TraceTogether 在新冠疫情防控中的应用

軟件 1804 8209180438 黃柏曛

2020 年 4 月 24 日

Part I

摘要

嚴重特殊傳染性肺炎疫情，是在 2019 年至 2020 年間由嚴重急性呼吸系統綜合症冠狀病毒 2 型（SARS-CoV-2）所引發的全球大流行疫情。疫情擴散對全球航空、旅遊、娛樂、體育、石油市場、金融市場等方面造成巨大影響。

為了控制疫情，新加坡將開源用來抗疫的 TraceTogether 的藍芽追蹤 Android APP。

藍芽追蹤技術，實施 BlueTrace 的應用程序的用戶使用其電話號碼註冊時，後端服務將生成唯一的隨機 UserID 並將其與用戶的電話號碼相關聯。電話號碼是唯一可個人識別的信息用戶要求。如果發現用戶長時間與感染者接觸，可以使用電話號碼與用戶聯繫。

考慮了藍牙和 GPS 聯繫人跟踪解決方案。選擇藍牙是因為它能夠以比 GPS 更低的假陽性率對近距離接觸進行分類。鑑於 GPS 精度在室內環境中會下降，因此整個購物中心或摩天大樓都將在單個 GPS 點的誤差範圍內。此外，公眾對位置跟踪的警惕和電池消耗的增加可能會阻礙採用。

新加坡接連爆發多起移工（新加坡稱「客工」）宿舍「COVID-19」（2019 年新型冠狀病毒疾病）群聚感染。22 日，新加坡新增 1016 起確診病例，當中大多感染者仍是移工，累計病例為 1 萬 141 起，總理李顯龍 21 日發表談話，宣布「阻斷措施」（Circuit Breaker）延長至 6 月 1 日。

新加坡被視為善用科技防疫的國家，《海峽時報》報導，李顯龍在談話中說「我們需要每一個人的合作和使用」智慧型手機行動應用程式（App），並鼓勵人們下載 TraceTogether。

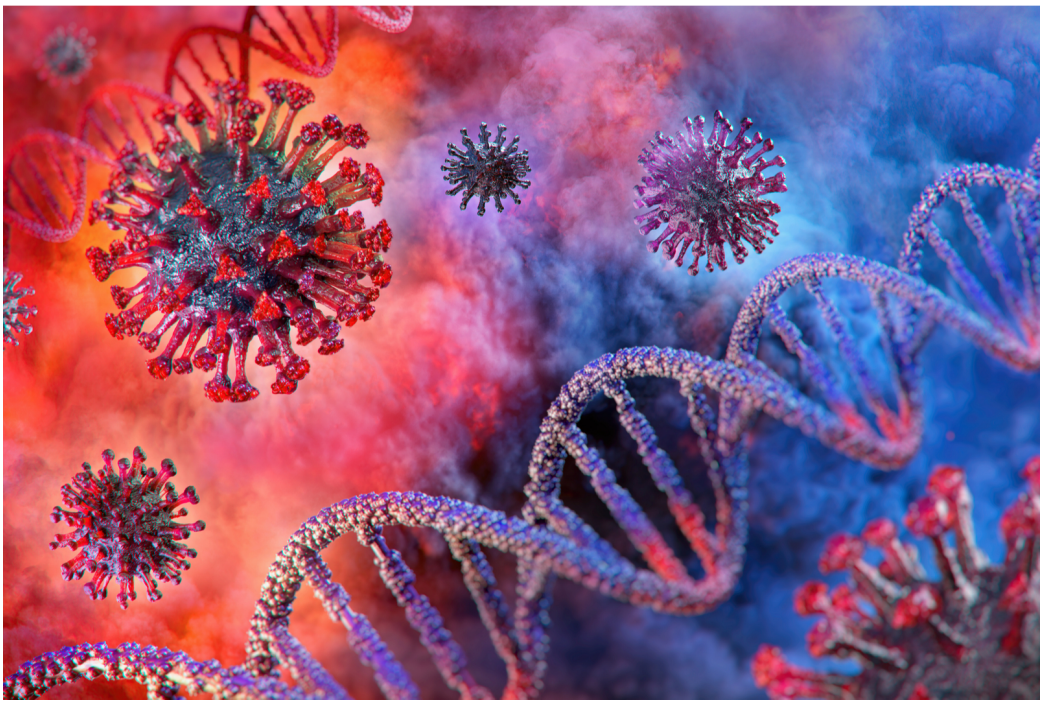
Smart Nation 計劃辦公室計劃的負責人說：“新加坡 GovTech 現在正在全天候工作，以完成我們的協議參考文件和參考實施，以便其他人可以部署自己的 TraceTogether 風格-每種都實現 BlueTrace 協議。”Vivian Balakrishnan 在 Facebook 帖子中說。

“我們相信，將我們的準則發布給全世界將有助於在應對不尊重邊界，政治制度或經濟的全球威脅方面增強信任和協作。”

目录

Part II

背景



嚴重特殊傳染性肺炎疫情，是在 2019 年至 2020 年間由嚴重急性呼吸系統綜合症冠狀病毒 2 型（SARS-CoV-2）所引發的全球大流行疫情。疫情在年冬首次爆發於中華人民共和國湖北省武漢市，隨後在 2020 年初迅速擴散至全球多國，逐漸變成一場全球性大瘟疫，是全球自第二次世界大戰以來面臨的最嚴峻危機。截至 2020 年 4 月 24 日，全球已有 220 多個國家和地區累計報告超過 260 萬名確診病例，超過 18 萬名患者死亡。

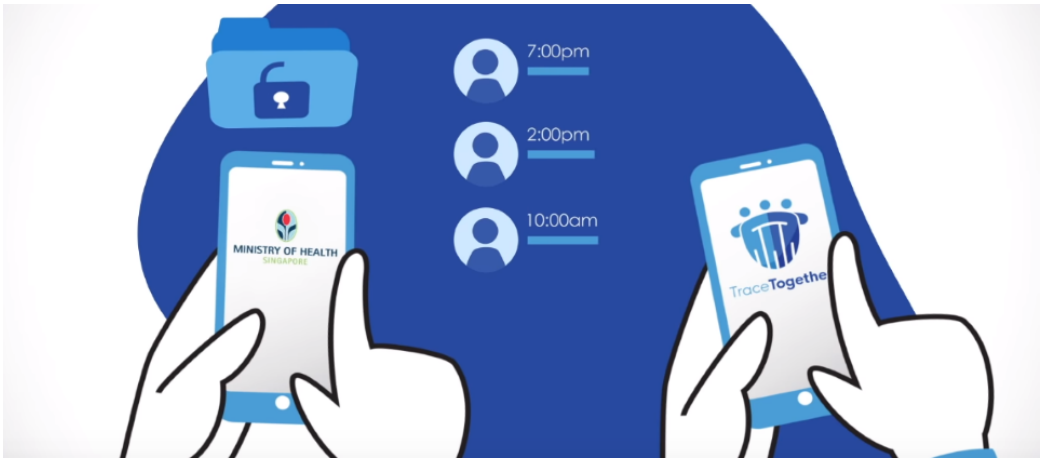
目前公認的數據統計認為，首宗感染個案發病時間是 2019 年 12 月 1 日。首位前往醫院就診的患者可能出現於 12 月 12 日。12 月 26 日，武漢市呼吸與重症醫學科醫生張繼先最早發現和上報此不明原因肺炎，並懷疑該病屬傳染病。其後該病在武漢市出現大規模疫情。2020 年 1 月 23 日，武漢市新冠肺炎疫情防控指揮部宣布採取疫區封鎖隔離措施，是近代公共衛生史上第一例將 1100 萬人口的大城市採取封鎖措施。3 月 12 日，中華人民共和國國家衛生健康委員會宣布，總體上中國大陸本輪疫情流行高峰已經過去。3 月 23 日，中華人民共和國國務院總理兼中央應對疫情小組組長李克強宣布，以武漢市為主戰場的中國本土疫情傳播已基本阻斷，抗疫取得初步成功。

1 月 13 日起，疫情陸續蔓延到泰國、日本及韓國等國家，1 月 21 日

波及美國西雅圖，為亞洲以外的首例確診個案。在 1 月 30 日中國境外證實有 3 個國家出現社區傳播，世界衛生組織於當日宣布疫情為「國際公共衛生緊急事件」。2 月底義大利、韓國與伊朗三國的確診人數急速增加，29 日，世衛組織將疫情的全球風險級別提升為「非常高」。3 月 11 日，世衛組織宣布此次疫情已構成「全球大流行」，世衛組織並於 3 月 13 日表示歐洲已經成為當前大流行瘟疫的中心。

病毒潛伏期一般最長多達 14 天，有個別病例可達 24 天。即使沒有發燒，沒有感染跡象或僅有輕微感染跡象的感染者也可以將病毒傳染給他人，症狀篩查無法有效檢測。這意味著它比中東呼吸綜合症（MERS）或嚴重急性呼吸系統綜合症（SARS）的疫情更難控制。實際上，這次疫情僅花四分之一的時間就造成 SARS 事件十倍的確診數字。目前尚無針對新型冠狀病毒的預防疫苗及治療方法。世界衛生組織助理總幹事布魯斯·艾爾沃德認為瑞德西韋是目前「唯一可能具有真正的功效」的藥物；而對症治療則是目前的主要治療方法。全世界目前有至少 3 種新型冠狀病毒肺炎的預防性疫苗正在處於試驗階段。目前對病症的研究仍存在知識差距，包括病毒來源、病毒發源地、發病機理、病毒的致病性和傳播能力等關鍵因素仍不能確定。

疫情危機持續同時，亦遇上全球醫療用品供應不足的問題。而疫情擴散對全球航空、旅遊、娛樂、體育、石油市場、金融市場等方面造成巨大影響。



為了控制疫情，新加坡將開源用來抗疫的 TraceTogether Android APP。

TraceTogether 採用的技術，是由新加坡數位服務部門所研發的藍牙追蹤（BlueTrace）協定，它以藍牙相對訊號強度指標（RSSI），來蒐集與紀錄兩個裝置之間的近距離接觸與時間，相關資訊在手機上的儲存時間為 21 天。

另一方面，新加坡政府會依據所建立的新型冠狀肺炎確診患者資料庫，追查在過去 14 天，曾與這些患者近距離接觸的民眾，再提出警告。

為了避免危害使用者的隱私，TraceTogether 並不會蒐集手機的位置資訊，且所蒐集的資料只存放在手機上，而且是加密的；除非使用者曾與確診者近距離接觸，否則政府單位永遠不會存取手機上的資料。

此外，在兩支手機互換資訊時，彼此間是以隨機的 ID 進行通訊，並未涉及任何身分資訊；電話號碼與 ID 的配對資訊則是存放在另一伺服器上，只有在必要時才會被存取。BlueTrace 設備通過在藍牙上交換消息來記錄彼此的遭遇。為了保護用戶的隱私，這些消息無法透露用戶的身份。此外，這些消息不能包含靜態標識符，以防止第三方隨時間推移跟踪用戶。

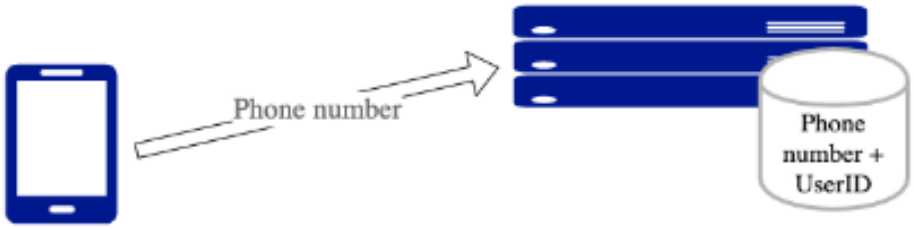
使用 BlueTrace 的設備既充當中央設備又充當外圍設備，並且可以在這些角色之間交替。當兩個設備連接時，中央設備讀取 Pe-ripheral 的 Encounter Message，然後回寫其自己的 Encounter Message。每個連接都允許在中央和外圍設備之間進行雙向數據交換。允許雙向通信可以促進對稱性並解決某些設備（可能是可穿戴設備）只能用作外圍設備的局限性。

Part III

方法

0.1 藍芽追蹤技術

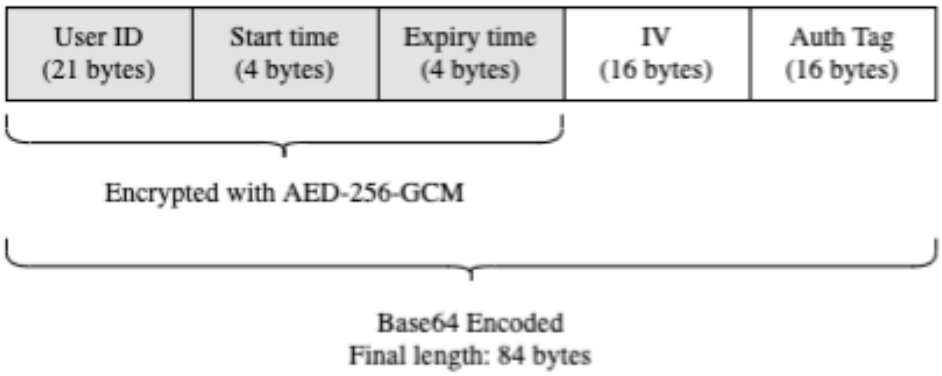
0.1.1 User registration and assignment of UserID



(a) User registration

當實施 BlueTrace 的應用程序的用戶使用其電話號碼註冊時，後端服務將生成唯一的隨機 UserID 並將其與用戶的電話號碼相關聯。電話號碼是唯一可個人識別的信息用戶要求。如果發現用戶長時間與感染者接觸，可以使用電話號碼與用戶聯繫。用戶註冊不需要電話的 BlueTrace 替代實現也是可能的。這些可能僅依靠推送通知令牌來提醒單個用戶。

0.1.2 Generation of TempIDs



(b) Format of TempID

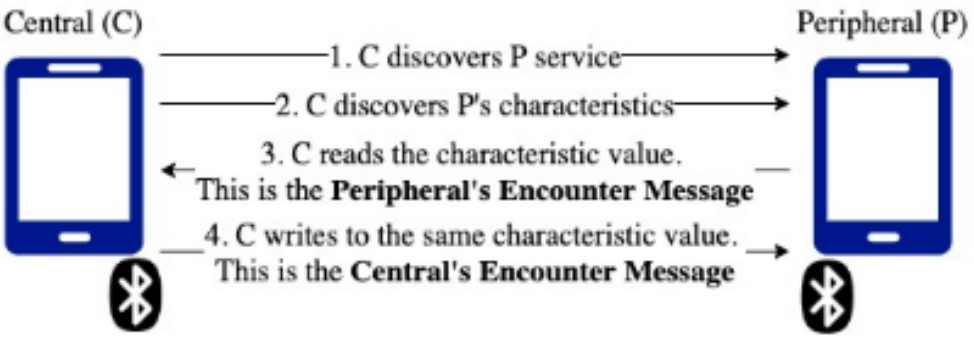
BlueTrace 設備通過在藍牙上交換消息來記錄彼此的遭遇。為了保護用戶的隱私，這些消息無法透露用戶的身份。此外，這些消息不能包含靜態標識符，以防止第三方隨時間推移跟踪用戶。但是，當受感染的用戶將這些消息上載到衛生機構時，該機構必須能夠從消息中獲取聯繫信息。BlueTrace 通過讓用戶交換臨時 ID（TempID）來解決此問題。每個 TempID 包括一個用戶 ID，創建的時間和使用 AES-256-GCM 對稱加密的到期時間，然後使用 Base64 編碼。僅健康授權機構擁有用於加密和解密 TempID 的秘密密鑰。每個 Tem-pID 都有一個隨機的初始化矢量（IV）生成.TempID 還包括兩個加密參數：IV 輸入和一個 Auth 標籤（用於完整性檢查）。

TempID 的壽命很短（15 minutes）。這有助於減少重發機會的機會，從而減輕重犯的影響。如果惡意用戶通過重新廣播他們的消息來冒充其他用戶，則他們只能在消息出現前的短時間內這樣做。該持續時間可能低於緊密接觸的閾值持續時間，因此不會導致誤報。

為了即使在互聯網連接不穩定的情況下也能確保設備提供有效的 TempID，設備每次都要從衛生機構的後端服務中提取一批轉發的 TempID。

BlueTrace 設備通過藍牙低功耗（BLE）協議交換消息。在 BLE 術語中，設備可以使用外設或中央。外設做廣告的服務，以及中樞掃描外圍設備的廣告以連接到其服務。服務是數據的集合，例如特徵，這些數據可以是特定的數據在設備之間交換，通過中央執行的讀寫操作。BlueTrace 設備在每次“握手”中交換的數據稱為“遇到消息”。

0.1.3 BLE handshake flow



(c) BLE handshake flowD

BlueTrace 設備通過藍牙低功耗（BLE）協議交換消息。在 BLE 術語中，設備可以使用外設或中央。外設做廣告的服務，以及中樞掃描外圍設備的廣告以連接到其服務。服務是數據的集合，例如特徵，這些數據可以是特定的數據在設備之間交換，通過中央執行的讀寫操作。BlueTrace 設備在每次“握手”中交換的數據稱為“遇到消息”。

使用 BlueTrace 的設備既充當中央設備又充當外圍設備，並且可以在這些角色之間交替。當兩個設備連接時，中央設備讀取 Pe-ripheral 的 Encounter Message，然後回寫其自己的 Encounter Message。每個連接都允許在中央和外圍設備之間進行雙向數據交換。允許雙向通信可以促進對稱性並解決某些設備（可能是可穿戴設備）只能用作外圍設備的局限性。

0.1.4 Scanning and advertising cycles

BlueTrace 設備在可配置週期上進行掃描和通告。掃描以大約 15-20% 的佔空比進行，在此期間設備將掃描其他 BlueTrace 設備作為 Central。設備可以選擇在每個掃描週期的長度和占空比中引入隨機抖動，以避免出現鎖步行為。廣告的佔空比較高，約為 90-100%。建議縮短掃描佔空比，以節省資源。還建議掃描和廣告工作週期的總和大於 1，以確保設備有機會看到彼此。

0.2 Bluetooth vs GPS

考慮了藍牙和 GPS 聯繫人跟踪解決方案。下表列出了主要區别。選擇藍牙是因為它能夠以比 GPS 更低的假陽性率對近距離接觸進行分類。鑑於 GPS 精度在室內環境中會下降，因此整個購物中心或摩天大樓都將在單個 GPS 點的誤差範圍內。此外，公眾對位置跟踪的警惕和電池消耗的增加可能會阻礙採用。

	Bluetooth	**GPS**
General Approach	Devices log encounters with other devices. Infected users upload their encounter history.	Devices log their GPS location. Infected users upload their location history.
Accuracy (As a reference, widely-accepted epidemiological parameter for close contact with COVID-19 patient is 30 minutes at a distance of less than 2 metres	Able to approximate close contacts within 2 metres, by filtering encounters by signal strength. Bluetooth has a range of 10 metres in indoor environments, but RSSI follows inverse square law and drops off quickly with distance. However, calibration is necessary for maximal effectiveness as different devices transmit at different powers..	Unable to filter for proximity. Accuracy of 10 metres, which decreases in urban environments with tall buildings. Limited vertical accuracy (for floor detection) means that most people within a single skyscraper would register within the margin of error. Poor accuracy in moving or underground environments like a subway train.
Adoption challenges	Requires high adoption to be effective, because effectiveness is a quadratic function of adoption.	Requires high adoption to be effective, because effectiveness is a quadratic function of adoption unless other data sources are incorporated. Public wariness and possible alarm about tracking location data of individuals could hamper adoption.
Battery use	Low	Medium

0.2.1 Generation of TempID by backend service vs on-device

在參考實現中，TempID 是由後端服務以低溫方式生成的。缺點是這需要設備週期性地連接到 Internet。我們通過一次發布一批 TempID 來考慮沒有連接的時間段（另一種方法是將 UserID 存儲在設備上，並使用非對稱加密密鑰在本地生成 TempID，而後端服務則保存相應的解密非對稱加密密鑰可以由後端服務生成，並使用註冊發送給用戶設備，但是，我們發現，這種加密方案使設備的計算需求超出了 OS 分配的限制，尤其是在後台執行模式下。將設備上的計算需求最小化，服務器端 TempID 生成具有第二個好處，即允許衛生機構通過記錄每日批 TempID 的發行記錄來了解

應用程序的採用和使用水平及其在流行控制中的潛在有效性。然後可以將其用作公共衛生政策干預措施的參考。

0.2.2 Centralised vs decentralised contact tracing

BlueTrace 設想將分散的鄰近數據收集和日誌記錄結合在一起，並具有集中式的聯繫人跟踪功能; 在不使用中央服務器的情況下，將交流消息和遇到的歷史記錄交換並存儲在分散的對等網絡中，我們推遲集中式收集和處理數據診斷到 COVID-19 的最後時刻，然後在 OpenTracereference 實現中將此數據提供給受信任的公共衛生機構。根據公共衛生機構所處的現行信任環境，其他轄區可能會有不同的考慮因素，可能會傾向於使用類似的混合模型或完全去中心化的模型。我們看到，純粹的去中心化聯繫追踪系統會帶來各種挑戰。錯誤地聲明自己感染了病毒，將導致其他用戶不必要的焦慮和恐慌，並削弱對系統的信任。因此，為了防止濫用，用戶必須以某種形式的授權將自己標記為積極的 COVID-19 案例，或者上載遇到的歷史記錄。最終，這必須由具有證書的醫療機構或醫護人員提供，他們可能或可能不是公共衛生當局的傳染病監視系統的一部分，但可能必須通過植根於中央公共衛生當局的信任鏈來獲取上載授權代碼。這也有利於確保將有關這種接觸者追踪系統的流行病以及其有效性和有效性的相關信息提供給公共衛生當局，以幫助規劃公共衛生干預措施。最後，集中化方法的另一個優勢是使人們可以保持在循環評估適當的後續行動。

Part IV

結果

新加坡接連爆發多起移工（新加坡稱「客工」）宿舍「COVID-19」（2019 年新型冠狀病毒疾病）群聚感染。22 日，新加坡新增 1016 起確診病例，當中大多感染者仍是移工，累計病例為 1 萬 141 起，總理李顯龍 21 日發表談話，宣布「阻斷措施」（Circuit Breaker）延長至 6 月 1 日。

新加坡被視為善用科技防疫的國家，《海峽時報》報導，李顯龍在談話中說「我們需要每一個人的合作和使用」智慧型手機行動應用程式（App），並鼓勵人們下載 TraceTogether。該 App 是由政府科技部門研發，透過藍牙訊號進行感染者追蹤（Contact tracing）的工具。

李顯龍指出，該國政府也在開發其他 App，「有些關於隱私權的擔憂，但是我們將會權衡，這和讓阻斷措施得以結束帶來的益處，同時維持安全開放。」目前新加坡並未強制每位國民下載。

感染者追蹤，意指追蹤所有曾和感染者接觸的人，進而控制傳染，這是一項極為耗費人力的工作。《紐約時報》報導指出，新加坡 1 月 23 日出現了第 1 例病例後，就開始詳細追蹤了與每一名感染者有過密切接觸的人，也在移工感染病例遽增之前成功掌控疫情。

透過數位裝置的普及，科技可以在追蹤過程中扮演重要角色。TraceTogether 是世界第一個藍牙感染者追蹤 App，由新加坡政府科技局（GovTech）的政府數碼服務團隊開發，在 3 月 20 日推出。

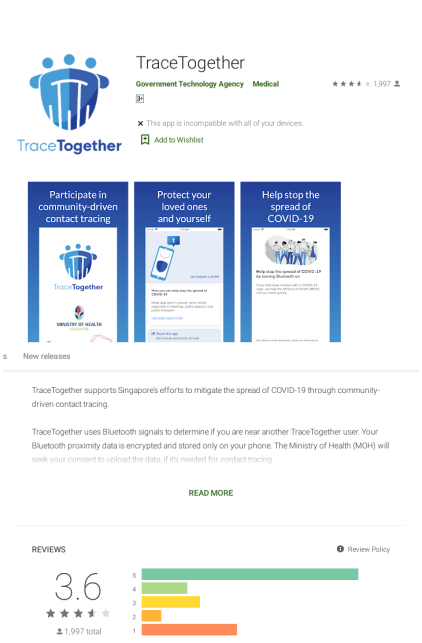
TraceTogether 透過藍牙相對訊號強度指標（RSSI）記錄用戶之間的接觸時間，一旦用戶確診，衛生部（MOH）會根據過去 14 天的行動繪出地圖。基於數據安全考量，相關紀錄會在手機保留 21 日，官網中指出「所有數據只會保存在你手機，不會直接分享給衛生部。如果衛生部有需要，他們會尋求你的同意。」

新加坡人口約 570 萬，《海峽時報》報導，4 月 1 日時，新加坡國家發展部長 Lawrence Wong 表示，TraceTogether 約有 100 萬下載次數，意即約 6 人中有 1 人下載。《路透社》報導，TraceTogether 在 3 月中剛推出時，新加坡確診病例為 385 例，來到李顯龍發表談話的 21 日，累計確診已超過 9000 例，TraceTogether 仍然維持大約 5 人中有 1 人下載。

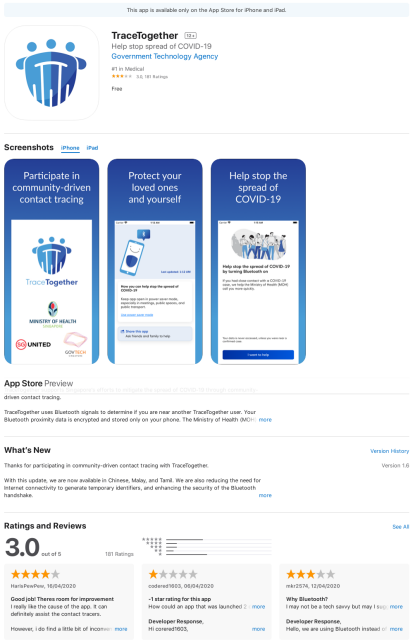
Part V

結論

然而在實際使用上 TraceTogether 依然不受大眾信用，我們可以從此 APP 在 Google Play 和 Apple Store 上的評分來看此應用程序依然有許多問題，像是後台耗電、個資隱私問題、還有程序優化。



(d) TraceTogether on Google Play



(e) TraceTogether on App Store

我們依然能看到即使藍芽追蹤的技術有確保隱私個資的洩漏機制，仍然無法獲取部份人的信任，但是為有效控制疫情全球進最大的努力並使用這類技術避免疫情擴散。

澳大利亞首席醫學官布倫丹·墨菲（Brendan Murphy）表示，該國一直在密切關注新加坡為防止 COVID-19 進一步傳播所採取的措施，其中包括新加坡已採用的一些技術。

墨菲在新西蘭國會聽證會上說，澳大利亞“非常熱衷”使用新加坡的冠狀病毒接觸追踪應用程序 TraceTogether。

他說：“我們實際上已經從新加坡獲得了代碼，我們非常熱衷於使用它，甚至比新加坡更廣泛地使用它。”

“顯然，與社區進行了一次關於其可接受性的對話，但是我們認為，TraceTogether 應用程序的構想確實非常出色，如果您對其進行了適當的

編程並獲得了正確的社區支持，那麼我們“正在積極地將其視為一項措施的一部分，該措施可能被用於考慮放鬆措施。”

TraceTogether 應用程序輕按藍牙信號以檢測附近的其他參與移動設備，從而使它們可以識別需要時保持密切聯繫的那些設備。

該應用程序能夠估計 TraceTogether 智能手機之間的距離以及此類交互的持續時間。

它可以識別參與的 TraceTogether 用戶，這些用戶彼此之間相距不超過 30 米，且相距不超過 2 米。然後，將數據捕獲，加密並在用戶手機上本地存儲 21 天，這涵蓋了病毒的潛伏期。

TraceTogether 基於 BlueTrace 協議構建，該協議由新加坡政府技術局的政府數字服務團隊設計。

上個月，新加坡政府宣布將開源該應用程序。

Smart Nation 計劃辦公室計劃的負責人說：“新加坡 GovTech 現在正在全天候工作，以完成我們的協議參考文件和參考實施，以便其他人可以部署自己的 TraceTogether 風格-每種都實現 BlueTrace 協議。”Vivian Balakrishnan 在 Facebook 帖子中說。

“我們相信，將我們的準則發布給全世界將有助於在應對不尊重邊界，政治制度或經濟的全球威脅方面增強信任和協作。”

TraceTogether 目前擁有超過 100 萬用戶。

談到取消澳大利亞政府針對 COVID-19 採取的一些措施時，墨菲說，只有在絕對有信心擁有一個能夠“積極”鎖定的真正良好的公共衛生應對系統的情況下，才可以放鬆管制。爆發。

“我們正在探索用於聯繫追踪的應用程序建議，現在我們在各州和領地擁有數千名公共衛生工作人員……唯一可以放鬆的方法是，如果您有能力真正進入努力控制疫情，”他說。

“如有必要，我們將更加努力。”

墨菲說，目前在澳大利亞要進行三天的聯繫追踪。

影子總檢察長馬克·德雷福斯（Mark Dreyfus）在周三向媒體發表講話時說，要使跟踪應用程序正常工作，需要公眾充分信任並信任公眾，他們的隱私將受到保護。

他說：“只有在公眾廣泛接受的情況下，跟踪應用程序才能工作，因此

很大一部分澳大利亞人準備將其安裝在手機上。”

“政府在這一領域的記錄不是很好。他們沒有被證明能夠建立信心，例如，在我的健康記錄，電子保存澳大利亞的健康記錄以及整個危機期間，我不得不說政府事實證明，這種方式並不能很好地吸引澳大利亞人的信任。

“它需要在這個跟踪應用程序上做得更好，因為我再說一遍，除非澳大利亞人信任，有信心，並且將這個應用程序上傳到手機上將保護他們的隱私，否則它將無法正常工作。”

在撰寫本文時，世界衛生組織報告說，已經確認了近 180 萬例病例，其中有 11.7 萬多人死於該病毒。澳大利亞報告了約 6,400 例病例，其中 61 人死亡。

澳大利亞已進行了 336,000 多次測試。

Part VI

Reference

- TraceTogether, safer together
- 嚴重特殊傳染性肺炎疫情 - 維基百科
- 【科普長文慎入】披羊皮的大野狼！新冠病毒裝無害入侵人體　7 種老藥新用抓「詐騙」- 未來城市
- 新加坡將開源用來抗疫的 TraceTogether 技術
- BlueTrace: A privacy-preserving protocol forcommunity-driven contact tracing across borders
- 手機 App 如何協助追蹤感染者？新加坡總理李顯龍：「我們需要每一個人的合作」
- TraceTogether on Google Play
- TraceTogether on App Store
- Australia looks to go harder with use of COVID-19 contact tracing app