

接觸者追蹤與人權保障—— 大數據防疫應用之法律探討

何之行 博士

中央研究院歐美所副研究員
中研院資創中心合聘副研究員

E-mail: chihho@sinica.edu.tw

「防疫措施與數位健康證明人權保障
論壇」29 Nov 2021



高科技智慧防疫，檢疫追蹤精準有力



發佈日期：2020-03-18

中央流行疫情指揮中心今(18)日表示，為能掌握居家隔離、居家檢疫者落實情形，降低社區傳染風險，避免影響防疫措施之推動，今(2020)年2月上旬，行政院所屬各單位結合創新科技建置資訊系統，期能以更有效的科技措施協助防疫作業，包括人員入境之「入境檢疫系統」，以電子化加速入境資料檢核及程序，結合後端「電子圍籬智慧監控系統」，透過手機定位方式掌握行蹤，以確保防疫措施之落實。

指揮中心指出，COVID-19(武漢肺炎)疫情日益嚴峻，世界各國確診病例快速攀升，入境人員填寫資料的程序及內容更需要嚴謹審慎。為提高入境流程效率、入境資料正確性，建置「入境檢疫系統」，於起飛前或落地後透過掃描QR Code，線上填寫健康聲明書等資料，加速入境通關程序，旅客資料也整合至「自主健康關懷的「防疫追蹤系統」及追蹤告警的「電子圍籬系統」，透過居家檢疫者的「手機定位」，一旦離開檢疫範圍，系統會發送「告警簡訊」給當事人、民政單位、衛政單位與轄區警察，以確實掌握相關人員行蹤。

此外，指揮中心表示，因應旅遊建議等級提升，入境居家關懷人數增加，接下來將由HTC規劃設計，透過LINE之LINE Bot系統平台自動化運作，讓居家檢疫者可以透過LINE Bot主動回報健康狀況，並取得防疫相關協助資訊，分擔第一線關懷人員的作業負擔。

鑒於全球武漢肺炎疫情仍持續發展中，政府正積極推動新科技，透過系統化分析，依行政區、隔離類別，以及地理分布及歷史軌跡等方式篩選呈現相關人員現況，快速掌握疫情發展；也請全民於疫情期間配合政府防疫作為，共同為維護國內防疫安全努力。



下午 08:48

實聯制掃描使用方式2選1

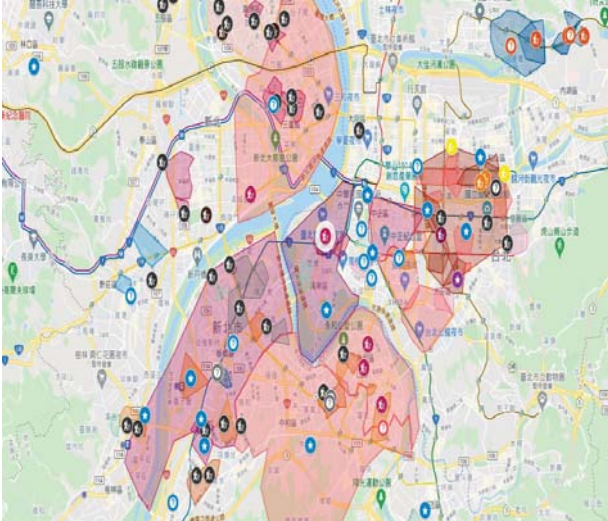


電子圍籬2.0流程

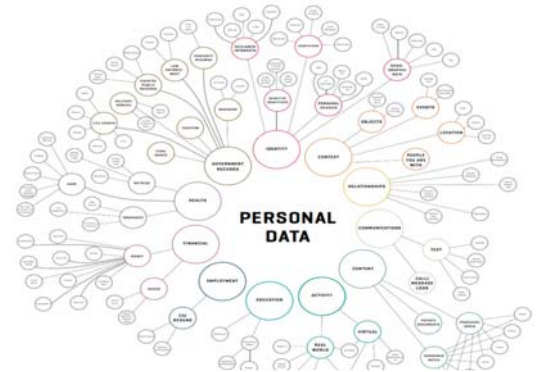
於2020/12/31 啟用



BIG DATA FOR HEALTH SURVEILLANCE



- Non-personal Data
- Personal Data ??
- Public Private Partnerships



簡訊實聯制:

- “免個資”?
 - 民眾免留個資給店家，簡訊記錄留給電信業者。
- 簡訊記錄非個資嗎?
 - 個資法第二條: 個人資料指自然人之姓名.... 聯絡方式、社會活動及其他得以直接或間接方式識別該個人之資料。
- 簡訊傳送至1922疾管署後，僅供指揮中心疫調使用。
 - 尚無疫調所需時，進行預防式資料蒐集?
- 以兩個潛伏期14天來計算，保留28天。



馬賽克理論 (MOSAIC THEORY)

- 乍看之下微不足道、瑣碎的圖案，但拼聚在一起後就會呈現一個寬廣、全面的圖像。
- 個人對於零碎的資訊或許主觀上並沒有隱私權遭受侵害之感受，但大量的資訊累積仍會對個人隱私權產生嚴重危害。
- Profiling: 鑲嵌式的深描剖繪



司改會：疫調簡訊 應禁止調取進行犯罪偵防

2021/6/24 18:24

0 Like

（中央社記者蕭博文台北24日電）司改會今天表示，警方運用「1922簡訊實聯制」辦案引發爭議，呼籲法務部、內政部發函禁止調取疫調簡訊進行犯罪偵防，相關主管機關則應研議修法，保障人民隱私及個資。

國內武漢肺炎（2019冠狀病毒疾病，COVID-19）疫情嚴峻，政府推出實聯制簡訊，讓民眾掃碼進出店家，協助未來疫情調查。

台中地方法院法官張淵森日前撰文表示，刑事警察局在搜索票聲請書中，利用嫌犯以簡訊實聯制發送的簡訊來鎖定嫌犯行蹤，質疑所謂「僅作為疫調使用」的承諾，難道只淪為口號。

對此，國家通訊傳播委員會20日指出，實屬誤解，刑事警察局是依據通訊保障及監察法規定取得簡訊內容，並未向指揮中心調閱，政府並未違反承諾。

民間司法改革基金會今天發布聲明表示，此次爭議在於現行調取通信紀錄的實務運作中，欠缺防止目的外使用的資訊隔離措施，導致執行通訊監察時不分範圍、「一票全都錄」，法務部及相關主管機關應盡速研議修法。

聲明指出，中央流行疫情指揮中心應盡速協調，由法務部、內政部正式發函禁止調取疫調簡訊進行犯罪偵防，法務部也應函釋將「1922簡訊實聯制」相關資訊排除在通訊保障及監察法所稱的通信紀錄之外，明令偵查機關不得調取。

我們需要的答案
其實隨手可得
只要開始向數據探索
Curiosity Forever
深入瞭解

地機族 第174話
到底是「微解封」還是「危解封」
大家看法分歧。
哇
哇

科技防疫下個資之蒐集處理利用

- 二次利用具適法性基礎？
- 明確法律授權？
- 同意 (consent)
- 資料去識別化 (De-identification)

個人資料保護法

- 何謂個人資料？

姓名、出生年月日、ID、指紋、職業、婚姻、教育、病歷、醫療、基因、健康檢查、**聯絡方式**、**社會活動** etc. + 其他得以直接或間接方式識別該個人之資料。(Q: 是否具識別該特定個人之可能性?)

- 保護範圍？

目的特定(限縮)原則: 個人資料之蒐集、處理與利用，不得逾越特定目的之必要範圍 (§5)。

- 區分**敏感性個資**與非敏感性個資
- 敏感性個資 (醫療、基因、健康檢查): 原則不得蒐集處理或利用，例外允許 (§6)。

敏感性個資之蒐集處理或利用(§6但)

- 法律明文規定。
- 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。
- 當事人自行公開或其他已合法公開之個人資料。
- 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，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
- 為協助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。
- 經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

公務機關得為特定目的外之利用 (§16但)

- 一、法律明文規定。(法律授權)
- 二、為維護國家安全或**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。
- 六、有利於當事人權益。
- 七、經當事人同意。

嚴重特殊傳染性肺炎防治及紓困振興特別條例 (2020.2.15)

- 第 7 條:中央流行疫情指揮中心指揮官為防治控制疫情需要，得實施**必要**之應變處置或措施。(Q: 何謂必要?如何監督?)
- 第 8 條: 於防疫期間，受隔離或檢疫而有違反隔離或檢疫命令或有違反之虞者，中央流行疫情指揮中心指揮官得指示對其實施錄影、攝影、公布其個人資料或為**其他必要**之防治控制措施或處置。為避免疫情擴散，對確診罹患嚴重特殊傳染性肺炎病人，亦同。
- 前二項個人資料，於**疫情結束**應依個人資料保護相關法規處理。

《通訊保障及監察法》徵調要件

- 警察機關向電信業者調取基地台定位的位址，以追蹤居家隔離的個人，但**手機的位址**屬《通訊保障及監察法》第 3-1 條所規定的**通信紀錄**，依同法第 11 條，原則上要**偵辦最重本刑三年以上之罪**才能調取。
- 居家隔離的人隨意外出可能觸犯《傳染病防治法》，僅為最高 30 萬元罰鍰的處罰（第 67 條），因此並不構成「依據通訊保障及監察法可調取通信紀錄」之事由。
- 不宜以個人資料保護法上的例外條款，直接合法化。《個人資料保護法》是普通法，依特別法優先於普通法之原則，應依據特別法規定。

DE-IDENTIFICATION

- 去識別、無從識別、去連結 vs. 匿名化 (Q: 是否無回溯可能性?)
- Big data challenges..
- USA: HIPAA (Health Insurance Portability and Accountability Act)
 - removal of 18 identifiers: deemed to be not personal data
- EU GDPR: Pseudonymised (假名化) data: still personal data
 - **NOT** a valid legal basis for processing data
- The limitation of de-identification

EU GDPR: Pseudonymization and anonymization 假名化及匿名化

They are just **safeguards** (安全維護措施) and conditions for processing,
not a legal base (非為處理資料之合法充足條件)

Pseudonymization (假名化，去識別):

personal data can no longer be attributed to a specific data subject
without the use of additional information (e.g. a key or encryption code)
(如掌握特定資訊，如金鑰，則仍可連結)



Anonymization (匿名化，去連結):

the data subject no longer identifiable (無從識別)



公共 vs 個人: 衡平基準?

- 法治國原則
- 立法授權: 法律保留原則
- 行政機關依法行政
- 禁止措施法源依據為何?
- 授權明確性原則 (避免概括或空白授權?)
- 比例原則 (最小侵害性?)
- 正當法律程序 (救濟可能性?)

The screenshot shows a web browser displaying an EURACTIV news article. The article title is "EU stands by its data privacy rules in response to COVID-19" by Gerardo Fortuna, dated April 28, 2020. The article features a video call with EU-27 health ministers, with a banner that reads "We CARE, we ACT" and "Emergency Response Coordination Centre". The article text states that the European Commission will not relax data protection rules in response to the pandemic. The page also includes a newsletter sign-up for "The Capitals Newsletter" and a list of EURACTIV members.

EU stands by its data privacy rules in response to COVID-19 – EURACTIV.com - Google Chrome

euractiv.com/section/coronavirus/news/eu-stands-by-its-data-privacy-rules-in-response-to-covid-19/

EURACTIV The Capitals Newsletters Login / Register Events Search

Agrifood Digital Economy & Jobs Energy & Environment Global Europe Health Politics Transport

Home / News / Health / Coronavirus / EU stands by its data privacy rules in response to COVID-19

EU stands by its data privacy rules in response to COVID-19

By Gerardo Fortuna | EURACTIV.com 2020年4月28日 (updated: 2020年4月29日)



Anne Bucher, Director General of Commission's DG Health and Food Safety, Health Commissioner Stella Kyriakides and Industry Commissioner Thierry Breton (from left to right) [EC]

Comments Print

Europe cannot win the fight against the coronavirus without digital technologies, the European Commission said in a video call with EU-27 health ministers on Monday (27 April). But this must not come at the expense of EU data protection rules, which must remain a "global gold standard".

Health Commissioner Stella Kyriakides invited ministers, representatives from EU health agencies and her colleagues Thierry Breton and Didier Reynders to discuss the potential of e-health in limiting the spread of the virus, including contact tracing apps, remote consultations and telemedicine.

During the debate behind closed doors, these tools were widely recognised as crucial in helping to protect EU citizens as restriction measures are being relaxed and economies restarted safely and

The Capitals Newsletter

Every morning, all the news from the capitals

Your email

Subscribe

Advertisement



EURACTIV EVENT REPORT

Reviving EU ambition on organ donation and transplantation

HUMAN ORGAN With the support of EKHA

EURACTIV Members

Acumen public affairs
Association of European Cancer Leagues (ECL)
BSEF - The International Bromine Council
Cosmetics Europe - The Personal Care Association
ECPC - European Cancer Patient Coalition
EHFG - European Health Forum Gastein

By continuing to browse the website, you are agreeing to our use of cookies I agree

← → ↻ iapp.org/news/a/how-to-employ-privacy-by-design-in-the-fight-against-covid-19/

ENGLISH (EN) ABOUT THE IAPP ENTERPRISE SERVICES CONTACT MYIAPP

20 iapp News Connect Train Certify Resources Conferences Join STORE

Beginning mid-May, a more convenient testing option is coming. Take your certification exam from your own private location with online proctoring. Learn more [here](#). DISMISS

How to employ privacy by design in the fight against COVID-19

Apr 28, 2020 Save This

Assaf Harel, CIPP/E

As COVID-19 is rapidly spreading around the world, public health

BigID BigIdeas on the GO After CCPA: CPRA and The Future State of US Privacy Featuring Rick Arney

EU GDPR DATA PROTECTION PRINCIPLES

- Data Minimisation (資料最小化原則)
- Purpose Limitation (目的特定原則)
 - Secondary use of data (資料二次利用)
 - Compatibility test (兼容性判斷)
- Transparency (透明性原則)
 - Data controller & data processor (資料管理者與資料處理者)
 - Notification (通知義務)
 - Explanation (解釋義務)
- Accountability (課責性原則)

二大模式： 以如何儲存CONTACT TRACING APP所收集資料為區分

集中型：挪威、冰島、法國

- 此模式最大特色是所收集資料是**儲存於單一database**且此database是由**相關政府**建康照護機關所控制。
- 此模式之優點是除保證隱私保護之外，相關政府機關可以接收較多資訊以控制疫情擴散。**公衛監測是政府之責任**而非美國二大資訊巨頭之事。

分散型 (Apple/Google model)：英國、德國等

- 此模式最大特色是相關接觸資料 (匿名化) **只存於使用者之行動手機上**而不是在中央處理器或database。
- 此模式受到**二大資訊巨頭的支持 (Apple and Google)** 及支持隱私權之市民團體。然而非所有政府都支持此一模式。法國政府就指出Apple在技術上不提供法國政府相關資源使法國研發之app能在iPhone上運作更順暢。

The Smittestopp app - helsenorge

helsenorge.no/en/smittestopp/#smittestopp-protects-your-privacy

The Smittestopp app

Smittestopp is an app from the Norwegian Institute of Public Health ("Folkehelseinstituttet (FHI)" in Norwegian). The app is intended to help prevent coronavirus from spreading among the population and is completely voluntary and safe to use. You must be 16 or older to use the app.




Illustration: ArtistGNDphotography

Chat

SMITTESTOPP APP

- 16 歲以上，自願同意。
- 資料控制者是The Norwegian Institute of Public Health
- Smittestopp 經由GPS location services 及藍芽技術收集資訊。
- 此資訊會每一小時被下載於中央處理器儲存且會被儲存30天。
- 位置資訊會在30天後被刪除。
- 經由此Smittestopp應用程式，挪威公共衛生研究所（FHI）將接收有關社會移動方式的匿名資訊。FHI：通過這種方式，有可能更加密切地監視針對冠狀病毒的措施是否奏效，以及隨著社會管制措施和限制之放鬆，感染者是否會建立更密切的聯繫。

NORWAY: CONTACT TRACING APP

- 2020年6月挪威資料保護主管機關（NDPA）宣告，政府應停止使用並刪除資料。
- 透過 GPS 與藍芽定位來追蹤用戶足跡。(非最小侵害手段)
- GPS定位資訊上傳至中央伺服器，儲存30 天後刪除。
(國家全面監控個人行蹤的風險)
- 上傳的資料包含非確診者個案，接收有關社會移動方式的匿名資訊。(違反資料最小蒐集原則)
- 蒐集足跡資料原初是為了即時防疫，但資料將被轉作後續的研究分析。(非特定目的蒐集)
- 挪威政府應主動說明為什麼資料可以被二次利用？又將如何去識別化，以確保個資安全？(透明性揭露)



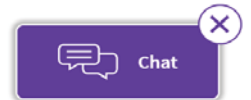
What are the differences between the new and old Smittestopp apps?

Apart from the identical name, the two apps have almost nothing in common. The new Smittestopp app is a brand new technological solution which differs from the old one in the following ways:

- The new app stores everything on your phone and does not upload information to a central location as the old one did.
- The new app uses Bluetooth and not GPS or any other satellite positioning systems. This way, it does not store data on where you have been.
- The new app uses far less battery power than the old one.
- The new app is only used for infection tracking, and not analysis or research.
- The new app does not collect data which can be used to identify you, so there is no data to gain access to.
- The new app does not automatically message other people. You do this yourself when and if you want to.

This is the logo for the new app:

If you still have the old Smittestopp app installed on your phone, you can safely delete it without affecting the new app. It is also safe to leave the old app on your phone. It is



NON-TRANSPARENT HEALTH CODE IN CHINA



【绿码】

凭码通行



【黄码】

实施7天内隔离，连续（不超过）7天健康打卡正常转为绿码



【红码】

实施14天隔离，连续14天健康打卡正常转为绿码

What's new in the EU GDPR?

Right to be forgotten

Right to data portability

Right to explanation?

Privacy Impact Assessment

Data controller & Data processor

International data transfer

Automated decision making

Privacy by design

1

The Debate: Whether There Is a “ Right to Explanation” in the GDPR (Art.22)?

GDPR Article 22(1)

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2

The Debate: Whether There Is a “ Right to Explanation” in the GDPR (Art.22)

GDPR Article 22(3)

*In the cases referred to in points (a) and (c) of paragraph 2, **the data controller shall implement suitable measures** to safeguard the data subject's rights and freedoms and legitimate interests, at least **the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.***

1

The Debate: Whether There Is a “ Right to Explanation” in the GDPR (Art.13-Art.15)

Article 13 Information to be provided where personal data are collected from the data subject

- (2) In addition to the information referred to in paragraph 1, **the controller shall**, at the time when personal data are obtained, **provide** the data subject with the **following further information** necessary to **ensure fair and transparent processing**:
- (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, **meaningful information about the logic involved**, as well as the **significance and the envisaged consequences** of such processing for the data subject.

EU Digital COVID Certificate | x +

ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

An official website of the European Union How do you know? v

safeguard public health.

New proposal to ensure coordination on safe travel in the EU

What is the EU Digital COVID Certificate?

Who can get the EU Digital COVID certificate?

How can citizens get the certificate?

How does it help free movement?

How does the certificate work?


Are citizens who are not yet vaccinated able to travel to another EU country?


Does it matter which vaccine citizens received?


Recognition of COVID certificates from third (non-EU) countries


In such a case – for instance as a reaction to new variants of concern – that Member State would have to notify the Commission and all other Member States and justify this decision.

How does the certificate work?

 The EU Digital COVID Certificate contains a QR code with a digital signature to protect it against falsification.

 When the certificate is checked, the QR code is scanned and the signature verified.

 Each issuing body (e.g. a hospital, a test centre, a health authority) has its own digital signature key. All of these are stored in a secure database in each country.

 The European Commission has built a gateway through which all certificate signatures can be verified across the EU. The personal data of the certificate holder does not pass through the gateway, as this is not necessary to verify the digital signature. The European Commission also helped Member States to develop national software and apps to issue, store and verify certificates and supported them in the necessary tests to on-board the gateway.

EU DIGITAL COVID CERTIFICATE

- To make sure that the digital certificate only includes **a minimum set of information** necessary to confirm and verify the holder's vaccination, testing or recovery status.
- The aim of the certificate is to facilitate free movement. It is **not be a pre-condition to travel**.
- Each issuing body (e.g. a hospital, a test center, a health authority) has its own **digital signature key**. All of these need to be stored in a secure database.
- All certificate signatures can be verified. But the personal data of the certificate holder does **not** pass through the gateway, as this is not necessary to verify the digital signature. **No personal data is exchanged**.

隱私權的限制

- 受憲法保障的基本權利(Fundamental right)
- 但，**非**絕對的權利(Absolute right)
- 公、私益間之衡平
- 群體利益、個人利益間之衡平
- 依比例原則以法律明定方式予以限制

法治國原則

- 民主自由社會與極權體制之分野
- 行政(防疫)機關舉措是否具備明確的法律授權?
- 是否依法行政?
- 是否符合正當法律程序?
- 是否符合最小侵害的比例原則?
- 是否有救濟可能性?
- 透明、社會信任

THANK YOU FOR YOUR ATTENTION