適用第八條第四項第一款到第三款的情形時

3　電信事業業者根據前項的規定，決定不通知所要求之持有個人資料之使用目的的要旨時，則必須立即將其要旨通知本人。

（公開）

第二十條　本人可以要求電信事業業者公開可以辨識該本人的持有個人資

本報告之智慧財產權屬於國家通訊傳播委員會

料。

2　電信事業業者受理根據前項之規定的要求時，經由使用書面交付本人的方法（要求公開者有其同意之方法時，使用該方法），必須立即公開該持有個人資料。但是由於公開的行為符合下列各款其中之一的情形時，則可以不必公開其全部或部分。

一　可能會有危及本人或第三方的生命、身體、財產及其他權益之疑慮的情形時

二　對該電信事業業者正確執行業務可能造成顯著阻礙之疑慮的情形時

三　違反法令（法律、保護個人資料之相關法律實施令（二○○三年政令第五○七號）及規則除外。於第四項及次條第二項中，亦同。）之行為的情形時

3　電信事業業者根據第一項的規定，決定不公開全部或部分持有個人資料的要求之要旨時或該持有個人資料不存在時，則必須立即將其要旨通知本人。

4　根據法令的規定，藉由相當於第二項本文所規定之方法的方法，對本人公開全部或部分可以辨識該本人之持有個人資料的情形時，關於該全部或部分的持有個人資料，不適用第一項及第二項的規定。

（修正等）

第二十一條　可以辨識該本人之持有個人資料的內容並非事實時，本人可以要求電信事業業者，修正、追加或刪除（以下於本條中，簡稱「修正等」。）該持有個人資料的內容。

2　電信事業業者根據前項之規定受理要求的情形時，關於其內容的修正等，除了根據法令的規定，有特別規定之手續的情形之外，在達成使用目的的必要範圍內，必須立即進行必要的調查，並根據其結果，進行該持有個人資料之內容的修正等。

3　涉及根據第一項規定之要求的全部或部分持有個人資料的相關內容，電信事業業者決定進行修正等時或不進行修正等的要旨時，必須立即將其要旨通知本人（進行修正等時，包含其內容。）。

（停止使用等）

第二十二條　可以辨識該本人之持有個人資料違反第五條之規定處理時或違反第七條之規定取得的行為時，本人可以對電信事業業者提出停止或消除（以下於本條中，簡稱「停止使用等」。）使用該持有個人資料的要求。

2　電信事業業者根據前項的規定受理要求的情形時，於判明該要求有其理由時，在為了更正違反之必要的限度內，必須立即停止該持有個人資料的使

本報告之智慧財產權屬於國家通訊傳播委員會

用等。但是停止該持有個人資料的使用等必須耗費大額費用的情形時及其他執行停止使用等行為有所困難的情形時，為了保護本人的權益，採取代替停止使用等必要措施時，則不在此限。

3　可以辨識該本人之持有個人資料違反第十五條第一項或第十六條之規定向第三方提供時，本人可以對電信事業業者提出停止向第三方提供該持有個人資料的要求。

4　電信事業業者根據前項的規定受理要求的情形時，於判明該要求有其理由時，必須立即停止向第三方提供該持有個人資料。但是停止向第三方提供該持有個人資料的要求必須耗費大額費用的情形時及其他停止向第三方提供的行為有所困難的情形時，為了保護本人的權益，採取代替停止提供等必要措施時，則不在此限。

5　有關涉及根據第一項規定之要求的全部或部分持有個人資料，電信事業業者決定進行停止使用等時或不進行停止使用等的要旨時，或有關涉及根據第三項規定之要求的全部或部分持有個人資料，決定停止向第三方提供時或不停止向第三方提供的要旨時，則必須立即將其要旨通知本人。

（理由的說明）

第二十三條　電信事業業者根據第十九條第三項、第二十條第三項、第二十一條第三項或前條第五項的規定，針對來自本人要求或被要求之措施的全部或部分，通知不採取該措施之要旨的情形時或通知採取與該措施不同措施之要旨的情形時，必須努力對本人說明其理由。

（回應公開等要求的手續）

第二十四條　關於根據第十九條第二項之規定的或第二十條第一項、第二十一條第一項或第二十二條第一項或第三項之規定的要求（以下於本條中簡稱「公開等之要求等」。），電信事業業者可以規定下列各款所揭示之內容為其要求或受理要求的方法。在這種情形時，本人必須遵守這些方法，進行公開等之要求等。

一　公開等之要求等的投訴單位

二　公開等之要求等時，應該提出之文件的表格及其他公開等之要求等的方式

三　確認提出公開等之要求等者為本人或第三項所規定之代理人的方法

四　收取次條第一項手續費的方法

2　關於公開等之要求等，電信事業業者可以要求本人提示足以具體指定其對象之持有個人資料的事項。在這種情形時，電信事業業者為了使本人容易且確實進行公開等之要求等，必須採取有助於具體指定該持有個人資料之

本報告之智慧財產權屬於國家通訊傳播委員會

資料的提供及其他考慮對本人之方便的適當措施。

3　可以經由下列所揭示之代理人進行公開等之要求等。但是根據第二十條第一項的規定，關於公開的要求，適用第二十條第二項各款其中之一，侵害本人秘密通訊的情形時等，則不在此限。

一　未成年者或成年被監護人的法定代理人

二　本人針對進行公開等之要求等所委任的代理人

4 電信事業業者根據前三項的規定，規定回應公開等要求等的手續時，必須考慮避免對本人造成過重的負擔。

（手續費）

第二十五條　電信事業業者根據第十九條第二項的規定，被要求使用目的的通知時，或根據第二十條第一項的規定，受理公開的要求時，關於該措施的執行，可以收取手續費。

2　電信事業業者根據前項的規定，收取手續費的情形時，必須考慮實際費用，在合理且被認可的範圍內，規定該手續費的金額。

（事前的要求）

第二十六條　本人根據第二十條第一項、第二十一條第一項或第二十二條第一項或第三項的規定，打算提起關於要求的訴訟時，對應該成為該訴訟被告的對象，必須先進行該要求，且沒有從到達之日起經過二星期以後的話，無法提起該訴訟。但是應該成為該訴訟被告的對象拒絕其要求時，則不在此限。

2　前項的要求，其要求於通常應該到達時，即視為到達。

3　前二項的規定根據第二十條第一項、第二十一條第一項或第二十二條第一項或第三項的規定，比照適用針對有關要求之假處分的聲請。

（對電信事業業者客訴之處理）

第二十七條　電信事業業者必須適當且迅速地處理個人資料處理之相關客訴。

2　電信事業業者為了達成前項的目的必須建置必要的體制。

（匿名加工資料的製作等）

第二十八條　電信事業業者於製作匿名加工資料（僅限構成匿名加工資料資料庫等的內容。以下同。）時，為了辨識特定個人及避免復原用來製作的個人資料，必須依照下列所規定之必要的內容為標準，加工該個人資料。

一　必須刪除全部或部分包含於個人資料中可以辨識特定個人的敘述等（包含利用沒有規則性可以復原全部或部分敘述等的方法來置換其他敘述等的方法。）。

二　必須刪除包含於個人資料中全部個人辨識符號（包含利用沒有規則

本報告之智慧財產權屬於國家通訊傳播委員會

性可以復原該個人辨識符號的方法來置換其他敘述等的方法。)。

三　務必刪除連結個人資料與該個人資料採取之措施所取得之資料的符號（僅限目前電信事業業者相互連線所處理之資料的符號。)(包含利用沒有規則性可以復原該符號的方法，來置換該個人資料與無法連結該個人資料採取之措施所取得之資料的符號。)。

四　務必刪除特異的敘述等（包含利用沒有規則性可以復原該特異敘述等方法來置換其他敘述等的方法。)。

五　除了前各款所揭示之措施之外，考慮包含在個人資料中的敘述等與包含在構成包含該個人資料之個人資料資料庫等其他個人資料中的敘述等的差異及其他該個人資料資料庫等的性質，務必根據其結果採取適當的措施。

2　電信事業業者製作匿名加工資料時，為了防止從用於製作之個人資料所刪除的敘述等以及個人辨識符號連同根據前項規定加工方法之相關資料洩漏，必須依照下列所規定之必要的內容為標準，採取為了這些資料之安全管理的措施。

一　務必明確規定處理加工方法等資料（係指從用於製作之個人資料所刪除的敘述等以及個人辨識符號連同根據前項規定的規定所進行之加工方法的相關資料（僅限使用該資料可以復原該個人資料的內容。)。以下於本條中亦同。）人員的權限及責任。

二　建置加工方法等資料處理相關規章種類，依照該規章種類適當處理加工方法等資料的同時，針對該處理狀況進行評鑑，務必根據其結果採取為了謀求改善之必要的措施。

三　為了防止沒有處理加工方法等資料之正當權限的人員處理加工方法等資料，務必採取必要且適當的措施。

3　電信事業業者製作匿名加工資料時，必須立即利用網路及其他適當的方法，公告包含於該匿名加工資料中之個人相關資料的項目。

4　電信事業業者受其他的個人資料處理事業業者的委託，製作匿名加工資料的情形時，該其他的個人資料處理事業業者必須根據前項所規定的方法公告包含於該匿名加工資料中個人相關資料的項目。在這種情形時，根據該公告，視同該電信事業業者公告該項目。

5　電信事業業者製作匿名加工資料之後，向第三方提供該匿名加工資料時，必須利用網路及其他適當的方法，事先公告關於包含於第三方提供之匿名加工資料的個人相關資料的項目及其提供的方法，同時利用電子郵件送信的方法或書面交付的方法及其他適當的方法，對該第三方清楚表明該提供

本報告之智慧財產權屬於國家通訊傳播委員會

之相關資料為匿名加工資料的要旨。

6　電信事業業者製作匿名加工資料之後，自行處理該匿名加工資料時，為了辨識有關用於製作該匿名加工資料之個人資料的本人，該匿名加工資料不得與其他的資料進行比對。

7　電信事業業者製作匿名加工資料時，為了該匿名加工資料之安全管理所必要且適當的措施，確保該匿名加工資料製作及其他處理相關客訴處理及其他該匿名加工資料的正確處理，必須努力自行採取必要的措施，且公告該措施的內容。

（匿名加工資料之提供）

第二十九條　身為匿名加工資料處理事業業者的電信事業業者，在向第三方提供匿名加工資料（自己加工個人資料所製作的內容除外。以下於本章中亦同。）時，必須利用網路及其他適當的方法，事先公告關於包含於第三方提供之匿名加工資料的個人相關資料的項目及其提供的方法，同時利用電子郵件送信的方法或書面交付的方法及其他適當的方法，對該第三方清楚表明該提供之相關資料為匿名加工資料的要旨。

（辨識行為的禁止）

第三十條　　身為匿名加工資料處理事業業者的電信事業業者，處理匿名加工資料時，為了辨識有關用於製作該匿名加工資料之個人資料的本人，根據從該個人資料所刪除的敘述等或個人辨識符號或第二十八條第一項、行政機關所持有之持有保護個人資料之相關法律（二○○三年法律第五十八號）第四十四條之十第一項（包含在同條第二項中比照適用的情形時。）或獨立行政法人等所持有之保護個人資料相關法律（二○○三年法律第五十九號）第四十四條之十第一項（包含在同條第二項中比照適用的情形時。）的規定，取得進行加工方法相關資料或該匿名加工資料不得與其他的資料進行比對。

（安全管理措施等）

第三十一條　身為匿名加工資料處理事業業者的電信事業業者，為了該匿名加工資料之安全管理的必要且適當的措施，確保匿名加工資料處理相關客訴處理及其他該匿名加工資料的正確處理，必須努力自行採取必要的措施，且公告該措施的內容。

第三章　各種資料的處理

（通聯記錄）

第三十二條　有關通聯記錄（係指使用者使用電信的日期、時間，該電信的對方及其他使用者之電信相關資料，該電信內容以外的資料。以下同。）電

本報告之智慧財產權屬於國家通訊傳播委員會

信事業業者可以記錄範圍僅限於資費、繳費通知、客訴回應，防止非法使用及其他執行業務上之必要的情形時。

2　除非有使用者同意的情形時、遵守法官所簽發之令狀的情形時、適用正當防衛或緊急避難的情形及其他有否定違法理由的情形時之外，電信事業業者不得向他人提供通聯記錄。

（使用明細）

第三十三條　電信事業業者對於記載在使用明細（係指記載對應使用者使用電信的日期、時間、該電信之收信對象等這些的資費資料及其他使用者使用該電信之相關資料的書面文件。以下同。）之資料的範圍，不得超過達成使用明細之目的的必要範圍。

2　電信事業業者將使用明細讓簽約用戶及其他可以閱覽者閱覽或交付時，必須採取必要的措施，以避免不當侵害使用者的秘密通訊及個人資料。

（發話人資料）

第三十四條　電信事業業者提供顯示發話人資料服務（係指顯示發話電話號碼、發話人位置之資料等發話人相關資料（以下簡稱「發話人資料」。）向受話人顯示的電話服務。以下同。）的情形時，必須對每次通訊設定不顯示發話人資料的功能。

2　電信事業業者提供顯示發話人資料服務的情形時，為了確保使用者的權利必須採取必要的措施。

3　電信事業業者除了有必要提供顯示發話人資料服務及其他服務的情形時之外，不得向他人提供發話人資料。但是在有使用者同意的情形時、遵守法官所簽發之令狀的情形時、使用電話犯下恐嚇罪之現行犯的情形時，根據被害人及搜查機關的要求進行反向追查時，人的生命、身體等有迫在眉睫之危險之緊急通報的情形，根據來自該通報對象的要求進行反向追查時以及其他具有否定違法理由的情形時，則不在此限。

（定位資料）

第三十五條　電信事業業者在事先取得使用者同意的情形時，僅以提供電信勞務之相關正當業務行為及其他有否定違法理由的情形為限，可以取得定位資料（係指顯示持有行動設備終端機器者的位置資料，非發話人資料的內容。以下同。）。

2　電信事業業者僅限於事先取得使用者同意的情形時、遵守法官所簽發之令狀的情形時及其他有否定違法理由的情形時，可以針對定位資料，可以提供他人及做為其他用途。

3　電信事業業者提供通知簽約用戶或其指示者定位資料的服務，或向第三方

本報告之智慧財產權屬於國家通訊傳播委員會

提供的情形時，為了防止不當侵害使用者權利的行為，採取必要的措施較為適當。

4　電信事業業者根據來自搜查機關的要求，被要求取得定位資料的情形時，僅限遵守法官所簽發之令狀時，才可以取得該定位資料。

5　電信事業業者除了前項之外，根據來自搜索待援者，進行救援的警察、海上保安廳或消防及其他比照適用之機構的要求，被要求取得待援者定位資料的情形時，僅限對該人的生命或身體具有迫切性的重大危險，且為了及早發現該待援者，被認為取得該定位資料的行為實屬不可或缺的情形時，才可以取得該定位資料。

（滯納者等資料）

第三十六條　電信事業業者尤其有必要防止拒繳電信勞務相關費用或非法使用行動語音通訊勞務，且被認為適當時，與其他電信事業業者之間，可以交換滯納者等資料（係指儘管超過付款日期仍然拒繳電信勞務相關費用者或適用行動語音通訊事業業者防止簽約者等的本人確認等及行動語音通訊勞務非法使用相關法律（二○○五法律第三十一號）第十一條各款的情形時，涉及提供行動語音通訊勞務等相關契約之名義所有人的姓名、住址、滯納金額、電話號碼及其他該人或該名義所有人之相關資料。以下同。）。但是交換該滯納者等資料之對象被認為可能有不當侵害本人權益的疑慮時，則不在此限。

2　電信事業業者與其他的電信事業業者之間交換滯納者等資料的情形時，關於其要旨以及被交換之滯納者等資料的項目、交換之電信事業業者的範圍及被交換之滯納者等資料之管理，最好事先將負有責任者的姓名或名稱，通知本人或置於本人容易得知的狀態較為恰當。

3　電信事業業者變更前項關於被交換之滯納者等資料管理負有責任者之姓名或名稱的情形時，針對變更的內容，最好事先通知本人或置於本人容易得知的狀態較為恰當。

4　交換滯納者等資料的電信事業業者，最好不得將該滯納者等資料使用於簽約時審查以外的目的較為恰當。

5　提供滯納者等資料或接受提供之電信事業業者，最好採取萬全之策正確管理該滯納者等的資料較為恰當。

（關於寄送垃圾郵件等的簽約用戶資料）

第三十七條　電信事業業者尤其有必要為了防止由於同時對多數使用者發送電子郵件，導致電子郵件在寄送、接收上的障礙且被認為適當時，可以和其他的電信事業業者交換簽約用戶資料（僅限於以違反正確寄送特定電子郵

本報告之智慧財產權屬於國家通訊傳播委員會

件等的相關法律（二○○二年法律第二十六號）的規定，同時對多數使用者寄送電子郵件及寄送其他有可能造成電子郵件在寄送、接收障礙之疑慮的電子郵件為理由，電信事業業者採取停止使用的措施或解除契約之簽約用戶的姓名、住址及其他該簽約用戶之相關資料。以下同。）。但是被認為交換對象的該簽約用戶資料可能有不當侵害本人權益之疑慮時，則不在此限。

2　電信事業業者與其他的電信事業業者之間交換簽約用戶資料的情形時，關於其要旨以及被交換之簽約用戶資料的項目、交換之電信事業業者的範圍及被交換之簽約用戶資料的管理，最好事先將負有責任者的姓名或名稱，通知本人或置於本人容易得知的狀態較為恰當。

3　電信事業業者變更前項關於被交換之簽約用戶資料管理負有責任者之姓名或名稱的情形時，針對變更的內容，通知本人或置於本人容易得知的狀態較為恰當。

4　交換簽約用戶資料的電信事業業者，最好不得將該簽約用戶資料使用於簽約時審查以外的目的較為恰當。

5　提供簽約用戶資料或接受提供之電信事業業者，最好採取萬全之策正確管理該簽約用戶資料較為恰當。

（電話號碼資料）

第三十八條　電信事業業者使用電話號碼資料（係指電信事業業者簽訂固網電話契約連帶得知的簽約用戶姓名或簽約用戶希望刊載在電話簿、電話號碼查詢的名稱及對應這些的電話號碼及其他簽約用戶相關的資料。以下同。）發行電話簿或進行電話號碼查詢業務的情形時，關於是否刊載在電話簿或電話號碼查詢，最好給予簽約用戶有所選擇的機會較為恰當。在這種情形下，簽約用戶選擇省略時，必須立即將該簽約用戶的資料排除於刊載在電話簿或電話號碼查詢業務的對象之外。

2　電信事業業者發行電話簿或從事電話號碼查詢業務的情形時，所提供之電話號碼資料的範圍，為了達成各業務目的達成，務必不得超過必要的限度較為恰當。但是有簽約用戶同意的情形時，則不在此限。

3　電信事業業者發行電話簿或從事電話號碼查詢業務的情形時，所提供之電話號碼資料的形態，最好不得具有不當侵害本人權益的內容較為恰當。

4　電信事業業者除了發行電話簿或從事電話號碼查詢業務的情形之外，不得提供電話號碼資料較為恰當。但是下列所揭示之情形時，則不在此限。

一　委託外部發行電話簿或從事電話號碼查詢業務的情形時

二　向發行電話簿或從事電話號碼查詢業務者提供的情形時

本報告之智慧財產權屬於國家通訊傳播委員會

三　其他適用第五條第三項各款的情形時

5　電信事業業者發行電話簿或從事電話號碼查詢業務者提供電話號碼資料的情形時，在該提供契約等，務必規定比照適用前各項之處理方式較為恰當。

第四章　雜項

（指引的重新審查）

第三十九條　關於本指引，基於社會形勢的改變、國民意識的改變、技術動向的改變等諸多環境的變化，如有必要應進行重新審查。

本報告之智慧財產權屬於國家通訊傳播委員會

附錄7：日本新冠肺炎密切接觸者應用程式使用規則

（目的）
第 1 條 本使用規則之目的係，針對如何使用厚生勞動省所提供的接觸確認應用程式，制定適用於使用者之使用條件等事項。
（定義）
第 2 條 本使用規則中所使用之術語定義如下。
一 「接觸」係指，在大約 1 米內之距離，保持 15 分以上之近距離接觸之可能性較高之狀態。
二 「陽性者」係指，新冠肺炎之陽性感染確診者。
三 「感染可能期間」之範圍，如為新冠肺炎有症狀之陽性者為從其發病之日起約兩天前以後，如為新冠肺炎無症狀陽性者則為從其接受檢查之日起約兩天前以後。
四 「接觸確認應用程式」以及「本 APP」是指，使用智慧手機的近距離通信功能（藍芽），檢測並記錄人與人之接近情況（包括接觸，下同。），在查明某位 APP 使用者為陽性者的情況下，獲得該陽性者同意後，被確認在過去 14 天內與處於感染可能期間內之該陽性者有過接觸史之其他 APP 使用者無需接收可識別該陽性者身分之訊息，即可接收到自己在過去 14 天內曾與處於感染可能期間內之陽性者有過接觸之通知訊息之應用程式。
五 「APP 使用者」係指，透過本 APP 使用本 APP 所提供之服務者。
六 「已安裝 APP 之終端」係指，安裝有本 APP 之智慧手機終端。
七 「日更密鑰」係指，與該終端具有一對一之對應關係，在已安裝 APP 之終端中以 24 小時為單位變更之識別碼。
八 「接觸符號」係指，基於日更密鑰所生成，在已安裝 APP 之終端中以 10 分鐘為單位變更的識別碼。
九 「通知服務器」係指，由厚生勞動省進行管理具有如下功能之服務器：與已安裝 APP 之終端進行協作，讓 APP 使用者可以在同意必要事項之基礎上對從終端上登錄之日更密鑰進行管理，並在一定之條件下將該日更密鑰提供給其他 APP 使用者之已安裝 APP 終端。
十 「管理系統」係指，為了對新冠肺炎之陽性者以及密切接觸者之訊息進行管理，而由厚生勞動省進行營運，用於都道府縣以及設置保健所之市，掌握和管理新冠肺炎感染者等訊息之支援系統。
十一 「受理編號」係指，在查明某位 APP 使用者為陽性者之情況下，由管理系統向該 APP 使用者隨機發行，進行通知之任意臨時編號。
（認可本使用規則）
第 3 條 APP 使用者必須遵循本使用規則中之規定事項使用本 APP，充分理解本使用規則之內容並認可本使用規則，否則無法使用本 APP。

本報告之智慧財產權屬於國家通訊傳播委員會

2 APP 使用者實際開始使用本 APP 的情況下，則視為 APP 使用者已經充分理解本使用規則的內容，並已經認可本使用規則。

（本 APP 之訊息生成、記錄以及提供等運行機制）

第 4 條 APP 使用者在開始使用本 APP 之前，必須充分理解關於本 APP 之訊息生成、記錄以及提供等運行機制的如下事項，並認可本使用規則，方可開始使用本 APP。

一 在 APP 使用者所持有之已安裝 APP 之終端上自動生成日更密鑰並進行記錄，所記錄的日更密鑰在其生成的 14 天後自動失效。

二 在 APP 使用者所持有的已安裝 APP 的終端上自動生成接觸符號並進行記錄，所記錄的接觸符號在其生成的 14 天後自動失效。

三 僅限 APP 使用者以及處於接近狀態的其他 APP 使用者各自啟動其已安裝 APP 的終端的藍芽功能時，可以使用藍芽功能，(i)將自身的已安裝 APP 的終端上所生成並記錄的接觸符號，自動提供給處於接近狀態的其他 APP 使用者的已安裝 APP 的終端，並進行記錄，(ii)將該其他 APP 使用者的已安裝 APP 的終端上所生成並記錄的接觸符號自動提供至自身的已安裝 APP 的終端中，並進行記錄。

四 因前項所述的操作而被記錄於已安裝 APP 的終端中的其他 APP 使用者的接觸符號，將在其產生記錄的 14 天後自動失效。

五 APP 使用者在查明自身為陽性者的情況下，如另行同意如下事項：(a)將已安裝至自身終端中的 APP 所記錄的日更密鑰（僅限在該陽性者的感染可能期間內所生成的日更密鑰。下同。）提供給其他 APP 使用者的已安裝 APP 的終端，並且，(b)如其他 APP 使用者在感染可能期間內與自身有過接觸狀態，無需提供可識別該陽性者個人身分的訊息，即可通知對方其可能與不特定的處於感染可能期間內的陽性者有過接觸，則可以執行如下事項：(i)將(A)至另行登錄到管理系統中的自身手機號碼或電子信箱的受理編號以及(B)該陽性者有新冠病毒感染症狀的情況下則將其發病日，沒有新冠病毒感染症狀的情況下則將其檢查日輸入到自身的已安裝 APP 的終端，(ii)從該已安裝 APP 的終端經由通知服務器前往管理系統查詢，確認所輸入的是否確為發行給該陽性者的受理編號，(iii)管理系統回答通知服務器，所查詢的受理編號是否確為發行給該陽性者的受理編號。相關查詢的結果，如管理系統回答所查詢的受理編號確為發行給該陽性者的受理編號，則記錄於該陽性者自身的已安裝 APP 的終端上的日更密鑰可以經由通知服務器自動提供至其他使用者的已安裝 APP 的終端上，該其他使用者在其已安裝 APP 的終端上最多可自動追溯搜索過去 14 天內該其他使用者的已安裝 APP 的終端內所記錄的接觸符號，如查明存在接觸陽性者的可能性較高的接觸符號，則該其他使用者的已安裝 APP 的終端會收到可能與不特定的處於感染可能期間內的陽性者有過接觸的通知。

2 APP 使用者實際開始使用本 APP 的情況下，則視為 APP 使用者已經充分理解前項的內容，並已經認可本使用規則。

本報告之智慧財產權屬於國家通訊傳播委員會

（本 APP 等相關智慧財產權等）
第 5 條 厚生勞動省提供給 APP 使用者的所有服務、程序以及各種著作物（包含本使用規則以及使用步驟書等，下同。）相關的著作權、著作人格權、商標權等智慧財產權以及經驗技術等智慧財產權相關權利，全部歸屬於厚生勞動省或其他正當權利人。除本使用規則中另有規定的情況外，相關的智慧財產權不會因 APP 使用者使用本 APP 而轉移給 APP 使用者，也不意味著設置或允諾使用權。
2 APP 使用者在使用本 APP 的過程中，應按照如下各條款中的規定處理厚生勞動省提供給 APP 使用者的一切服務、程序以及各種著作物。
一 僅用於遵循本使用規則正確地使用本 APP。
二 不得複製、篡改、編輯、發布等，此外也不得進行反向工程剖析。
三 無論是否出於營利目的，均不得轉讓、出借或過繼給第三方，也不得以擔保抵押的方式提供給第三方。
四 不擅自刪除或修改厚生勞動省或厚生勞動省所指定的人士的著作權標識或商標權標識。
3 無關前兩項，在使用開源代碼時，如有應遵守該開源規定的事項，則以該規定為優先。關於該開源代碼，您可以訪問 https://github.com/cocoa-mhlw/cocoa 進行確認。
（使用可能時間以及使用的停止等）
第 6 條 本 APP 之可使用時間原則上為一天中之 24 小時以及一年中之 365 天。然而由於管理系統之運轉情況，本 APP 之部分功能可能存在暫時無法提供之情況。
2 厚生勞動省認為符合如下各條款中任何一項之情況下，可以事先以在厚生勞動省之新冠肺炎感染對策相關網站或本 APP 內通知 APP 使用者之基礎上，停止、暫停或中斷本 APP 之使用。如情況確實緊急，可以在未經事先通知而直接停止、暫停或中斷本 APP 之使用。
一 本 APP 之營運設備等預計將進行維護之情況下
二 通訊服務商無法提供服務的情況下
三 發生天災、政局變動等緊急事態或本 APP 發生重大營運障礙之情況下
四 本 APP 由於法律法規及其相關措施而無法繼續營運之情況下
五 厚生勞動省判斷需要停止、暫停或中斷本 APP 的使用之其他各種情況下
3 在本 APP 之使用情況明顯過於集中之情況下，厚生勞動省可以限制本 APP 之使用。
（面向 APP 使用者的用戶支持）
第 7 條 為了受理涉及本 APP 之使用者諮詢和協商，厚生勞動省設置了客戶服務台和呼叫中心。
2 設置客戶服務台的目的係，透過電子郵件受理來自 APP 使用者的關於本 APP 的諮詢和協商，並給出答覆，從而為本 APP 的使用者提供支援，並收集用於改

本報告之智慧財產權屬於國家通訊傳播委員會

善本 APP 功能等的訊息。可接收郵件的時間原則上為每年 365 天、每天 24 小時。郵件服務器的運行狀況等可能會導致偶爾無法接收郵件。此外，根據使用者所諮詢的內容，可能需要一定時間後才能給出答覆或無法給出答覆。

3 對於在本 APP 中收到可能與處於感染可能期間內的陽性者有過接觸的通知的 APP 使用者，呼叫中心透過電話受理其諮詢，根據需要將其引流至各地區的諮詢窗口，在判明 APP 使用者自己為陽性者的情況下，為 APP 使用者提供支援，協助其從安裝有該 APP 的終端向通知服務器發送處理編號以及記錄於該 APP 使用者的安裝有 APP 的終端中的日更密鑰。呼叫中心並非由醫生、保健師、護士等醫療專業人員應對 APP 使用者的健康諮詢。呼叫中心的電話號碼和工作時間請參照上文的通知，又或者營運方將電話號碼發送給需要支援的 APP 使用者。由於電話線路的事故和擁堵等原因，可能出現電話無法接通或接通耗時的情況。此外，根據您所諮詢的內容，營運方也有可能無法給出答覆。

（禁止事項以及遵守事項）

第 8 條 APP 使用者在使用本 APP 的過程中，不得進行如下各條款中所述的行為。

一 將本 APP 用於原本目的之外的其他目的。

二 違法訪問行為、對本 APP 的服務器以及網絡系統造成危害的行為、對本 APP 進行不正當操作的行為，有意鑽漏洞的行為。

三 類似或同樣的問題反覆提問的行為，對服務提供方提出不正當要求的行為、對於服務提供方合理管理和營運本 APP 以及第三方正常使用本 APP 造成妨害或構成阻礙的其他行為。

四 故意向本 APP 傳輸感染病毒、惡意軟體等檔案之行為。

五 違反或可能違反法律法規和公序良俗之行為、為反社會勢力輸送利益等協助行為、偽裝成服務提供方或第三方之行為、故意散布虛假訊息之行為。

六 不正當蒐集、開示或提供第三方之個人訊息、使用訊息等行為。

七 厚生勞動省判斷對本 APP 之合理營運造成或可能造成阻礙之其他行為。

2 在判斷 APP 使用者已經進行或可能進行前項各條款中的任何一種行為的情況下，厚生勞動省可以不經事先通知，而直接停止該 APP 使用者對於本 APP 的使用權。

3 APP 使用者在使用本 APP 之過程中，應遵守如下事項。

一 如同時持有多台智慧手機終端，盡量只將本 APP 安裝至最常用之一部手機中。

二 不將已安裝 APP 的終端交給第三方進行管理。

三 在本 APP 有更新版本，並且 APP 使用者處於可下載之狀態時，應下載最新版本並將其更新至已安裝 APP 之終端上。

四 如將已安裝 APP 的終端轉讓、過繼或借出給第三方，或丟棄該終端，應提前刪除本 APP。

本報告之智慧財產權屬於國家通訊傳播委員會

（APP 使用者的設備等）
第 9 條 APP 使用者應自行自費準備使用本 APP 所需之所有設備以及軟體（包括智慧手機終端以及一切通信手段。）。其所需之必要手續也應由 APP 使用者自身負責進行。
2 使用本 APP 所需之通信費用等本 APP 之使用所需之一切費用，均由 APP 使用者承擔。
3 如 APP 使用者為未成年人，該 APP 使用者應在獲得其監護人或其法定代理人同意的基礎上，透過其所認可的智慧手機終端使用本 APP。
4 APP 使用者使用本 APP 時之周邊環境情況，以厚生勞動省之新冠肺炎感染對策相關網站所登載之條件為準。
（免責事項）
第 10 條 因使用本 APP（無關使用時感染病毒・惡意程序等理由。）或無法使用本 APP（無關本 APP 停止、暫停、中斷服務或服務受限，本 APP 的動作不良或通信線路障礙等理由。）以及其他 APP 使用者或第三方因使用本 APP 或因與其相關的原因而蒙受的損失，厚生勞動省概不負責。如因厚生勞動省自身的故意或重大過失而造成全部或部分損失的情況下，則該全部或部分損失不受此限。
2 已安裝 APP 之終端間之距離之測定受藍芽信號強度之影響，設計時並沒有考慮到藍芽信號是否會穿過障礙物（玻璃窗或薄的隔斷墻等），測定值會因已安裝 APP 的終端的性能、手持方向等條件和狀態的影響而產生偏差，因此本 APP 所測量到的接觸距離和時間均不保證其正確性。
（APP 的使用中止以及記錄的刪除）
第 11 條 APP 使用者可以隨時隨意從已安裝 APP 的終端上刪除並停止使用本 APP。如已從已安裝 APP 的終端上刪除本 APP，則記錄於該終端上之訊息也隨之全部刪除，無法復原。
（本使用規則的修改）
第 12 條 厚生勞動省在其認為必要時，可以不另行向 APP 使用者進行事先通知，而隨時對本使用規則進行修改。
2 厚生勞動省在修改本使用規則的情況下，應立即將修改內容公開至厚生勞動省的新冠肺炎感染對策相關網站以及本 APP 內，修改後的本使用規則在修改內容被公開時即告生效。
3 公開了經前項所述之修改的本使用規則之後，在 APP 使用者實際使用本 APP 的情況下，則視為該 APP 使用者已經充分理解修改後的本使用規則的內容，並認可修改後的本使用規則。
（轉讓等禁止）
第 13 條 本 APP 之使用權不得轉讓、出借或過繼給第三方，也不得以繼承或擔保抵押之方式提供給第三方。
（聯絡方式）

本報告之智慧財產權屬於國家通訊傳播委員會

第 14 條 使用者如因本 APP 使用之相關事宜而需要聯絡厚生勞動省，請參考登載於本 APP 內或厚生勞動省的新冠肺炎感染對策相關網站內之聯絡方式，按照厚生勞動省所指定之方法進行聯絡。

（法律依據以及協議管轄）

第 15 條 關於本使用規則以及本 APP 之使用所有事項，均以日本國之法律為依據。

2 對於起因於本 APP 之使用或與本 APP 相關之厚生勞動省與 APP 使用者之間之一切糾紛，均以東京地方裁判所為一審專屬協議管轄法院。

本報告之智慧財產權屬於國家通訊傳播委員會

附錄8：日本新冠肺炎密切接觸者應用程式隱私保護方針

【2020 年 12 月 15 日　隱私保護方針修訂通知】

接觸確認 APP 以往採取之機制是：如某位使用者登記為陽性者，則會通知過去 14 天內可能與其有過接觸之其他使用者。為了配合保健所正在積極展開之流行病學調查，厚生勞動省從與流行病學調查保持吻合性之視角出發，開始發布 APP 修正版，改為由確認為陽性之使用者將其發病日或檢查日輸入到接觸確認 APP 中，並通知在改日期的約 2 天前以後（感染可能期間內）有可能與該陽性者有過接觸的使用者。為此，營運方對隱私保護方針做了修訂。主要變更點如下：

・明確註明，接觸確認 APP 之運行機制改為：陽性者需要在受理編號之基礎上輸入發病日或檢查日，並向通知服務器發送其約 2 天前以後（感染可能期間內）所生成之日更密鑰，從而通知在感染可能期間內與該陽性者有過接觸之 APP 使用者。

・明確註明，在厚生勞動省使用接觸確認 APP 所獲取之訊息中，只包括在感染可能期間內所生成之日更密鑰。

・厚生勞動省還明確表示，不會獲取陽性感染者在接觸確認 APP 中輸入之發病日或檢查日，並將其提供給其他之 APP 使用者。

○接觸確認應用程序隱私保護方針

厚生勞動省在提供接觸確認應用程序（以下簡稱「本 APP」。）之過程中，應遵守其所適用的法律法規，最大限度地保護使用者之隱私，依據如下保護方針提供服務。

1 本 APP 之運行機制

①在 APP 使用者（係指透過本 APP 使用本 APP 所提供之服務者。下同。）之已安裝 APP 之終端（係指安裝有本 APP 之智慧手機終端。下同。）上自動生成並記錄日更密鑰（與該終端具有一對一的對應關係，在已安裝 APP 之終端中以 24 小時為單位變更之識別碼。下同。）。

②在 APP 使用者之已安裝 APP 之終端上自動生成並記錄接觸符號（基於日更密鑰所生成的，在已安裝 APP 的終端中以 10 分鐘為單位變更的識別碼。下同。）。

③APP 使用者以及處於接近（在大約 1 米以內的距離保持 15 分以上的近距離接

本報告之智慧財產權屬於國家通訊傳播委員會

觸的可能性較高的狀態。下同。）狀態的其他 APP 使用者各自啟動其已安裝 APP 的終端的藍芽功能時，則使用藍芽功能，(i)將自身之已安裝 APP 的終端上所生成並記錄的接觸符號，自動提供給處於接近狀態下的其他 APP 使用者的已安裝 APP 的終端，並進行記錄，(ii)將該其他 APP 使用者的已安裝 APP 的終端上所生成並記錄的接觸符號自動提供至自身的已安裝 APP 的終端中，並進行記錄。

④APP 使用者在查明自身為陽性者（確診新冠肺炎感染為陽性者。下同。）之情況下，如希望在 APP 中登記為陽性者，則執行如下事項：(i)將（A）在管理系統上（為了對新冠肺炎的陽性者以及密切接觸者的訊息進行管理，而由厚生勞動省進行營運，用於都道府縣以及設置保健所的市，對於新冠肺炎感染者等訊息進行掌握和管理的支援系統下同。）另行登錄之自身手機號碼或電子郵件所接收到之受理編號（在查明某位 APP 使用者為陽性者的情況下，由管理系統向該 APP 使用者隨機發行，進行通知的任意臨時編號。下同。）以及(B)該陽性者有新冠病毒感染症狀的情況下則將其發病日，沒有新冠病毒感染症狀的情況下則將其檢查日（發病日或檢查日之約 2 天前以後稱為「感染可能期間」。）輸入到自身之已安裝 APP 之終端，從而(ii)該已安裝 APP 的終端經由通知服務器（由厚生勞動省進行管理之具有如下功能的服務器：與已安裝 APP 的終端進行協作，讓 APP 使用者可以在同意必要事項的基礎上對從終端上登錄的日更密鑰進行管理，並在一定的條件之下將該日更密鑰提供給其他 APP 使用者之已安裝 APP 之終端。下同。）前往管理系統查詢，確認所輸入之是否確為發行給該陽性者的受理編號，然後(iii)管理系統回答通知服務器，所查詢的受理編號是否確為發行給該陽性者之受理編號。

⑤相關查詢的結果，如管理系統回答所查詢的受理編號確為發行給該陽性者之受理編號，則記錄於該陽性者自身的已安裝 APP 的終端上之日更密鑰（僅限在該陽性者的感染可能期間內所生成之日更密鑰。）可以經由通知服務器自動提供至其他使用者的已安裝 APP 的終端上，該其他使用者在其已安裝 APP 的終端上最多可自動追溯搜索過去 14 天內該其他使用者的已安裝 APP 的終端內所記錄的接觸符號，如查明存在符合接觸狀態（在大約 1 米以內的距離保持 15 分以上之接近狀態。下同。）之接觸符號記錄，則該其他使用者之已安裝 APP 之終端會收到可能與不特定之處於感染可能期間內之陽性者有過接觸之通知。

2 厚生勞動省透過本 APP 會獲取以及不會獲取之訊息

本報告之智慧財產權屬於國家通訊傳播委員會

(1) 厚生勞動省會獲取的訊息

・厚生勞動省會透過本 APP 獲取如下所示之訊息。

①在上述 1④的流程中所獲取的陽性者之受理編號

②在上述 1⑤的流程中所獲取的陽性者之日更密鑰（僅限在該陽性者之感染可能期間內所生成之日更密鑰。）

③上述 1 中之改善本 APP 所需的程序運行訊息（包括本 APP 所受理的內容、受理時間、受理是否成功、受理過程中所參考之訊息、作為受理結果之輸出訊息、受理時之狀態，但是不包括受理編號、日更密鑰和接觸符號。）以及本 APP 之運行環境相關訊息（包括 COCOA APP 之版本、何種 OS、OS 之版本、設備機種，以下與 APP 運行訊息並稱「運行訊息」等。）

(2) 厚生勞動省不會獲取之訊息

・厚生勞動省不會透過本 APP 獲取如下所示之訊息：(1)所記載之訊息之外之訊息（包括但不限於如下所示的訊息。）。

・厚生勞動省不會透過本 APP 從 APP 使用者處獲取其姓名、出生年月日、性別、住址、電話號碼、電子郵件、終端位置訊息等可識別 APP 使用者個人身分的訊息，以及能夠識別 IP 地址、MAC 地址、主機名以及其他之可識別安裝 APP 之個別終端之訊息。

・接觸符號將分別在 APP 使用者各自持有的已安裝 APP 之終端內以加密之狀態進行記錄，包括 APP 使用者在內之任何人都無從得知已安裝 APP 之終端之間之接觸性格訊息，厚生勞動省也不會獲取該訊息。

・厚生勞動省不會透過本 APP 獲取可識別陽性者個人身分之訊息。為此，厚生勞動省在獲得陽性者同意之基礎上獲取與該陽性者之間過去 14 天內與處於感染可能期間內的該陽性者之間的接觸的相關訊息後，其他 APP 使用者透過本 APP 接收通知時，不會向該接收通知者提供可識別該陽性者個人身分之訊息。此外，厚生勞動省也不會獲取 1④(i)(B)中所輸入的發病日或檢查日，並將其提供給其他的 APP 使用者。

・對於透過本 APP 接到通知可能與處於感染可能期間內之陽性者有過接觸者，厚生勞動省也不會獲取可識別其個人身分之訊息。為此，厚生勞動省也不會透過本 APP 向該陽性者提供可識別接收通知者個人身分之訊息。

・厚生勞動省不會透過本 APP 獲取接到可能與處於感染可能期間內的陽性者有

本報告之智慧財產權屬於國家通訊傳播委員會

過接觸之通知之其他 APP 使用者與該陽性者之間之對應關係以及接觸日期等相關訊息。

3 厚生勞動省透過本 APP 所獲取之訊息之使用目的以及使用方法

(1) 受理編號

・厚生勞動省為避免非陽性者在本 APP 中謊稱陽性，將會使用在 2(1)①中所獲取之陽性者受理編號。換言之，所採用之運行機制如下：新冠肺炎為陽性之 APP 使用者在本 APP 中將其自身登記為陽性時，管理系統會向該陽性者發行受理編號並進行通知，陽性者在已安裝 APP 之終端上輸入受理編號後，厚生勞動省之通知服務器所獲取之受理編號將用於通知服務器向管理系統查詢所輸入之受理編號是否為向該陽性者發行之受理編號，確認該受理編號確為向該陽性者發行之後方可完成陽性者登記。

・厚生勞動省不會將所獲取之受理編號用於原本目的之外之其他用途。在確認所輸入受理編號是否為向該陽性者發行之受理編號之後，將立即在 APP、通知服務器以及管理系統中分別刪除該受理編號。

(2) 日更密鑰

・為了通知其他 APP 使用者其可能在 14 天內與處於感染可能期間內之陽性 APP 使用者有過接觸，厚生勞動省會使用其所獲取的 2(1)②中所記載的陽性者之日更密鑰（僅限在該陽性者的感染可能期間內所生成的日更密鑰。在本(2)中下同。）。換言之，採用如下之運行機制：陽性 APP 使用者之陽性登記完成之後，厚生勞動省之通知服務器所獲取之該陽性者之日更密鑰將會提供至其他 APP 使用者之已安裝 APP 的終端中，該終端內所記錄之接觸符號自動檢索之結果，如存在符合接觸狀態之接觸符號，該其他 APP 使用者會接到可能與處於感染可能期間內的陽性者有過接觸的通知。

・在陽性 APP 使用者希望登記為陽性的情況下，厚生勞動省將事先在本 APP 上針對如下事項獲得其明確之同意如下事項：(a)向其他 APP 使用者的已安裝 APP 的終端提供記錄於自身的已安裝 APP 的終端中的日更密鑰，並且，(b)如其他 APP 使用者在感染可能期間內與自身有過接觸狀態，則在不提供可識別該陽性者個人身分的訊息的前提下，通知對方其可能與不特定的處於感染可能期間內的陽性者有過接觸。

・厚生勞動省所獲取的日更密鑰用於原有目的之外不用於其他用途。所有之日更

本報告之智慧財產權屬於國家通訊傳播委員會

密鑰（包括該陽性者在其感染可能期間之外所生成的日更密鑰。）在其生成於已安裝 APP 的終端的 14 天後自動失效。

(3) APP 運行訊息等

・為了以 APP 使用者所傳送的本 APP 故障可能性等的相關訊息為基礎，迅速對本 APP 進行改善，厚生勞動省會用到 2（1）③中所記載的 APP 運行訊息等。

・除非 APP 使用者感覺到本 APP 可能存在故障，並主動傳送 APP 運行訊息等，否則厚生勞動省不會獲取 APP 運行訊息等。

・如果已經傳送了 APP 運行訊息等之 APP 使用者還希望進一步自發性地協助本 APP 的故障調查，則可以透過電子郵件，向 6 中所記載之客戶服務台發送 APP 運行訊息 ID（針對 APP 運行訊息等而生成的隨機號碼，用於與所諮詢事宜以及 APP 運行訊息等建立關聯的符號。）。厚生勞動省會利用 APP 運行訊息 ID，將在郵件服務台所受理的諮詢內容和 APP 運行訊息等進行關聯管理。在進行訊息管理時，厚生勞動省會在本 APP 上預先獲得使用者之明確同意。

・厚生勞動省不會將 APP 運行訊息等用於原本使用目的之外之其他用途。在該 APP 運行訊息等所涉及之故障調查結束後，會立即從服務器上刪除 APP 運行訊息等。

4 同意之撤回與記錄之刪除

・本 APP 使用之相關同意，可以透過在已安裝 APP 之終端中刪除本 APP 之方式進行撤回。APP 使用者透過上述的方法撤回同意的情況下，則記錄已安裝 APP 的終端內的所有的 APP 使用者相關訊息也隨之全部刪除，無法復原。

・記錄於已安裝 APP 的終端上的與其他 APP 使用者之間的接近訊息（記錄於其他 APP 使用者的已安裝 APP 的終端中的接觸符號）在記錄時會進行加密，並在 14 天後自動失效。

・記錄於安裝 APP 的終端中的運行訊息，將在其生成的 14 天後自動刪除。

5 APP 使用者訊息的管理

・各安裝終端的接近相關訊息，僅在該安裝終端內進行管理，不會向安裝終端的外部進行提供。

・在本 APP 的系統的營運過程中，除 3（3）中所記載的 APP 使用者明確同意之情況外，厚生勞動省將會對所處理之數據採取適宜的訊息安全對策，不會透過本 APP 以外之系統（包括但不限於管理系統）去確認、校驗國家或地方公共團體所

本報告之智慧財產權屬於國家通訊傳播委員會

管理之能識別特定個人之訊息，並由此去識別 APP 使用者之個人身分。

・為了使透過本 APP 之外之其他系統等（包括但不限於管理系統。）不與日本國家政府或地方公共團體所管理之可識別個人身分之訊息進行查詢比較，來識別 APP 使用者之個人身分，厚生勞動省在本 APP 之系統營運中，將針對所處理之數據採取適宜之安全管理措施。將本 APP 之系統營運部分外包時，也會要求承包方採取適宜的安全管理措施。

6 郵件服務台和呼叫中心

・為了受理涉及本 APP 的使用者諮詢和協商，厚生勞動省設置了郵件服務台和呼叫中心。

・對於透過郵件服務台和呼叫中心所獲取的包含郵件地址和電話號碼在內之訊息，厚生勞動省僅將其用於回答使用者之諮詢或協商（包括調查該諮詢或協商所涉及之相關故障等。）。

7 向第三方提供

・在未經本 APP 使用者明確同意之情況下，厚生勞動省不會向第三方提供透過本 APP 所獲得之訊息以及透過郵件服務台和呼叫中心所獲取之訊息。

8 業務委托

・厚生勞動省可能將本 APP 以及郵件服務台和呼叫中心之全部或部分業務委托給第三方（不僅包括厚生勞動省之直接業務委托，還包括該業務受委托方所進行之二次委托。），並由該受托方負責處理透過本 APP 或透過郵件服務台和呼叫中心所獲取之訊息。此種情況下，厚生勞動省會對該受托方進行管理和監督，敦促其採取適當的安全管理措施。

・與厚生勞動省有業務委托關係，並且會處理透過本 APP 或透過郵件服務台和呼叫中心所獲取的訊息的受托方的詳細訊息，厚生勞動省將在接觸確認 APP 的網頁上進行公開。

9 個人隱私問題之諮詢方式

・本 APP 使用過程中涉及到個人隱私的相關問題之訊息，將登載於本 APP 內或厚生勞動省之接觸確認 APP 相關網站內，請向厚生勞動省指定之諮詢窗口進行諮詢。

本報告之智慧財產權屬於國家通訊傳播委員會

附錄9：日本 KDDI 個人隱私政策摘要

KDDI 公司意識到個人資料保護之重要性，將遵循電信通訊事業法、個人資料保護法、My number 法等，與其他本公司業務進行相關之法律。以及個人資料保護法指引（通則篇、確認紀錄義務篇、向外國第三方提供篇、匿名加工資料處理篇）、電信通訊事業個人資料保護指引，與其他本公司業務相關等指引，對個人資料依以下方式處理。

1. 以適當且公正之方式處理所獲得之資料，

•所獲得之資料範圍包含：

(1)由客戶所提供之書面、Web，與口頭資料。

(2)客戶在使用服務過程中所產生之 Cookie、Web beacon，與廣告用之識別碼等資料。

(3)自公共機關獲得之資料。

(4)由電話簿、官報，與各種已公布之資料中所獲得之資料。

(5)自日本信用資訊機構（如 JICC）所獲得資料。

(6)其他因客戶介紹等，自第三方合法獲得資料。

2. 在遵守使用範圍前提下 ，KDDI 公司與其關係公司，得相互使用所持有之資料

•資料利用範圍包含：

(1)客戶同意。

(2)依法令。

(3)為保護本人生命、身體或財產之情形，而取得本人同意有困難之時。

(4)為提升公共利益或維護兒童身心健全發展，而取得當事人同意有困難時。

(5)協助國家機關或地方公共團體或受其委託者執行法令所規定之事務，基於取得本人同意有可能對執行該事務造成阻礙的之虞時。

在各事業領域，為達成其服務與業務之使用目的必要範圍內所利用資料，係屬得在 KDDI 公司與其關係公司間相互使用之資料。

3. 若已達到利用目的，或未達利用目的但該目的業務終止，即應刪除所保留之個人資料，惟 KDDI 公司於契約終止後，仍得於利用目的範圍內利用個人資

本報告之智慧財產權屬於國家通訊傳播委員會

料。

4. KDDI 公司於變更前之目的具關聯、合理性之情況下得變更利用目的， 惟需將變更目的通知本人並公布。

5. 對匿名加工資料之適當處理

(1)KDDI 公司處理匿名加工資料時，必須採取無法識別出特定個人，以及無法復原個人資料之必要措施。

(2)此外，公司於使用匿名加工資料時，不得以識別（再識別）原先個人資料之本人身分為目的進行個人資料核對。

(3)處理匿名加工資料時，須依法令公布包含匿名加工資料之個人相關項目。

(4)KDDI 公司將匿名加工資料提供給第三方時，須依法令公布第三方提供包含匿名加工資料之相關個人資料與項目，並對該第三方明確表示所提供之資料為匿名加工資料。

6. 向外國第三方提供資料時應遵循法令，並取得同意等必要措施。

7. 對個人資料管理應實施適當安全管理措施。

•技術保護措施

•組織保護措施

(1) 對員工（包含派遣人員）進行監督。

(2) 對接受個人資料處理委託業務業者進行監督。

8. 須提供不希望收到廣告訊息之用戶，取消收受訊息之申請管道。

9. 在客戶本人與其代理人之要求揭露、更正，或要求利用目的之通知下，須即時做出應對措施。

10. 對個人資料之相關諮詢，須適當且迅速地做出應對措施。

•本公司會為客戶提供個人資料修改（包含修正、追求、刪除或停止向第三方提供資料）之諮詢窗口。

•本公司就客戶本人或其代理人對利用目的為通知之請求，除以下各款之情況外，須迅速進行通知：

(1) 就該識別本人之個人資料利用目的明確之情況

(2) 有侵害本人亦或第三人之生命、身體、財產與其他權利利益之虞時。

(3) 有侵害本公司權利亦或正當利益之虞時。

(4) 協助國家機關或地方公共團體或受其委託者執行法令所規定之事務，為

本報告之智慧財產權屬於國家通訊傳播委員會

使該事物得順遂進行。

●本公司須迅速適當處理客戶對個人資料利用、提供、揭露與修正等與個人資料處理相關之客戶投訴。

本報告之智慧財產權屬於國家通訊傳播委員會

附錄10： 日本 NTT Docomo 個人資料憲章

NTT Docomo 個人資料憲章 -革新創造行動準則-

本公司 NTT Docomo 秉持「創造出新型溝通文化世界」之企業理念，以實現前所未有的繁榮未來，持續挑戰各種革新型創新活動。我們心目中的創新，意味著銜接所有生活相關的事物，為客戶提供舒適的生活並造就更多感動，同時為目前社會面臨的各種難題找到新的解決方案，為全國各地，甚至跨世代的所有人創造更繁榮且更舒適的生活。我們率先為每一位顧客提供安心與安全、健康、學習等服務，甚至包括日常生活中的各種樂趣，除了提供最適合個人的資訊之外，也為客戶帶來難以言喻的喜悅。同時，我們備有最完整的體制來因應各種不同的商業改革，也能進一步解決社會問題。

我們不甘滿足於現況，在追求與配合社會需求的同時，我們也顧慮要與顧客同步創造出未來的願景。我們的願景是透過活用顧客的個人資料以及所有相關資料，進一步取得可造就各種智慧的人工智慧等技術，繼而從資料中衍生新的價值，再將這些附加價值回饋給顧客以及社會。

同時，本公司 NTT Docomo 在運用顧客重要的個人資料時，除勢必遵守相關法令外，另一個重要使命乃為保護顧客隱私權，肩負起顧慮並實踐對顧客相關隱私權之防守任務。有一些顧客對於我們運用個人資料可能或多或少會感受到不安與疑慮。我們將秉持過往的強烈信念，在不辜負顧客信任的前提下，持續提供顧客安心及安全感，並負起最大責任處理所有顧客的個人資料。我們將持續把與客戶間的"羈絆"視為最重要的一環，誠摯傾聽顧客的意見，運用資料為顧客與社會創造出新的價值，同時持續思考最適用於保護每位顧客隱私權的方式，並不斷地將這個理念傳達給每位顧客。

為了實現「運用資料為顧客與社會持續提供新價值」以及「提供給每位顧客最適切的隱私權保護」，我們在進行所有企業活動時，將以下揭露的行動準則視為所有經手顧客個人資料時應遵循的原則。

何謂個人資料

我們認為考量到隱私權而應處理的資料不限於「個人資料保護法」所規定的個人資料內容。該行動準則規定對象中的「個人資料」當然也包括個人資料保護法定義的個資，但同時還應包括「機器與瀏覽器使用的 ID
等可識別個人相關的所有資料」。例如，我們透過「某人」使用特定機器，取得使用該機器之歷史資料時，即使無法具體辨識使用該機器的個人，也應該將透過此方式取得的資料視為行動準則規定的對象，一併定義為「個人資料」。

行動準則

◆重視與顧客間的溝通，確保準則的透明度

- 必須讓顧客理解個人資料是如何取得、將如何被運用，以確保相關資訊透明度。

本報告之智慧財產權屬於國家通訊傳播委員會

●取得及運用個人資料時，需要以重點或影像等簡單明瞭的方式向顧客說明，以顧客便於理解的方式呈現。

●同時需排除顧客內心的不安與疑問，為了讓客戶能更安心，也需要進一步優化溝通的管道。

♦思考顧客本身的利益與對社會的回饋

●透過運用個人資料，提供顧客與社會新的價值。

●在運用個人資料的同時，需考慮是否能造就顧客利益或社會回饋，以不損害顧客信任為前提使用資料。

●需以適切合法的方式，同時顧慮顧客的感受，取得並運用個人資料。

♦尊重每一位顧客的意願

●對於個人資料使用方式的感受因人而異，需顧慮每位顧客的差異，因應使用的個人資料性質與運用型態，提供顧客能自行決定是否提供個人資料的方式（如選擇退出 opt out 方式等）。

●選擇的方式需盡量以簡單明瞭的方式呈現。

♦與合作夥伴配合時也需考慮顧客的隱私權

●為了提供顧客與社會新的價值，在與合作夥伴搭配進行開放式創新活動時，需考慮將提供給合作夥伴的個人資料匿名化、做成統計資料，除了需遵循法令，也需考慮顧客的隱私權。

●提供資料給合作夥伴時，需因應提供資料的性質，確認資料來源的可信度，並向資料提供來源端限制資料的使用或提供，採取相關適切的方式保護顧客隱私。

♦採取適切的資訊安全對策保護顧客個人資料

●為預防顧客重要個人資料遭外洩或竊取、竄改等意外，需要採取適當的組織型、人為、物理、技術型方式保護顧客資料。

●定期執行資訊安全相關評估，實施降低資訊安全風險的對策。

♦整頓並運用保護顧客隱私權的體制

●我們會秉持隱私納入設計的理念，在開發新產品及服務的同時，顧慮顧客隱私權。

●為徹底考量隱私權，我們將向經手處理顧客個人資料的員工，實施公司內部研修與教育啟發訓練，並持續與相關人員共享這些資訊。

●同時，我們於公司內部設有評估隱私權影響度的專門諮詢機關，評估使用個人資料時對顧客隱私權有何種程度的影響，整頓並運用相關部門與機制。

※為了持續取得客戶信任，我們將持續驗證行動準則的內容及使用，並視狀況適當修改準則內容。

本報告之智慧財產權屬於國家通訊傳播委員會

附錄11： 日本 NTT Docomo 隱私政策

NTT Docomo 株式會社（以下稱為「本公司」。）為提供各種服務以提升顧客生活舒適度，將取得顧客個人資料（不限於個人資料保護法規定內容，包括所有攸關個人資料之所有資料）進行運用。故本公司在進行事業活動時，需肩負起慎重適當運用個人資料之重要使命，主動闡述相關理念，執行紀律，是故揭露「NTT Docomo 個人資料憲章」。

本公司遵循「NTT Docomo 個人資料憲章」，制定本隱私權政策，明訂顧客個人資料處理相關方針。

在本隱私權政策中，我們將闡明「本公司如何處理顧客個人資料」「顧客可如何管理個人資料」等內容。為了簡單明瞭且具體地將這些內容傳達給所有顧客，我們也公告了「知識促進理解！運用 Docomo 個人資料」這份資料，還請一併參考。

1. 適切處理個人資料

本公司在處理個人資料時，嚴守國內外適用法令及指引，持續精進隱私權政策，致力於讓顧客可取得方便、安心且安全的服務。同時，本公司以公正的方式取得個人資料，在整頓適切的公司管理體制與公司規程同時，也定期對員工進行必要之教育訓練。

2. 取得個人資料

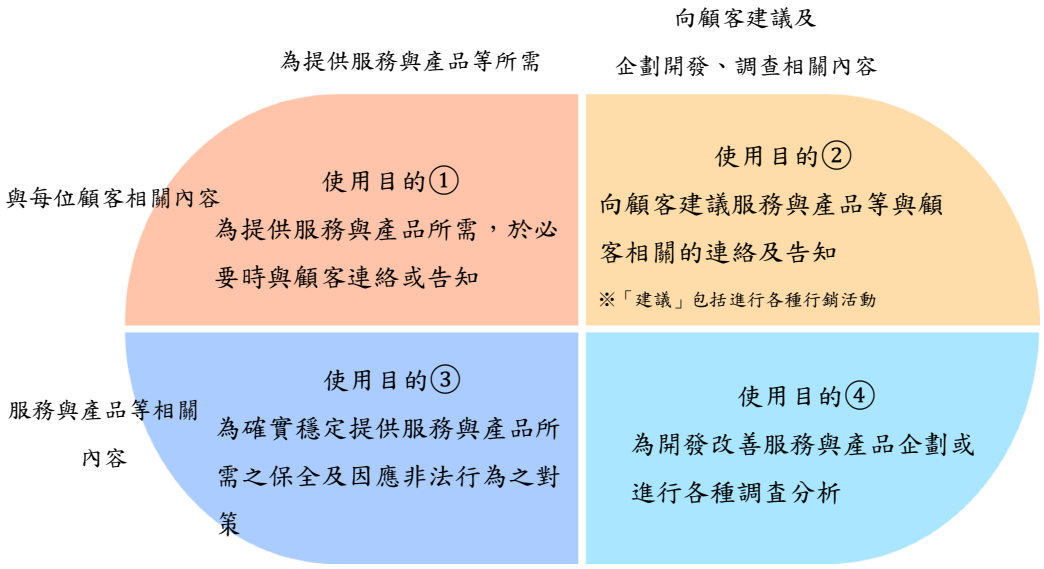
本公司透過以下方式取得個人資料。

- 顧客親自將個人資料傳達給本公司
  本公司透過顧客於 Docomo 店面以書面方式填寫個人資料，或透過顧客於手機等畫面登錄、送出等方式取得個人資料。
- 顧客使用本公司服務時，自動記錄個人資料
  使用本公司服務時，透過本公司伺服器自動記錄顧客的使用紀錄，依手機終端設定自動將終端記錄的資訊傳送給本公司。
- 顧客使用非本公司服務時，本公司間接取得個人資料
  顧客於店家購物時，使用 d 點數等方式取得非本公司之服務時，本公司可同時取得顧客購物及使用相關服務等歷史資訊。

3. 個人資料使用目的

(1) 本公司為達以下使用目的，需就必要範圍運用個人資料。

本報告之智慧財產權屬於國家通訊傳播委員會



- 為提供服務與產品所需，於必要時與顧客連絡或告知

舉例包含以下使用目的。

- 依簽約內容提供各種服務及功能並實施其他合約內容
- 申請及使用服務時，需確認申請者為本人或家人
- 確認申請條件是否吻合
- 為進行徵信*調查與徵信後管理

  * 指電信公司需針對使用顧客之過去使用歷史紀錄查詢是否有不良紀錄等，進行調查。
- 為計算請款金額（包括代收費用）與進行請款、點數管理
- 為處分向顧客取得之債權與權利、抵押品與其他交易
- 為使用判斷年齡相關服務，通知顧客年齡時
- 為通知顧客合約相關之必要事項
- 為處理、配送顧客下單產品及提供售後服務
- 發生非法簽約、非法使用及未付款問題時，與顧客連絡
- 為因應顧客對服務內容之意見、要求及諮詢等內容

- 向顧客建議服務與產品等與顧客相關的連絡及告知

舉例包含以下使用目的。

- 顧客諮詢資費方案時，提供顧客適切的資費方案訊息
- 為了通知顧客本公司、合作夥伴及加盟店等的各種活動與其他促銷活動
- 各種活動與其他促銷活動舉辦之抽獎活動，通知中獎人、發送贈品與謝禮及其他通知
- 為了向客戶推薦產品與服務及行銷內容
- 為了向顧客提供或發送適合顧客之本公司及其他公司廣告
- 為了贈送與提供本公司及關聯子公司、採權益法持有之公司及ｄ點數加盟店可使用的折價券等優惠
- 提供本公司判斷為適當的各種產品與服務、活動、行銷相關資訊及廣

本報告之智慧財產權屬於國家通訊傳播委員會

告發送（包括本公司以外的第三方）

- 為確實穩定提供服務與產品所需之保全及因應非法行為之對策

舉例包含以下使用目的。

- 為運用暨維修網路、應用程式、系統等
- 為預防產品與服務、網路、應用程式、系統等發生障礙、故障與事故及發生時的因應對策
- 預防非法簽約、非法使用、未付款問題以及發生時的因應對策

- 為改善並開發各種服務與產品等企劃，進行各種調查與分析

舉例包含以下使用目的。

- 為開發新產品、新服務、新技術企劃
- 為改善服務品質、提升相對應服務
- 為調查分析販售狀況及使用狀況
- 為調查顧客對於產品與服務及各種促銷與其他行銷策略的態度與實際銷售狀況(不限於本公司，合作夥伴，加盟店等產品)
- 調查分析並衡量各種促銷與其他行銷策略效果
- 為實施問券調查
- 為調查本公司產品與服務的銷售與使用狀況、本公司產品與服務之運用與改善，企劃新產品及新服務，進行問券調查與分析其他市調資料

此外，若顧客同意本公司另行制定的「所在位置資料使用」事項，將在達成如下使用目的之範圍內使用所在位置資料。

- 為了贈送本公司及關聯子公司、採權益法持有之公司及 d 點數加盟店可使用的折價券等優惠，發送並提供本公司判斷為適切之各種產品與服務、行銷、活動（包括本公司以外之第三方）相關訊息
- 調查分析本公司產品與服務之販售及使用狀況，為提升本公司產品與服務之運用，企劃新產品與新服務，進行問券調查與分析市調資料

※ 若顧客欲停止同意本公司依上述使用目的使用位置資料，請於顧客個人資料資料儀表板進行變更設定。在變更設定生效前取得之位置資料還是有可能被使用，敬請知悉。

※ 不管顧客是否同意上述內容，本公司遵循提供電信服務所需之範圍內，在法令許可的範圍下，依個別服務、應用程式等內容徵詢顧客同意，取得並使用顧客所在位置資料。此外，若需停用個別服務、應用程式獨立使用所在位置資料時，請依照個別服務，應用程式指定的方式執行停用。

(2) 本公司不會以如下方式運用個人資料。

- 判斷是否提供服務給顧客時，對客戶有不當的差別待遇。

(3) 本公司在終止提供顧客服務合約後，也可能持續使用顧客個人資料。

(4) 本公司因受其他業者委託，為執行業務而使用個人資料時，將在執行該業務所需之範圍內使用個人資料。

本報告之智慧財產權屬於國家通訊傳播委員會

4. 個人資料處理相關同意

本公司在使用個人資料或將個人資料提供給第三方時，會事先取得顧客同意。雖然本公司有可能在法令許可範圍下，為了3(1)揭露內容以外的目的，未經顧客同意就將顧客個人資料提供給第三方，但在這個狀況下勢必充分顧慮顧客權益。

為了避免顧客因同意各種事項，最終搞不清楚自己究竟同意了甚麼內容，本公司會將顧客同意過的主要事項羅列於「個人資料資料儀表板」，讓顧客能自行確認。

5. 顧客個人資料管理

若顧客不同意本公司使用個人資料或提供給第三方，可就一定範圍進行表示。顧客目前表示的內容請透過「個人資料資料儀表板」確認。

顧客要求公開本公司所持有之個人相關資料的程序，請參考「個人持有資料相關申請程序等」內容。

6. 個人資料之安全管理

本公司為讓顧客安心使用服務，揭露資料資訊安全相關方針，聲明「資料資訊安全政策」。本公司為預防個人資料外洩、遺失、毀損及進行個人資料安全管理，採取必要且適當的措施。

7. 委外處理個人資料

本公司就販售與受理業務、故障維修業務、費用與徵信相關業務、網頁與系統營運業務、活動與行銷等實施業務、資料加工與分析業務及其他業務內容，有可能將個人資料局部或全部委外處理。本公司將選擇會妥善處理個人資料的廠商，執行確切的監督管控。

8. 公告個人資料處理相關其他事項

若本公司有需告知有關共同使用個人資料及匿名加工資料之處理方式及其他公告事項時，將隨時揭露於「個人資料處理相關其他事項公告」。

9. 與個人資料相關處理方式之諮詢

有關本公司處理個人資料相關疑問請洽以下諮詢窗口。

- NTT Docomo 株式會社　客服諮詢室
  0570-073-030（收費）　　營業時間：上午 10 點～下午 6 點（週六、週日、國定假日及過年期間不營業）

同時，本公司隸屬以下個人資料保護團體業者。針對以下事業經手的個人資料處理進行訴願及諮詢等內容，可直接與相關事業窗口聯絡。

- 電信通訊事業相關窗口

  一般財團法人日本資料通訊協會電信通訊個人資料保護推廣中心
  https://www.dekyo.or.jp/kojinjyoho/

- 信用卡事業相關窗口

  一般社團法人日本信用卡協會
  03-5645-3360（收費）

2019 年 12 月 11 日

本報告之智慧財產權屬於國家通訊傳播委員會

附錄12： 日本 NTT Docomo 行動空間統計指引

1. 本指引目的

本指引的目的在於製作與提供行動空間統計數據時應遵循的基本事項。

2. 術語定義

本指引使用的術語及意思定義如下。

行動空間統計

透過提供電信通訊服務過程中取得的使用數據是以建構與整頓社會數據基礎為目的統計出來的，且經過個人數據去識別化處理。以公共領域、學術研究領域、產業等領域作為數據提供來源，對局部使用數據的位置與屬性進行去識別化處理、統計處理以及隱匿處理。

使用數據

此為透過提供電信通訊服務過程中取得的數據總稱，包含位置與屬性數據。

位置數據

為局部使用數據，為顯示手機等所在位置的數據，包括數據產生的時刻等相關附加數據。

屬性數據

為局部使用數據，運用電信通訊服務時，透過用戶提供的數據及漫遊等資訊取得國碼的數據。

去識別化處理

處理使用數據中的姓名、電話及生日等可識別對象的資訊，刪除可識別數據，包括將數據數值四捨五入或者變換成不可逆編碼。

去識別化資料

意指經去識別化處理取得的資料。

統計處理

此為透過去識別化資料進行統計推測，引導出統計型「集團相關數據」的處理，包括人口分布推算、移動人數推算、性別與年齡層等依不同屬性推算人口結構數量等內容。

統計結果

經統計處理取得的數據。

隱匿處理

讓統計結果排除少數偏差數值的數據。

3. 製作與提供移動空間統計相關基本原則

(1)行動空間統計需遵循第 4 項及第 7 項規定的製作程序，製作出無法特定出電信通訊服務使用者個人的統計數據。

(2)行動空間統計數據需依第 8 項規定的提供方針提供。

本報告之智慧財產權屬於國家通訊傳播委員會

4. 製作行動空間統計數據的程序

(1)行動空間統計需經過將使用數據去識別化處理、統計處理及隱匿處理來完成。

(2)行動空間統計提供的數據意指已完成上述三個處理階段的數據。

(3)製作行動空間統計數據時，視為將自動處理上述三個階段，運用的系統須遵循公司內部相關規章進行管理。

5. 去識別化處理

(1)去識別化處理除了排除姓名、電話及生日等可識別的數據以外，同時需結合密鑰形成不可逆編碼*。

(2)產生上述統計處理用不可逆編碼時，為了預防由不可逆編碼還原回可識別數據，需要使用安全的單向函數。

(3)上述單向函數包含依循國內外評估專案及評估機關*2 推薦的雜湊函數*3，採用加密雜湊函數*4。

(4)加密雜湊函數相關密鑰*5 需要採取嚴格的運用控管體制，包括內部密鑰管理者區分等制度。

*1.由某輸入數據所產生的符號，具有無法逆向演算回原本數值的特性。

*2.例如，國內加密技術評估專案 CRYPTREC 或美國國立標準技術研究所（NIST）等。

*3.無法從輸出文字列取得輸入文字列之具單向特性的函數之一。是將任意長度的文字列變換成固定長度文字列的函數，具有對同一個輸入值產生相對應的同一文字列輸出特性。

*4.雜湊函數的一種，透過函數處理採用加密密鑰，可更進一步提高安全性。

*5.使用密鑰雜湊函數處理之電子型參數。

6. 統計處理

(1)統計處理是透過蒐集去識別化資料，以統計方式來推算人口分布、移動人數、性別與年齡層等具不同屬性的人口數據。

(2)統計處理取得的結果不包括第 5 項統計處理之不可逆編碼內容。

7. 隱匿處理

(1)隱匿處理需排除統計結果取得的少數偏差值。

(2)需參考過往公家機關統計採用的案例與國內外技術開發動向，就統計結果有效性與預防可特定出個人的觀點，採取適切的方式實施隱匿處理。

8. 提供移動空間統計

(1)提供行動空間統計數據時，需要制定使用目的。訂定提供數據等條件時，需留意是否違反公序良俗。

(2)需根據個案決定提供行動空間統計數據之公開與二次提供數據的合約條款。

9. 員工與委外廠商之管理措施

(1)製作行動空間統計及相關組織的提供數據管理負責人（以下稱為管理負責人。）需要適當監督控管處理行動空間數據的員工，督導員工是否有

本報告之智慧財產權屬於國家通訊傳播委員會

遵循本指引進行安全管理。

(2)委外製作行動空間統計數據或將相關業務委任給外部時，管理負責人需對其行動空間統計數據進行安全管理，同時也需對委外廠商進行適當的監督。

10. 停止使用使用數據的程序

(1)顧客若申請停用行動空間統計使用數據時，需終止對該顧客之服務。

(2)若顧客同意重啟使用相關數據，則顧客在經營運方許可後，可再次使用與該顧客相關的行動空間統計數據。

(3)停用以及重啟使用數據等程序，從申請到反應於系統生效，需要幾天的時間。

本報告之智慧財產權屬於國家通訊傳播委員會

附錄13： 韓國大數據個人情報保護準則

「빅데이터 개인정보보호 가이드라인」 전문

「大數據個人情報保護準則」全文

主管機關：韓國放送通信委員會（방송통신위원회）

發布年月：2014 年 12 月 23 日

翻譯說明

一、 為便於台灣讀者易於閱讀及理解,本報告將盡可能與我國著作權法用語統一，並放棄信雅達原則，惟在不影響閱讀下，部分法律專門用語於翻譯時保留。

二、 韓國法律條文書寫方式如列:單項次不冠數字,數項次冠以① ② ③；款次冠以 1. 2. 3.（數字右方加具頓號）。

제 1 조(목적)

第 1 條（目的）

이 가이드라인은 공개된 개인정보 또는 이용내역정보 등을 전자적으로 설정된 체계에 의해 수집·저장·조합·분석 등 처리하여 새로운 정보를 생성함에 있어서 이용자의 프라이버시 등을 보호하고 안전한 이용환경을 조성하는 것을 목적으로 한다.

因應電子化設定系統對已公開之個人情報及利用內容情報等為蒐集·儲存·統合·分析等處理所產生之新情報，為保護使用人的隱私，並組成安全的利用環境，特制定本準則。

本報告之智慧財產權屬於國家通訊傳播委員會

제 2 조(정의)

第 2 條（定義）

이 가이드라인에서 사용하는 용어의 정의는 다음과 같으며, 본 조에서 정의되지 않은 용어는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「개인정보 보호법」 등 관련 법률에서 정의한 바에 따른다.

本準則用詞，定義如下；本條未定義者依「情報通信網利用促進暨情報保護等相關法律」、「個人情報保護法」等相關法律。

1. “공개된 정보”란 이용자 및 정당한 권한이 있는 자에 의해 공개 대상이나 목적의 제한 없이 합법적으로 일반 공중에게 공개된 부호·문자·음성·음향 및 영상 등의 정보를 말한다.

1. 已公開情報：指使用人及具正當權限之人，於未限制公開對象及目的，合法對一般公眾所公開之符號·文字·聲音·音量及影像等資訊。

2. “이용내역정보”란 이용자가 정보통신서비스를 이용하는 과정에서 자동으로 발생하는 서비스 이용기록, 인터넷 접속정보, 거래기록 등의 정보를 말한다.

2. 利用內容情報：指使用人在利用情報通信服務過程中，自動發生之使用服務紀錄、線上存取資訊、交易紀錄等資訊。

本報告之智慧財產權屬於國家通訊傳播委員會

3. “정보 처리시스템”이란 공개된 개인정보 또는 이용내역정보 등을 전자적으로 설정된 체계에 의해 조합·분석 등 처리하여 새로운 정보를 생성하는 시스템을 말한다.

3. 情報處理系統：指以電子化設定系統對已公開之個人情報及利用內容情報等為統合·分析等處理，而產生新情報之作業系統。

4. “비식별화”란 데이터 값 삭제, 가명처리, 총계처리, 범주화, 데이터 마스킹 등을 통해 개인정보의 일부 또는 전부를 삭제하거나 대체함으로써 다른 정보와 쉽게 결합하여도 특정 개인을 식별할 수 없도록 하는 조치를 말한다.

4. 去識別化：指藉由刪除數據值、假名處理、總計處理、範圍化、遮隱數據等刪除或取代個人情報之部分或全部，致連結其他資訊亦無法識別特定個人之措施。

제 3 조(개인정보의 보호)

第 3 條（個人情報之保護）

① 정보통신서비스 제공자가 정보 처리시스템을 통해 공개된 정보, 이용내역정보를 수집·저장·조합·분석 등 처리하고자 하는 경우, 개인정보의 보호를 위해 다음 각 호의 조치를 취하여야 한다.

① 情報通信服務提供者，有透過情報處理系統公開情報、對利用內

本報告之智慧財產權屬於國家通訊傳播委員會

容情報為蒐集·儲存·統合·分析等處理時，應採取下列各款措施以保護個人情報。

1. 개인정보가 포함된 공개된 정보 및 이용내역정보는 비식별화 조치를 취한 후 수집·저장·조합·분석 등 처리하여야 한다.

1. 包括已公開情報之個人情報及利用內容情報，進行蒐集·儲存·統合·分析等處理前應採取去識別化措施。

2. 비식별화 조치된 공개된 정보 및 이용내역정보를 조합·분석 등 처리하는 과정에서 개인정보가 생성되지 않도록 하여야 한다. 다만, 개인정보가 생성되는 경우에는 지체없이 파기하거나 비식별화 조치를 취하여야 한다.

2. 於統合·分析等處理去識別化之已公開情報及利用內容情報過程中，應避免產生個人情報。但個人情報產生時，應立即採取去識別化措施或廢棄，不得遲延。

② 비식별화 조치된 공개된 정보 및 이용내역정보를 정보처리시스템에 저장·관리하는 경우 다음 각 호의 보호조치를 취하여야 한다.

② 以情報處理系統儲存·管理去識別化之已公開情報及利用內容情

本報告之智慧財產權屬於國家通訊傳播委員會

報時，應採取下列各款保護措施。

1. 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제장치의 설치·운영

1. 設置·運作侵入阻斷系統等控制存取裝置，以阻斷非法存取

2. 접속기록의 위조·변조 방지를 위한 조치

2. 防止偽造·變造存取紀錄之措施

3. 백신 소프트웨어의 설치·운영 등 악성 프로그램에 의한 침해 방지조치

3. 設置·運作防毒軟體等，以防止惡意程式侵害之措施

4. 기타 안전성 확보를 위해 필요한 보호조치

4. 為了其他安全防護之必要保護措施

제 4 조(공개된 정보의 수집·이용)

第 4 條（已公開情報之蒐集·利用）

① 정보통신서비스 제공자가 개인정보가 포함된 공개된 정보를 비식별화 조치한 경우에는 이용자의 동의 없이 수집·이용할 수 있다. 다만, 이용자의 동의를 받거나 법령상 허용하는 경우에는 비식별화 조치를 취하지 아니하고 수집·이용할 수 있다.

① 情報通信服務提供者，對包括已公開情報之個人情報已進行去識

本報告之智慧財產權屬於國家通訊傳播委員會

別化措施，無需經過使用人同意即可蒐集·利用。但有取得使用人之同意或法令上許可之情形，縱未採取去識別化措施亦得蒐集·利用。

② 정보통신서비스 제공자는 제 1 항에 따라 개인정보가 포함된 공개된 정보를 수집·이용하는 경우 공개된 정보의 수집 출처, 수집·저장·조합·분석 등 처리하는 사실 및 그 목적을 이용자 등이 언제든지 쉽게 확인할 수 있도록 개인정보 취급방침을 통해 공개하여야 한다.

② 情報通信服務提供者，依第 1 項對包括已公開情報之個人情報為蒐集·利用之情形，為使使用人得隨時輕易地確認，應將已公開情報之蒐集出處、蒐集·儲存·統合·分析等處理之事實及其目的，公開於個人情報取得指引。

③ 정보통신서비스 제공자는 이용자 등의 요구가 있으면 즉시 다음 각 호의 모든 사항을 이용자 등에게 알려야 한다.

③ 情報通信服務提供者，於使用人等提出要求時，應立即向使用人告知下列各款所有事項。

1. 개인정보의 수집 출처

1. 個人情報之蒐集出處

2. 개인정보의 수집·저장·조합·분석 등 처리의 목적

本報告之智慧財產權屬於國家通訊傳播委員會

2. 個人情報之蒐集·儲存·統合·分析等處理之目的

3. 해당 개인정보의 처리 정지를 요구할 권리가 있다는 사실

3. 具終止該當個人情報處理要求權利之事實

제 5 조(이용내역정보의 수집·이용)

第 5 條（利用內容情報之蒐集·利用）

① 정보통신서비스 제공자는 다음 각 호의 경우를 제외하고는 이용자의 동의를 받거나 비식별화 조치를 취한 후 이용내역정보를 수집·이용할 수 있다.

① 情報通信服務提供者，除下列各款情形，於取得使用人同意或採取去識別化措施後，得對利用內容情報予以蒐集·利用。

1. 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 이용내역정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우

1. 為履行情報通信服務提供相關契約之必要利用內容情報，因經濟性·技術性事由，通常情形取得同意有明顯困難時

2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우

2. 依提供情報通信服務核算資費之必要時

本報告之智慧財產權屬於國家通訊傳播委員會

3. 다른 법률에 특별한 규정이 있는 경우

3. 其他法律有特別規定時

② 정보통신서비스 제공자는 제 1 항에 따라 이용내역정보를 수집하는 경우 해당 정보가 수집·저장·조합·분석 등 처리되는 사실 및 목적을 이용자가 언제든지 쉽게 확인할 수 있도록 개인정보 취급방침을 통해 공개하여야 한다.

② 情報通信服務提供者，依第 1 項蒐集利用內容情報時，為使使用人得隨時輕易地確認，應將該當情報之蒐集·儲存·統合·分析等處理之事實及目的，公開於個人情報取得指引。

③ 정보통신서비스 제공자는 이용내역정보의 수집·저장·조합·분석 등 처리를 거부할 수 있는 방법 및 절차를 마련하여야 한다.

③ 情報通信服務提供者，應完備得拒絕利用內容情報之蒐集·儲存·統合·分析等處理之辦法及程序。

④ 정보통신서비스 제공자는 이용자의 검색프로그램 등에서 이용자 또는 검색프로그램 등 공급자가 설정해 놓은 이용내역정보의 수집 거부 선택을 이용자의 동의 없이 변경해서는 아니 된다.

④ 情報通信服務提供者，在使用人之搜尋程式等內，未經使用人同

本報告之智慧財產權屬於國家通訊傳播委員會

意，不得變更使用人或搜尋程式等提供者於設定所選擇之拒絕蒐集利用內容情報。

제 6 조(새로운 정보의 생성)

第 6 條（產生新情報）

① 정보통신서비스 제공자는 비식별화 조치하여 수집한 공개된 정보 및 이용내역정보를 정보 처리시스템을 통해 조합·분석하여 새로운 정보를 생성할 수 있다. 다만, 새롭게 생성된 정보에 개인정보가 포함되어 있을 경우, 즉시 파기하거나 비식별화 조치를 취하여야 한다.

① 情報通信服務提供者，為去識別化措施所蒐集之已公開情報及透過情報處理系統所統合·分析之利用內容情報，得產生新情報。但新產生之情報有包括個人情報時，應立即廢棄或採取去識別化措施。

② 정보통신서비스 제공자는 제 1 항에 따라 개인정보가 포함된 정보가 생성될 수 있다는 사실 및 그 처리 방법을 이용자가 언제든지 쉽게 확인할 수 있도록 개인정보 취급방침을 통해 공개하여야 한다.

② 情報通信服務提供者，為使使用人得隨時輕易地確認，應將依第 1 項包括個人情報可能產生情報之事實及其處理方式，公開於個

本報告之智慧財產權屬於國家通訊傳播委員會

人情報取得指引。

제 7 조(민감정보 생성의 금지)

第 7 條（禁止產生敏感情報）

특정한 개인의 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 이용자의 사생활을 현저히 침해할 우려가 있는 정보의 생성을 목적으로 공개된 개인정보 등을 수집·저장·조합·분석 등 처리하여서는 아니 된다. 다만, 이용자의 사전 동의를 받거나 법률에 따라 허용된 경우에는 그러하지 아니하다.

不得以產生特定個人之思想·信念、勞動組織·政黨之加入·退出、政治傾向、健康、私生活等相關資訊，及其他明顯可能侵害使用人私生活之資訊為目的，而對已公開個人情報為蒐集·儲存·統合·分析等處理。但取得使用人事前同意或法律許可之情形，不在此限。

제 8 조(통신 내용의 조합, 분석 또는 처리 금지)

第 8 條（通信內容之統合、分析或處理禁止）

정보통신서비스 제공자는 전송중인 이메일, 문자메시지 등의 통신 내용에 대하여 양 당사자의 동의를 얻은 경우를 제외하고, 통신 내용의 전부 또는 일부를 조합, 분석 또는 처리하여서는

本報告之智慧財產權屬於國家通訊傳播委員會

아니 된다.

情報通信服務提供者，對傳輸中電子郵件、簡訊等通訊內容，除取得雙方當事人同意，不得對通訊內容之全部或部分為統合、分析或處理。

제 9 조(공개된 정보 및 이용내역정보의 이용)

第 9 條（使用已公開情報暨利用內容情報）

① 정보통신서비스 제공자는 비식별화 처리된 공개된 정보 및 이용내역정보를 자신의 서비스 제공업무 수행을 위해 내부에서 이용할 수 있다. 다만, 이용자가 거부 의사를 표시한 때에는 그러하지 아니하다.

① 情報通信服務提供者，對已去識別化處理之已公開情報，及為執行服務提供業務之利用內容情報，得於內部利用之。但使用人有表示拒絕之意思時，不在此限。

② 정보통신서비스 제공자는 제 1 항에 따라 공개된 정보 및 이용내역정보를 이용하는 경우 해당 정보가 이용된다는 사실 및 그 목적을 이용자가 언제든지 쉽게 확인할 수 있도록 개인정보 취급방침을 통해 공개하여야 한다.

② 情報通信服務提供者，依第 1 項利用已公開情報及利用內容情報時，為使使用人得隨時輕易地確認，應將該情報被利用之事實及其目的，公開於個人情報取得指引。

本報告之智慧財產權屬於國家通訊傳播委員會

제 10 조(제 3 자 제공)

第 10 條（第 3 人提供）

정보통신서비스 제공자는 개인정보가 포함된 공개된 정보, 이용내역정보, 생성 정보의 경우, 이용자의 동의를 얻어 제 3 자에게 제공할 수 있다. 다만, 비식별화 처리된 공개된 정보, 이용내역정보, 생성 정보는 이용자 동의 없이 제 3 자 제공이 가능하다.

情報通信服務提供者，包括已公開情報之個人情報、利用內容情報、新產生之情報，於取得使用人同意，得向第 3 人提供之。但經去識別化處理之已公開情報、利用內容情報、新產生之情報，得未經使用人同意向第 3 人提供之。

제 11 조(적용범위)

第 11 條（準用範圍）

이 가이드라인에서 규정하지 않은 사항은「정보통신망 이용촉진 및 정보보호 등에 관한 법률」,「개인정보 보호법」 등 관련 법률에 따른다.

本準則未規定事項依「情報通信網利用促進暨情報保護等相關法律」、「個人情報保護法」等相關法律。

本報告之智慧財產權屬於國家通訊傳播委員會

參考書目

中文參考資源

1. 8 功能最齊全，亞太電信 GtPay 推智慧繳費，ePrice，2019 年 7 月 18 日，https://m.eprice.com.tw/telecom/talk/106/5374182/1/。
2. GtPay 行動支付服務條款與隱私政策，GT 智慧生活，https://gttvweb.wowotv.tw/event/GtPay/。
3. Hami Pay 服務暨隱私權條款與 Hami Point 啟用條款，中華電信，https://wserv.emome.net/EULAforNewHami。
4. MBA-人潮客群分析平台規格介紹，中華電信，https://www.cht.com.tw/home/enterprise/businessapplication/bigdata/684。
5. Wail 服務移轉公告，台灣大哥大，https://www.wali.tw/event/13/。
6. 中央社，COVID-19 疫苗數位證明平台 最快 8 月底上路，2021/08/17，https://www.cna.com.tw/news/firstnews/202108170190.aspx。
7. 中央社，實聯制簡訊遭誤解用於辦案 法務部：研議修法保障個資，2021/06/24，https://www.cna.com.tw/news/asoc/202106240357.aspx。
8. 王憶紅，中華電 Hami Wallet 再度更名為 Hami Pay 年底拚 200 萬用戶，自由時報，2018 年 10 月 1 日，https://ec.ltn.com.tw/article/breakingnews/2567367。
9. 行政院，暫緩數位身分證發行計畫 蘇揆:完善法制後再推動，2021/01，https://www.ey.gov.tw/Page/9277F759E41CCD91/e80e55a2-0102-4031-b6d3-a7c40f4cac6a。
10. 法務部主管法規查詢系統，

本報告之智慧財產權屬於國家通訊傳播委員會

https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=FL010631。

11. 金管會將於近日發布「電子支付機構管理條例」12 項授權法規命令並自 110 年 7 月 1 日施行，金融監督管理委員會，2021/06/24，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202106240004&dtable=News。
12. 孫家銘，掌握高雄七大熱門景點人潮 旅遊警示燈號測試版上線，新頭殼新聞，2021/07/27，https://newtalk.tw/news/view/2021-07-27/610975。
13. 疾病管制署，「臺灣社交距離 APP」已上架 鼓勵全民下載使用掌握疫情擴散相關資訊，https://www.mohw.gov.tw/cp-16-60680-1.html。
14. 財政部 109 年度綜合所得稅行動電話認證，https://qa.twca.com.tw/taxmid/。
15. 國家發展委員會，個資法問與答，https://pipa.ndc.gov.tw/News_Content.aspx?n=7D3602579D2BF23F&sms=2F28806F8A42AE16&s=C179B0C8D448D449。
16. 張淵森，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，2021/06/19，https://opinion.udn.com/opinion/story/120701/5542571。
17. 陳冠榮，friDay 錢包大改版，遠傳攜手 Bankee、Richart 推出存錢計畫 App，TechNews 科技新報，2020 年 3 月 5 日，https://technews.tw/2020/03/05/far-eastone-telecommunications-launches-friday-57-app/。
18. 陳絲倩、陳羿愷，電子支付市場的新變革 – 你需要知道的二三事，Winkler Partners 博仲，2021/05/19，http://www.winklerpartners.com/?p=11167&lang=zh-hant。
19. 陳蕙綾，金融監理沙盒成功首案誕生 信用小白電信借貸未來可望一體適用，鉅亨新聞，2019/08/15，https://news.cnyes.com/news/id/4367746 。

本報告之智慧財產權屬於國家通訊傳播委員會

20. 曾靈，台灣大哥大行動支付鳴槍！「Wali 智慧錢包」上線搶 30 萬用戶數，數位時代，2016 年 1 月 28 日，https://www.bnext.com.tw/article/38596/BN-2016-01-28-172613-117。
21. 黃彥棻，【專訪行政院政務委員郭耀煌】落實總統政見，數位發展部最快 2022 第一季掛牌，iThome，2021/05/18，https://www.ithome.com.tw/news/144110。
22. 臺灣社交距離 APP 注意事項及個資保護說明，https://ailabs.tw/taiwan-social-distancing-APPpersonal-data-protection-note/。
23. 蔡毓華，自資料流通機制建置擴大資料經濟市場，資策會科法所，2020/04，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8440。
24. 衛生福利部疾病管制署，「疫調輔助平臺」7 月 26 日上線 指揮中心：運用資訊科技以便捷疫調工作，https://www.cdc.gov.tw/Bulletin/Detail/rVZ1dkbtACeqf4cypmsrkg?typeid=9。
25. 衛生福利部疾病管制署，網傳「簡訊實聯制監控人民行蹤」指揮中心：不實訊息勿轉傳以免觸法，https://www.mohw.gov.tw/cp-17-60900-1.html。
26. 衛生福利部疾病管制署，簡訊實聯制數據係以合法性、正當性、必要性進行使用，絕無違法情事，https://www.cdc.gov.tw/Bulletin/Detail/HS0hjvHxAOTCPtNPmDo7Bw?typeid=9。
27. 簡訊實聯制隱私權公告，https://emask.taiwan.gov.tw/real/info5.html。

外文參考資源

1. 〈(お知らせ) NTT ドコモ、埼玉高速鉄道、ビズライト・テ

クノロジー、LIVE BOARD 世界初、鉄道車両内でのダイナミック DOOH 事業を共同で推進〉，株式会社 NTT ドコモ，2019/11/11，https://www.nttdocomo.co.jp/info/news_release/2019/11/11_00.html。

2. 〈（お知らせ）ドコモが三井住友 DS アセットマネジメントとドコモ統計データの投資信託への活用に関する業務提携に合意-取組み第一弾として「モバイル空間統計」を投資信託の運用に活用-〉，株式会社 NTT ドコモ，2020/12/01，https://www.nttdocomo.co.jp/info/news_release/2020/12/01_01.html。
3. 〈（お知らせ）ドコモのパーソナルデータの取り扱いについて-パーソナルデータ憲章の公表、およびプライバシーポリシーをよりわかりやすく再編-〉，株式会社 NTT ドコモ，2019/08/27，https://www.nttdocomo.co.jp/info/news_release/2019/08/27_00.html。
4. 〈（お知らせ）国内最大規模の交通ビッグデータ「人口流動統計」を開発-ドコモ、国総研、東京大学による産官学共同開発-〉，株式会社 NTT ドコモ，2018/06/04，https://www.nttdocomo.co.jp/info/news_release/2018/06/04_00.html。
5. 〈【第 6 回】「Society 5.0」実現に必要不可欠な次世代通信技術「5G」のここがすごい！〉，株式会社日立システムズ，https://www.hitachi-systems.com/report/specialist/society5/06/index.html。
6. 〈KDDI、応用地質、トヨタ、IoT で防災・減災を実現するデータ協業に合意〉，KDDI 株式会社，2018/04/24，https://news.kddi.com/kddi/corporate/newsrelease/2018/04/24/3094.html。

本報告之智慧財產權屬於國家通訊傳播委員會

7. 〈NTT ドコモ パーソナルデータ憲章 -イノベーション創出に向けた行動原則-〉，株式会社 NTT ドコモ，https://www.nttdocomo.co.jp/utility/personal_data/charter/?icid=CRP_UTI_privacy_to_CRP_UTI_personal_data_charter。
8. 〈NTT ドコモ プライバシーポリシー〉，株式会社 NTT ドコモ，https://www.nttdocomo.co.jp/utility/privacy/?icid=CRP_common_footer_to_CRP_UTI_privacy。
9. 〈Society 5.0〉，內閣府，https://www8.cao.go.jp/cstp/society5_0/。
10. 〈デジタル改革関連法案について〉，内閣官房 IT 総合戦略室，2021/03/03，https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/dejigaba/dai14/siryou1.pdf。
11. 〈デジタル社会の形成を図るための関係法律の整備に関する法律，法律第三十七號，2021/05/19。
12. 〈プライバシーポリシー〉，KDDI 株式会社，https://www.kddi.com/corporate/kddi/public/privacy/。
13. 〈モバイル空間統計ガイドライン〉，株式会社 NTT ドコモ，https://www.nttdocomo.co.jp/corporate/disclosure/mobile_spatial_statistics/guideline/。
14. 〈モバイル空間統計に関する情報〉，株式会社 NTT ドコモ，https://www.nttdocomo.co.jp/corporate/disclosure/mobile_spatial_statistics/index.html。
15. 〈人の流れを予測し可視化する「人口動態分析/予測」技術を開発〉，KDDI 株式会社，2018/04/24，https://news.kddi.com/kddi/corporate/newsrelease/2018/04/24/3095.html。
16. 〈令和 3 年版情報通信白書〉，総務省，2020/03，https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01h

本報告之智慧財產權屬於國家通訊傳播委員會

onpen.pdf。
17. 〈包括的データ戦略〉，高度情報通信ネットワーク社会推進戦略本部，2021/06/18，https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20210618/siryou3.pdf。
18. 〈科学技術・イノベーション基本法・科学技術・イノベーション創出の活性化に関する法律〉，內閣府，https://www8.cao.go.jp/cstp/cst/kihonhou/mokuji.html。
19. 〈個人情報の保護に関する法律，法律第五十七號，2003/05/30。
20. 〈個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編（令和 3 年 1 月一部改正版本）〉，個人情報保護委員会，https://www.ppc.go.jp/files/pdf/210101_guidlines02.pdf。
21. 〈個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）（平成 29 年 3 月一部改正版本）〉個人情報保護委員会，https://www.ppc.go.jp/files/pdf/guidelines04.pdf。
22. 〈個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）〉個人情報保護委員会，https://www.ppc.go.jp/files/pdf/guidelines03.pdf。
23. 〈個人情報の保護に関する法律についてのガイドライン（通則編）（令和 3 年 1 月一部改正版本）〉，個人情報保護委員会，https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf。
24. 〈個人情報の保護に関する法律等の一部を改正する法律について〉，個人情報保護委員会，2021/04/27，https://www.soumu.go.jp/main_content/000747671.pdf。
25. 〈個人情報の保護に関する法律等の一部を改正する法律案〉，法律第四十四號，2020/06/12。
26. 〈接触確認アプリケーションプライバシーポリシー〉，厚生労働省，2020 年 12 月 15 日　プライバシーポリシー改定のお

本報告之智慧財產權屬於國家通訊傳播委員會

知らせ，
https://www.mhlw.go.jp/cocoa/privacypolicy_japanese.html。
27. 〈接触確認アプリケーション利用規約〉，厚生労働省，https://www.mhlw.go.jp/cocoa/kiyaku_japanese.html。
28. 〈第 5 期科学技術・イノベーション基本計画（2016）〉，內閣府，https://www8.cao.go.jp/cstp/kihonkeikaku/index5.html。
29. 〈第 6 期科学技術・イノベーション基本計画〉，內閣府，https://www8.cao.go.jp/cstp/kihonkeikaku/index6.html。
30. 〈買い物の利便性を向上させる地域循環バスの実証実験を開始～「モバイル空間統計」を活用し、高齢者や子育て世代のバス利用の需要を発見～〉，株式会社 NTT ドコモ，2020/08/24，https://www.nttdocomo.co.jp/binary/pdf/info/news_release/topics_200804_01.pdf。
31. 〈新型コロナウイルス接触確認アプリ（COCOA) COVID-19 Contact-Confirming application）〉，厚生労働省，https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/cocoa_00138.html。
32. 〈新型コロナウイルス感染者等情報把握・管理支援システム(HER-SYS)〉，厚生労働省，https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000121431_00129.html#oldjimren。
33. 〈電気通信事業における個人情報保護に関するガイドライン，平成 29 年総務省告示第 297 号〉，2017/09/14，https://www.soumu.go.jp/main_content/000507466.pdf。
34. 〈電気通信事業における個人情報保護に関するガイドライン〉，総務省，2017/09/14，https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html。
35. 2021 telecommunications industry outlook, Deloitte US,

本報告之智慧財產權屬於國家通訊傳播委員會

https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/telecommunications-industry-outlook.html.

36. ATIS – US Ignite Smart City Data Governance Policies Create a Foundation for Data Sharing with City Partners, ATIS (May 27, 2021), https://www.atis.org/press-releases/atis-us-ignite-smart-city-data-governance-policies-create-a-foundation-for-data-sharing-with-city-partners/.
37. Best Practices and Guidelines for Location Based Services, CTIA, https://www.ctia.org/the-wireless-industry/industry-commitments/best-practices-and-guidelines-for-location-based-services.
38. Building resilience through mobile positioning data in Estonia and Indonesia, Positium (July 12, 2021), https://positium.com/blog/resilience-mobile-phone-data-estonia-indonesia.
39. BUNDESMINISTERIUM FÜR WIRTSCHAFTS UND ENERGIE [BMWi], Gesetz zum Schutz der Privatsphäre in der digitalen Welt beschlossen (May 28, 2021), https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2021/05/20210528-gesetz-zum-schutz-der-privatsphaere-in-der-digitalen-welt-beschlossen.html.
40. CMA-ICO joint statement on competition and data protection law, Competition and Markets Authority, https://www.gov.uk/government/publications/cma-ico-joint-statement-on-competition-and-data-protection-law.
41. Contracts and Terms, Telia, https://www.telia.ee/en/lepingud-ja-tingimused#teenusetingimused.
42. Coronavirus (COVID-19): notice under regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002 –

本報告之智慧財產權屬於國家通訊傳播委員會

NHSE, NHSI, https://www.gov.uk/government/publications/coronavirus-covid-19-notification-of-data-controllers-to-share-information/coronavirus-covid-19-notice-under-regulation-34-of-the-health-service-control-of-patient-information-regulations-2002-nhse-nhsi.

43. Corona-Warn-APP open-source project, https://www.coronawarn.APP/en/.
44. Country information – Germany, EUROPEAN COMMISSION [EC], https://ec.europa.eu/digital-single-market/en/country-information-germany.
45. COVID-19 Mobility Analysis of Statistics Estonia: Collaborating with mobile network providers during an emergency situation, measuring human mobility under social distancing measurements, Migration Data Portal (Apr. 28, 2021), https://www.migrationdataportal.org/data-innovation/covid-19-mobility-analysis-statistics-estonia-collaborating-mobile-network.
46. CovovPassCheck-APP, https://www.digitaler-impfnachweis-APP.de/en/covpasscheck-APP.
47. CovPass-APP, https://www.digitaler-impfnachweis-APP.de/en.
48. Crowd Insights for Municipalities, Telia, https://business.teliacompany.com/crowd-insights/Crowd-Insights-for-Cities.
49. Crowd Insights for Retail, Telia, https://business.teliacompany.com/crowd-insights/Crowd-Insights-for-Retail.
50. Crowd Insights for Transport, Telia, https://business.teliacompany.com/crowd-insights/Crowd-Insights-for-Public-Transport.
51. Data Protection Act 2018, https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

本報告之智慧財產權屬於國家通訊傳播委員會

52. Data Protection Impact Assessment: NHS COVID-19 Data Store, NHS, https://www.england.nhs.uk/publication/data-protection-impact-assessment-nhs-covid-19-data-store/.
53. Datenschutzerklärung luca APP, https://www.luca-APP.de/APP-privacy-policy/.
54. Department for Business, Energy & Industrial Strategy, Smart Data Working Group: Spring 2021 report, GOV. UK (June 14, 2021), https://www.gov.uk/government/publications/smart-data-working-group-spring-2021-report.
55. Department for Digital, Culture, Media & Sport, National Data Strategy, GOV. UK (Dec. 9, 2020), https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy.
56. DEUTSCHER BUNDESTAG, Datenschutz und Schutz der Privatsphäre in der Telekommunikation (Mar. 25, 2021), https://www.bundestag.de/dokumente/textarchiv/2021/kw12-de-datenschutz-telekommunikation-826510.
57. Digital Government Factsheet 2019, European Commission.
58. Digital Government: Building a 21st Century Platform to Better Serve the American People, Digital Government, https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html.
59. Digital Regulation Cooperation Forum workplan 2021/22, Competition and Markets Authority, https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-20212.
60. Digital Regulation Cooperation Forum: embedding coherence and cooperation in the fabric of digital regulators, Competition and Markets Authority, https://assets.publishing.service.gov.uk/government/uploads/system/

本報告之智慧財產權屬於國家通訊傳播委員會

uploads/attachment_data/file/982898/DRCF_response_to_DCMS__PDF.pdf.

61. EE, EE Launches Identity Checker to Help Business Protect Customers Against Fraud, https://newsroom.ee.co.uk/ee-launches-identity-checker-to-help-businesses-protect-customers-against-fraud/.
62. E-Estonia, mobility services, https://e-estonia.com/solutions/location-based-services/mobile-parking/.
63. Electronic Communications Act, Riigi Teataja, https://www.riigiteataja.ee/en/eli/501042015003/consolide.
64. European Commission, Commission proposes a trusted and secure Digital Identity for all Europeans (June 3, 2021), https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663.
65. Events & Tourism, Telia, https://business.teliacompany.com/crowd-insights/Crowd-Insights-for-Events-and-Tourism.
66. FCC Proposes Over $200M in Fines for Wireless Location Data Violations, Federal Communications Commission (Feb. 28, 2020), https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations.
67. Federal Communications Commission, Cell Phone Fraud, https://www.fcc.gov/consumers/guides/cell-phone-fraud.
68. Federal Trade Commission, SIM Swap Scams: How to Protect Yourself, https://www.consumer.ftc.gov/blog/2019/10/sim-swap-scams-how-protect-yourself.
69. Fedral Ministry for Econmic Affairs and Energy, Telekommunikationsmodernisierungsgesetz (Feb. 24, 2021), https://www.bmwi.de/Redaktion/DE/Artikel/Service/Gesetzesvorhaben/telekommunikationsmodernisierungsgesetz.html.
70. GreenMagenta - the name says it all, Deutsche Telekom AG, https://www.telekom.com/en/corporate-responsibility/corporate-

本報告之智慧財產權屬於國家通訊傳播委員會

responsibility/greenmagenta-the-name-says-it-all-624448.
71. HOIA- protect yourself and your clostest ones, https://hoia.me/en/.
72. Infosüsteemide andmevahetuskiht, Riigi Teataja, https://www.riigiteataja.ee/akt/106082019017.
73. Jesse Kurtto, Could a pan-European digital identity be a reality by 2022?, Ubisecure (Sep. 13, 2021), https://www.ubisecure.com/authentication/european-digital-identity-framework/.
74. Joseph Cox, I Gave a Bounty Hunter $300. Then He Located Our Phone, VICE (Jan. 9, 2019), https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.
75. Kavya Sekar and Laurie A. Harris, Contact Tracing for COVID-19: Domestic Policy Issues, CRS In Focus IF11609, Aug. 3, 2020.
76. Kdata, https://www.kdata.or.kr/.
77. Luca, https://www.luca-APP.de/.
78. M25 Mobile Phone Data Journey Times, Atkins, https://datainsights.atkinsglobal.com/assets/pdf/Case_Study_M25_V03.pdf.
79. More partners, more devices, more security – Deutsche Telekom spices up Magenta SmartHome, Deutsche Telekom AG, https://www.telekom.com/en/media/media-information/consumer-products/-deutsche-telekom-spices-up-magenta-smarthome-501526.
80. New Report: Europe behind on key digital metrics, telcos essential to achieve leadership, ETNO, https://etno.eu/news/all-news/8-news/694-state-of-digi-2021-pr.html.
81. NHS COVID-19 APP: privacy notice, Department of Health & Social Care, https://www.gov.uk/government/publications/nhs-covid-19-APP-privacy-information/nhs-covid-19-APP-privacy-notice.

本報告之智慧財產權屬於國家通訊傳播委員會

82. NHS COVID-19 Data Store, NHS, https://www.england.nhs.uk/contact-us/privacy-notice/how-we-use-your-information/covid-19-response/nhs-covid-19-data-store/.
83. NHS, COVID-19 APP support, https://www.covid19.nhs.uk/.
84. Privacy notice, Corona-Warn-APP, Privacy notice, https://www.coronawarn.APP/assets/documents/cwa-privacy-notice-en.pdf.
85. Protection of personal data and privacy, Riigiportaal EESTI. EE, https://www.eesti.ee/en/security-and-defense/safety-and-security/protection-of-personal-data-and-privacy.
86. REGULATION (EU) 2021/953 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953.
87. Rein Ahas, Margus Tiru, Erki Saluveer, Christophe Demunter, Mobile telephones and mobile positioning data as source for statistics: Estonian experiences.
88. Ryan Gallagher, Henrik Moltke, The Wiretap Rooms: The NSA's Hidden Spy Hubs in Eight U.S. Cities, The Intercept (June 25, 2018), https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/.
89. S.652 - Telecommunications Act of 1996.
90. Sara Morrison, How your mobile carrier makes money off some of your most sensitive data, Vox (Mar. 13, 2021), https://www.vox.com/recode/22325420/t-mobile-verizon-att-ad-targeting-data.
91. Smart City Data Governance Policies: Creating a Foundation for

本報告之智慧財產權屬於國家通訊傳播委員會

Data Sharing with City Partners, ATIS – US Ignite, May 27, 2021.
92. SmartHome Schutzbrief, Deutsche Telekom AG, https://www.smarthome.de/ideen/smarthome-schutzbrief.
93. Statement: Open Communications – Enabling people to share data with innovative services, Ofcom, https://www.ofcom.org.uk/consultations-and-statements/category-1/open-communications.
94. Taylor Hatmaker, AT&T collaborates on NSA spying through a web of secretive buildings in the US, TechCrunch (June 26, 2018), https://techcrunch.com/2018/06/25/nsa-att-intercept-surveillance/.
95. Telia and Ericsson switch on Estonia's first commercial 5G network, Ericsson (Nov. 10, 2020), https://www.ericsson.com/en/news/2020/11/estonia-switches-on-5g.
96. Tervishoiuteenuste korraldamise seadus, Riigi Teataja, https://www.riigiteataja.ee/akt/118062021008?dbNotReadOnly=true#para59b1lg3.
97. The Digital Regulation Cooperation Forum, Competition and Markets Authority, https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum.
98. The Estonian coronavirus mobile application HOIA is now available for download, Republic of Estonia Ministry of Social Affairs (Aug. 20, 2020), https://www.sm.ee/en/news/estonian-coronavirus-mobile-application-hoia-now-available-download.
99. The Right to Privacy in Estonia, Human Rights Committee (Mar. 2016).
100. The Telegraph, The Atkins-EE partnership: using big data to solve infrastructure problems, https://www.telegraph.co.uk/education/stem-awards/design/atkins-ee-big-data-partnership/.

本報告之智慧財產權屬於國家通訊傳播委員會

101. The UK GDPR, ICO, https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/.
102. The Use of Digital Measures to Combat COVID-19, Northern Ireland Assembly, at 15, http://www.niassembly.gov.uk/assembly-business/committees/2017-2022/health/research-papers-2020/the-use-of-digital-measures-to-combat-covid-19/.
103. The White House, Fact Sheet: The White House Launches "The Opportunity Project," Utilizing Open Data to Build Stronger Ladders of Opportunity for All (Mar. 7, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/03/07/fact-sheet-white-house-launches-opportunity-project-utilizing-open-data.
104. Timothy Vollmer, Obama issues Executive Order in support of open data, Creative Commons (May 10, 2013), https://creativecommons.org/2013/05/10/obama-issues-executive-order-in-support-of-open-data/.
105. T-Mobile Privacy Notice, T-Mobile Privacy (May 5, 2021), https://www.t-mobile.com/privacy-center/our-practices/privacy-policy.
106. UN E-Government Survey 2020, United Nations, https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf.
107. 개인정보보호 법제 하에서의 정보 활용성 향상 전략，KISDI Premium Report，2017/12/27。
108. 김재섭，[단독] 이통 3 사, 따로 DB 만들어 ‘위치 정보’ 몰래 모았다，2020/09/02，https://www.hani.co.kr/arti/economy/it/960279.html。
109. 스마트시티통합플랫품 기반구축，2020/5，

本報告之智慧財產權屬於國家通訊傳播委員會

https://smartcity.go.kr/wp-content/uploads/2019/08/200603-%EC%8A%A4%EB%A7%88%ED%8A%B8%EC%8B%9C%ED%8B%B0%ED%86%B5%ED%95%A9%ED%94%8C%EB%9E%AB%ED%8F%BC%EA%B8%B0%EB%B0%98%EA%B5%AC%EC%B6%95.pdf。

110. 심연숙, “마이데이터(MyData) 활용의 국내외 현황 및 활성화 방안”, The Journal of the Convergence on Culture Technology (JCCT), Vol. 6, No. 4, 2020/11/30。
111. 심연숙，“마이데이터(MyData) 활용의 국내외 현황 및 활성화 방안”，The Journal of the Convergence on Culture Technology (JCCT), Vol. 6, No. 4，2020/11/30.
112. 알파에서 오메가까지 한눈에! KT GEPP 홍보 책자 발간，https://blog.kt.com/1525?category=705035。
113. 이대희，이태원 기지국 접속자 정보 수집, 헌재에서 다룬다，2020/07/30，http://www.pressian.com/pages/articles/2020073017151595841。
114. 작성일，세계 최초!! 스마트검역정보시스템 실시로 해외 감염병 유입 사각지대 최소화，질병 관리청，2019/10/31，http://www.nih.go.kr/gallery.es?mid=a20503010000&bid=0002&b_list=9&act=view&list_no=144510&nPage=1&vlist_no_npage=2&keyField=&keyWord=&orderby=。
115. 정복덕，빅데이터, 수집 시부터 철저히 비식별화 조치해야，KCC，2014/12/23，https://www.kcc.go.kr/user.do?mode=view&page=A05030000&dc=K05030000&boardId=1113&cp=4&ctx=ALL&searchKey=ALL&searchVal=%EB%B9%85%EB%8D%B0%EC%9D%B4%ED%84%B0&boardSeq=40287。
116. 정필모, 정부 통신사 아무도 지키지 않는 [위치정보법], 2020/10/11，https://www.theminjoo.kr/board/view/inspection/338137?st=wrote_

本報告之智慧財產權屬於國家通訊傳播委員會

post&keyword=%EC%A0%95%ED%95%84%EB%AA%A8&page=2。
117. 정필모，정부 통신사 아무도 지키지 않는 [위치정보법]，2020/10/11，https://www.theminjoo.kr/board/view/inspection/338137?st=wrote_post&keyword=%EC%A0%95%ED%95%84%EB%AA%A8&page=2。
118. 코로나 꼼짝마! 글로벌 감염병 확산 방지 프로젝트 (GEPP), http://naver.me/G2UGJm9H。
119. 통신 정보 분석해 금융 혜택… KT, 부산은행 등과 MOU (2021/04/22)，https://biz.chosun.com/site/data/html_dir/2020/04/22/2020042201508.html。
120. 통신 정보 분석해 금융 혜택… KT，부산은행 등과 MOU，2021/04/22，https://biz.chosun.com/site/data/html_dir/2020/04/22/2020042201508.html。

本報告之智慧財產權屬於國家通訊傳播委員會