COVID-19, Technology and Data Privacy: A Call to Action for Governments

Witness Webinar Working Group Convenor, Victoria Lemieux
June 2, 2020

Objective of this Brief
This policy brief discusses the question: “Can Governments respond to the COVID-19 pandemic and still respect personal privacy?”

It aims to:
⇒ present a brief environment scan of how technology is being applied across many countries to effectively control the resurgence or second wave of the pandemic (see Appendix)
⇒ synthesize the views of global experts relating to COVID-19, technology and data privacy
⇒ offer contextualized potential solutions to inform policy decision making i.e. how governments can respond effectively and in a timely manner.

Background
Covid-19
COVID-19 is an infectious disease caused by a recently discovered coronavirus, namely SARS-CoV-2. Coronaviruses are known to cause respiratory infections ranging from mild to severe in humans. COVID-19 is claimed to have emerged in December 2019 and has evolved to become a life-threatening global pandemic [1].

Governments around the world are searching for solutions to respond effectively to this crisis. Initial efforts ranged from control measures, such as implementing quarantines and physical distancing, to ramping up efforts to find a vaccine and testing for the virus.

How this brief was developed?
The brief draws upon the “Witness Seminar” methodology, developed in the 1990s by The History of Twentieth Century Medicine Group of the Wellcome Trust [2] wherein group discussions of special interest on selected topics are made and proceedings are transcribed/published without the goal of reaching consensus. With the physical distancing measures implemented in Canada, a one-day, “Witness Webinar” was held via Zoom platform on May 5, 2020. The witnesses included individuals from academia, the public sector, the private sector and non-governmental organizations with backgrounds in public health policy and research, biomedical research, ethics, law, technology, communications, privacy and data protection, civil liberties advocacy, primary health care, art curation, and entrepreneurship who were from Canada, the United States, Australia, the UK, Ireland, Switzerland, and Japan. The proceedings (see link: https://covidprivacy.pwias.ubc.ca/). The synthesis in this brief is intended to present a summary of focal themes that emerged from an analysis of the Witness Webinar discussion. It is not intended to represent a consensus view.
At present, efforts from governments are focused on preventing a second wave, i.e., reopening economies safely, relaxing quarantines, yet preventing resurgence of the disease.

Technology
Governments are discussing the use of or, in some cases, already implementing technologies, such as ‘contact tracing apps’, quarantine enforcement apps, ‘immunity passports’, and health screening apps. Examples of these technologies are provided in the appendix.

Data Privacy
While these technologies are being implemented across many countries effectively (for example, in Taiwan, Singapore, Australia, Finland) there are contextual concerns with privacy raised in many countries, including Canada.

Concerns and Potential Solutions
Mass Surveillance and Loss of fundamental freedoms
According to a number of the lead witnesses, the use of contact tracing apps raised concerns about mass surveillance and the potential loss of fundamental freedoms [3]. Witnesses also identified that forcing individuals to use immunity passports, or socially stigmatizing them if they refused, is also a challenge as it essentially removes individuals’ freedom to choose [4].

Government overreach i.e. temporary surveillance becomes permanent
Some witnesses expressed apprehensions about temporary data collection and surveillance measures that can be expanded or made permanent in the long-term.

Some witnesses pointed to historical examples that tracking and surveillance of citizen activities can often continue after an emergency [5]. As lead witnesses observed, this phenomenon occurs as governments like to retain their powers (and, by extension, data they hold) and are reluctant to relinquish this power, once they have acquired it [6].

Obtaining Citizen Consent
Witnesses also pointed to a basic flaw with current approaches to obtaining consent [7]. Some researchers argue that the use and availability of unconsented data is necessary and justifiable in pandemic contexts where the common good is prime [8]. As evidenced by lead witnesses (and also from research evidence), citizens will agree to the use of unconsented data when they understand the urgency of the common good, provided there is appropriate governance as well as communication with citizens [9].

Discrimination and Marginalization
Lead witnesses also cautioned that fear of mass data collection and surveillance can be acute among specific segments of the population [10]. For some groups, the conversations about using health technologies, for tracking and tracing can be “very triggering” [11] of fear as a sentiment. There is potential for data gathered by COVID-19 related apps to further discriminate against already marginalized groups. A recent news report from South Korea describes how a contact tracing app raised controversy over possible discrimination against LGBTQ
individuals due to public disclosure of information that allowed for patient identification [12].

Excessive Privacy protection adversely impacts Public Health
Some lead witnesses pointed to the risk of critical public health data being unavailable due to excessive privacy restrictions and saw the value of keeping collected information even after the pandemic for research advancing the common good [13].

Witnesses pointed to privacy restrictions causing barriers to secondary use of clinical data in medical research or preventing the tracking and tracing of older adults who are living with dementia and who wander and go missing permanently [14].

COVID-19, Technology and Privacy: Call to Action
Design and Use Privacy-Preserving Technologies
In order to effectively realize the benefits of technology, lead witnesses emphasized the need for human-centred, collaborative, privacy-by-design applications (e.g. contact tracing apps) and also the use of privacy-preserving technologies (e.g. Blockchain) [15]. The Google-Apple API was mentioned as a well-suited example of a privacy preserving approach [16]. A number of witnesses described the advantages of Self-Sovereign Identity (SSI) technologies, which place control of data in individuals’ own hands. The basic tenets of SSI are that: (1) every individual is the original source of their own identity; (2) identity is not an administrative mechanism for others to control; and (3) each individual is the root of their own identity and central to its administration [17].

Witnesses recommended privacy impact assessments as a measure to ensure that all technologies preserve privacy and handle data appropriately [18].

Maintain Trust through Transparent and Timely Communications
Witnesses noted the importance of being transparent with citizens, explaining how technologies involved in data collection actually work, how their data will be collected, and the purpose for which data will be used [19]. Individuals need to understand why the data collection is necessary and that its use is proportionate and justifiable.

The Australian government’s approach to introducing a contact tracing app was mentioned by a lead witness as a good example of how to communicate/engage with citizens and maintain trust [20] while effectively implementing a privacy preserving approach. The lead witness mentioned the introduction and implementation of new legislation that clearly indicates to citizens that their data will not be available for any misuse or control/surveillance in any manner after the pandemic had passed (end of 2020), even with a court order. Furthermore, the data collected is only available to public health authorities within affected individuals’ own geographic jurisdictions in order to implement appropriate public health measures, and for a certain period of time only [21]. A recent report suggests that Australian government communication around the role of the app in reopening the economy safely has had
an impact on the public’s use of the app [22]. The key learning from this experience is directly transferable to the Canadian context, according to a lead witness from Australia [23].

Decide Now on an “After the Pandemic” Future
Lead witnesses raised the need to decide up-front on how much of any data collected may be retained, and for what purposes [24]. It was noted that information and privacy commissioners have an important role to play in such decisions [25]. Witnesses also urged caution when introducing new legislation in a time of crisis. If legislation is introduced, or when emergency powers are invoked, they recommended ensuring there are sunset clauses in place with firm dates and rigorous follow-up [26].

Develop a Prevention and Preparedness Plan for the Next Crisis
Decision-making during a crisis is difficult. Some witnesses pointed out that it will be beneficial to own up to mistakes and consider what lessons there may be to learn [27]. Discussing what worked or what did not work and evaluating actual outcomes against desired outcomes will help in developing a strong prevention and preparedness plan for the next crisis. Witnesses also called for investing now to build a strong digital ecosystem for the future. Finland was mentioned as an example [28]. As part of digital transformation, several witnesses called for development of robust data standards and frameworks (e.g., for consent, interoperability, data aggregation, quality, security, anonymization, pseudonymization, and deletion) [29].

Moreover, several experts called for an engaged approach with citizens and other key stakeholders in order to implement privacy preserving approaches using enabling technologies, drawing upon experiences globally and applying them appropriately to the Canadian context [30].

Lead witnesses did not reach a consensus on the way forward, nor was this the goal of the Witness Webinar. Rather, they presented diverse perspectives through their interactions on this important topic, serving to highlight key issues and pointing to possible policy responses.

Acknowledgements
The author would like to thank the Peter Wall Institute for Advanced Studies and Blockchain@UBC for their support. Thanks are due to fellow Witness Webinar Working Group members Charles Dupras, Holy Longstaff, Samantha Pollard, Jennifer Pougnet, and Chandana Unnithan for their contributions to the Witness Webinar, and their thoughtful comments and contributions to the drafting of this brief. Any errors or omissions remain attributable to the author.

References
[3] See, for example, witness statement from Ann Cavoukian

[4] See, for example, witness statement from Ciara Staunton, COVID-19 Proceedings.


[6] Ibid.


[10] See, for example, Paola Ardiles witness statement, COVID-19 Proceedings.


[15] See, for example, witness statements from Ann Cavoukian, Paola Ardiles and Nadia Diakun, COVID-19 Proceedings.


[18] See, for example, Ciara Staunton witness statement, COVID-19 Proceedings.

[19] See, for example, Chandana Unnithan witness statement, COVID-19 Proceedings.

[20] Ibid.


[25] Ibid.

[26] See, for example, Ciara Staunton witness statement, COVID-19 proceedings.

[27] See, for example, Nora Weber witness statement, COVID-19 Proceedings.

[28] See, for example, Jennifer Pougnet witness statement, COVID-19 Proceedings.

[29] Ibid.

[30] See, for example, Chandana Unnithan and Ciara Staunton witness statements, COVID-19 Proceedings.
## Appendix: COVID-19 Technologies

Prepared by Anisha Dhillon

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Purpose</th>
<th>Stakeholders</th>
<th>Technologies</th>
<th>Data Types</th>
<th>Privacy Concerns/Considerations</th>
<th>Additional Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple jurisdictions</td>
<td>Mobility tracking</td>
<td>Google, Apple, Map users, Public health officials, mobile device manufacturers, businesses, etc.</td>
<td>Google Maps, Google Location Services, Apple Maps, GPS, Bluetooth, cellular data, Wi-Fi, mobile apps</td>
<td>Geolocation data, mobility data</td>
<td>The data collected by Google may be used for contact tracing and exposure notification.</td>
<td>Google’s Mobility Report: Great movement trends over time by geography, across different categories of places such as retail and recreation, grocery and pharmacies, parks, transit stations, workplaces, and residential areas.</td>
</tr>
<tr>
<td>58 countries including major cities, does not include China and North Korea</td>
<td>Mobility tracking</td>
<td>Apple, Apple Maps users, public health officials, and local governments from the 58 countries</td>
<td>Apple Maps, iOS smartphone application, Navigation database.</td>
<td>The data collected includes geographical location, movement patterns, and mode of transportation.</td>
<td>The data is aggregated and not associated with individual users.</td>
<td>Google’s Mobility Report: COVID-19 Mobility Reports.</td>
</tr>
<tr>
<td></td>
<td>Google/Apple COVID-19 Exposure Notification API</td>
<td>Apple, Google, local cities using the API in contact tracing applications, local health authorities.</td>
<td>Apple/Google/Apple COVID-19 Exposure Notification API.</td>
<td>The exposure notification API generates Bluetooth identifiers that are transmitted over 60 minutes.</td>
<td>The API uses Bluetooth technology to identify individuals who may have been exposed to an infected individual.</td>
<td>Apple’s Mobility Report: COVID-19 Mobility Reports.</td>
</tr>
<tr>
<td></td>
<td>World Health Organization</td>
<td>Global health bodies to promote the accuracy of COVID-19 data</td>
<td>WHO, UNICEF, and other partners working with WHO.</td>
<td>COVID-19 case data, including reports on testing, and infection incidents.</td>
<td>Data verification will be validated by authorities where available.</td>
<td>WHO’s COVID-19 update.</td>
</tr>
<tr>
<td></td>
<td>U.K., Germany</td>
<td>Governments, health authorities, companies, etc.</td>
<td>Facial recognition technology, Health data</td>
<td>Health data</td>
<td>Immunity passports have been discussed in various jurisdictions.</td>
<td>Manchester University.</td>
</tr>
</tbody>
</table>

Reference:
<table>
<thead>
<tr>
<th>Country</th>
<th>Region/Province</th>
<th>Initiator</th>
<th>Mobile App/Tool</th>
<th>Data Collection Method</th>
<th>Data Use</th>
<th>Health Privacy Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td></td>
<td>Canada Roche Data Science Coalition; Self-Care Catalysts</td>
<td>Smartphone application</td>
<td>Voluntarily submitted user data (patient data from individuals who have tested positive, suspect they are positive, or who have recovered from COVID-19)</td>
<td>Health officials can access the data through the Roche Data Science Coalition's website. The data is shared with the Roche Data Science Coalition data repository and made available to the research community.</td>
<td>Users can choose to be a data donor or use the app without donating their data. If they choose to donate, their data is de-identified and only shared with the Roche Data Science Coalition.</td>
</tr>
<tr>
<td>Alberta, Canada</td>
<td></td>
<td>Government of Alberta; Alberta Health Services</td>
<td>ABTraceTogether smartphone application; Bluetooth</td>
<td>Proximity data</td>
<td>Health officials are concerned that the app may not be able to detect all cases of COVID-19 due to factors such as battery life and signal strength.</td>
<td>The app is designed to help trace contacts of COVID-19 patients and is not intended to be a substitute for public health investigation.</td>
</tr>
<tr>
<td>Ontario, Canada</td>
<td></td>
<td>Ontario government; hospital/responsibilities</td>
<td>Database containing “critical information” of COVID-19 positive patients</td>
<td>The “critical information” accessible to hospital/responsibilities includes: names, addresses, dates of birth, and whether a person has tested positive for COVID-19</td>
<td>Health officials are made aware of the emergency order to allow them to access the database.</td>
<td>The app is designed to help trace contacts of COVID-19 patients and is not intended to be a substitute for public health investigation.</td>
</tr>
<tr>
<td>Waterloo, Ontario, Canada</td>
<td></td>
<td>VihaHall Corp staff and residents at Sunnydale Home Long Term Care</td>
<td>COVID-19 Electronic Screening with blockchain-enabled application</td>
<td>Health data of long-term care patients</td>
<td>Health officials are made aware of the emergency order to allow them to access the database.</td>
<td>The app is designed to help trace contacts of COVID-19 patients and is not intended to be a substitute for public health investigation.</td>
</tr>
</tbody>
</table>

North America

Health Storylines. (n.d.). The real heroes in the fight against COVID-19 could be you. [https://www.healthstorylines.com]


[Image of a mobile device with a map and a blockchain symbol]
### North America

**U.S.**
- **Visibility tracking:** provides real-time data on human movements and travel behaviors, which could help identify high-risk areas.
  - Mobile marketing industry (ads霸王), public health officials, Policymakers, Universities institutions and public health schools.
  - Location Services on smartphones, e.g. GPS, Bluetooth, cellular cards in NFIP hotspot, satellite towers.
  - Geolocation data (mobility data).
  - By providing location services for enterprise applications, users opt-in for location data collection that is used to fine-tune the mobile marketing industry (Yu, 2023).
  - There are concerns that users have not consented to data collection or they are not aware of how their data is used. Thus, publishing the anonymized and aggregated location data, the mobile marketing industry can support public health officials and disaster managers in formulating the impact of social distancing measures. Privacy advocates warn that “true anonymization of data is difficult and the combination of other publicly available data can result in the ability to track and identify people at an individual level” (Yu, 2023).

**Tracing:**
- The Rapid Medical Products was awarded a contract by the U.S. Defense Department for developing a connected auto lamps to ventilators, helping to address the need for critical supplies. (Fan & Lively, 2020).
- County shields were a task of using GPS to track people to ensure for COVID-19 positive patients who need to follow isolation orders (Taggart, 2020).
- A result of testing ten residents of Nantucket, and the scores are highlighted by the American Civil Liberties Union of Connecticut, the Westport Police Department announced a protocol that would not proceed with the protocol program (Thurber, 2020).
- A result of testing ten residents of Nantucket, and the scores are highlighted by the American Civil Liberties Union of Connecticut, the Westport Police Department announced a protocol that would not proceed with the protocol program (Thurber, 2020).
- The president of the Kansas City County Commission commented: “We do not want to use the GPS while tracking to enforce the quarantines, however, if we must we will. This must take seriously” (Taggart, 2020).

**Tracing:**
- The police department is implementing a full-time program designed to enhance efforts to track victims of sexual violence with the assistance of Doggery, a Canadian commercial drone company. The CEO of Doggery, Cameron Steel, stated that in its current design the drone is not capable of detecting individuals, however, in the coming months the drones are capable of detecting other sources, especially in social distancing protocols from 198 feet away (Kauf, 2020). Due to privacy concerns raised by residents and the American Civil Liberties Union of Connecticut, the Westport Police Department announced a protocol that would not proceed with the protocol program (Thurber, 2020).

**West Virginia, U.S.**
- **Tracking:**
  - Kanawha County, Kanawha County Sheriffs.
  - GPS ankle monitors
  - Geolocation data.

**Westport, Connecticut, U.S.**
- **Social distancing and screening for COVID-19 symptoms:**
  - Westport Police Department
  - Arrests have been made by the police department in Elizabeth, New Jersey, with a recorded message for residents from the mayor, advising residents to socially distance and stay at home (Parriss, 2020).

**Elizabeth, New Jersey, U.S.**
- **Social distancing monitors:**
  - Elizabeth Police Department
  - Arrests
  - N/A

### Central America

**Honduras**
- **Access to telecommunications and permits to leave the house for specific errands:**
  - Civitas is a blockchain enabled application.
  - Government ID numbers are linked to unique blockchain records.

<p>| Country | Access to telecommunications and permits to leave the house for specific errands | Civitas is a blockchain enabled application | Government ID numbers are linked to unique blockchain records |
|---------|--------------------------------------------------------------------------------|
| Honduras | Honduran Government, Emerg, Inter-American Development Bank, Press, News | Civitas is a blockchain enabled application | Government ID numbers are linked to unique blockchain records | Government ID numbers are linked to unique blockchain records allows users to access telecommunications services and will indicate if users are able to leave the house for specific errands. Government does not view the records, only health care providers are able to view the records. Due to lockdown protocols, people are being categorized that determines what day they are permitted to leave their house to run specific errands. Violators may face fines and imprisonment. The permits allow users to travel amongst those days with specific restrictions. Law enforcement does not have access to the records and can only use the permit records if the user is permitted to travel at that given time. Government ID numbers are linked to unique blockchain records allows users to access telecommunications services and will indicate if users are able to leave the house for specific errands. Government does not view the records, only health care providers are able to view the records. Due to lockdown protocols, people are being categorized that determines what day they are permitted to leave their house to run specific errands. Violators may face fines and imprisonment. The permits allow users to travel amongst those days with specific restrictions. Law enforcement does not have access to the records and can only use the permit records if the user is permitted to travel at that given time. |</p>
<table>
<thead>
<tr>
<th>Region</th>
<th>Country</th>
<th>Tracking</th>
<th>Quarantine</th>
<th>Geolocation</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Western Asia</td>
<td>Israel</td>
<td>Tracking</td>
<td></td>
<td></td>
<td>According to government, the cellular data of Israeli citizens is restricted to a select list of authorized officials. Privacy concerns and concerns about the accuracy of the surveillance methods have been raised by various groups. (e.g. Israel Medical Association; Israel Association of Public Health Physicians; the Association of Civil Rights in Israel). Right group v. National police (a judicial association). The High Court of Justice ruled that the government could not continue with the program. April 20th or apply for an extension without notifying the practice rule legislation. Under the government’s regulations, Shin Bet will no longer have access to the cellular data once the tracking program ends, while the Health Ministry will be able to access the data for an additional 10 days. The Israeli parliament approved the extension of the tracking program for another 30 days on May 5, 2020 pending the surveillance powers of Shin Bet. The legislation process concerning the program is under debate. Request approval extension of Shin Bet’s tracking of virus carriers (2020). Times of israel <a href="https://www.timesofisrael.com/extension-of-shin-bet-tracking-of-virus-carriers/">https://www.timesofisrael.com/extension-of-shin-bet-tracking-of-virus-carriers/</a></td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>South Korea</td>
<td>Tracking; quarantine enforcement</td>
<td></td>
<td></td>
<td>The Government of South Korea; Ministry of the Interior and Safety; Korean Centers for Disease Control and Prevention (KCDC)</td>
</tr>
<tr>
<td>South Korea</td>
<td>Tracking; quarantine enforcement</td>
<td></td>
<td></td>
<td></td>
<td>The Government of South Korea; Ministry of the Interior and Safety; Korean Centers for Disease Control and Prevention (KCDC)</td>
</tr>
<tr>
<td>South Korea</td>
<td>Contact tracing</td>
<td></td>
<td></td>
<td></td>
<td>The Ministry of Land, Infrastructure and Transport (MOLIT), the Government of South Korea; healthcare officials; law enforcement</td>
</tr>
<tr>
<td>China</td>
<td>Ease lockdown restrictions</td>
<td>Chinese government; mobile payment platform, Alipay</td>
<td></td>
<td></td>
<td>The Alipay Health Code app uses the Alipay and WeChat/WeChat Mini Program applications; QR Codes</td>
</tr>
<tr>
<td>China</td>
<td>Medical supply chain blockchain solution</td>
<td>Chinese government; Zhengzhou Provincial Health Commission and the Economy and Information Technology Department, Alipay</td>
<td></td>
<td></td>
<td>Blockchain enabled solution to address concerns in the medical supply chain</td>
</tr>
</tbody>
</table>
**Asia-Pacific**

<table>
<thead>
<tr>
<th>Country</th>
<th>Quarantine enforcement</th>
<th>Government or country agency</th>
<th>Technology or application</th>
<th>Location data or contact data</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hong Kong</strong></td>
<td>Quarantine enforcement of inbound travelers</td>
<td>Government of Hong Kong; Competition Technology</td>
<td>Queering technology, StayHomeSafe; a smartphone application that connects to a tamper-proof bracelet since the user scans the QR code on the bracelet</td>
<td>Does not track location algorithm of application relies on signals that are unique to the wearer's home</td>
<td>According to Competition Technology, the queering technology of the application relies on GPS, Bluetooth, tracking. Application developers state the application is privacy preserving because the algorithm learns from the sample signals of the user's home and depends on signals such as the home Wi-Fi network, Wi-Fi from roadway, Bluetooth, and cellular network. (Hu, 2020).</td>
</tr>
<tr>
<td><strong>Taiwan</strong></td>
<td>Tracking; Quarantine enforcement</td>
<td>Government of Taiwan (Government of the Republic of China); telecom/telecoms companies</td>
<td>Monitoring of phone signals</td>
<td>Location data; cell data</td>
<td>Referenced as a mobile phone-based &quot;electronic fence.&quot; Taiwan's approach monitors phone signals to inform law enforcement if an individual is in contravention of their home quarantine orders or if they have turned their phone off. Concerns have been expressed regarding the intrusive nature of the approach, especially with respect to the government's partnership with telecommunications companies. (Lee, Y., 2021; March 20) Taiwan's new electronic fence for quarantines leads wave of virus monitoring. Reuters. <a href="https://www.reuters.com/article/china-health-coronavirus-taiwan-same/electronic-fence-for-quarantines-leads-wave-of-virus-monitoring-20210320">https://www.reuters.com/article/china-health-coronavirus-taiwan-same/electronic-fence-for-quarantines-leads-wave-of-virus-monitoring-20210320</a></td>
</tr>
<tr>
<td><strong>India</strong></td>
<td>Contact tracing</td>
<td>Government of India Ministry of Electronics and Information Technology; Ministry of Home Affairs</td>
<td>Azuga Setu; smartphone application; Bluetooth, GPS</td>
<td>Location data; proximity data</td>
<td>Concerns have been expressed about the transparency of the application, and the transfer of data to a central server once a user indicated through the application that they are COVID positive. Additionally, while the application stated as an voluntary, the Ministry of Home Affairs announced the application was mandatory for all public and private employees. In response to privacy concerns which have been accumulating since the application's implementation in early April, the code for the application went open source on GitHub on May 21st. The government announced a bug bounty program offering cash rewards to individuals who are able to find security flaws and any vulnerabilities. (Gupta, P., 2021; May 17) Hackers found bug in Azuga Setu can win you $1 lakh to $2.5 lakh through the Indian government's bug bounty programme. Business booster India. <a href="https://www.businessbooster.in/article/tech/bugs/techs/bugs/azuga-setu-can-win-you-1-lakh-to-2-5-lakh-through-the-indian-governments-bug-bounty-programme/article-twin76330345.html">https://www.businessbooster.in/article/tech/bugs/techs/bugs/azuga-setu-can-win-you-1-lakh-to-2-5-lakh-through-the-indian-governments-bug-bounty-programme/article-twin76330345.html</a></td>
</tr>
<tr>
<td><strong>Singapore</strong></td>
<td>Contact tracing</td>
<td>Singapore Ministry of Health and Government Technology Agency (GovTech)</td>
<td>TraceTogether; smartphone application; Bluetooth</td>
<td>Proximity data; duration of contact data</td>
<td>TraceTogether is a voluntary contact tracing application, as with COVIDSafe. TraceTogether does not collect location data. Proximity and duration of contact data is deleted from the mobile device every 21 days. (Bak Trace. 2021, Policy: <a href="https://bluetrace.io/policy">https://bluetrace.io/policy</a>)</td>
</tr>
<tr>
<td>Country</td>
<td>Area</td>
<td>Government/Agency</td>
<td>Network/Technology</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------</td>
<td>--------------------------------------</td>
<td>---------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Russia</td>
<td>Eastern Europe and Northern Asia</td>
<td>Government of Russia</td>
<td>Facial recognition cameras and AI</td>
<td>The network of facial recognition cameras is connected to a COVID-19 central server that uses AI to identify an individual captured leaving their home and determine whether they are considered to be an &quot;endangered person. (Russia Uses Bimetric Surveillance, 2020). Prior to the pandemic, the facial recognition cameras have been used to identify protesters and have since continued to be used by privacy groups and citizens (Russia Uses Bimetric Surveillance, 2020). The system has informed Moscow police of “alleged 2018 violations of quarantine” (Russia Uses Bimetric Surveillance, 2020).</td>
<td></td>
</tr>
<tr>
<td>UK</td>
<td>Europe</td>
<td>NHS, UK government</td>
<td>NHS COVID-19 smartphone application, Bluetooth</td>
<td>When a user chooses to report themselves through the application as showing symptoms of COVID-19 their data is automatically shared to a central server. Once the data is uploaded to the central server, the user cannot delete the information. The government has indicated that the data will be used towards public health research. (Lomas, 2020). The contact tracing app taken by the NHS has caused concerns among cybersecurity experts due to concerns regarding privacy and how the data is stored and exchanged between smartphones. The application will not be able to use Google and Apple’s API framework due to the centralized approach. (Hamilton &amp; Ghosh, 2020).</td>
<td></td>
</tr>
<tr>
<td>The Netherlands</td>
<td>Europe</td>
<td>Government of the Netherlands, Tymenzo</td>
<td>Blockchain enabled decentralized marketplace for critical medical supplies</td>
<td>Timenzo, a blockchain solution platform is partnering with the Dutch government to address concerns in the medical supply chain and the need for critical supplies. Using blockchain technology, Timenzo aims to create transparency about the entire and critical supply lines such as PPE and ventilators, and reduce the risk of price hoarding, quality issues and even fraud in the network, allowing for a single version of the truth that will enable critical product distribution (Van Hook &amp; Lacity, 2020).</td>
<td></td>
</tr>
<tr>
<td>Switzerland</td>
<td>Europe</td>
<td>Government of Switzerland, Federal Office of Information Technology, Systems and Telecommunication (FOI), the Swiss Federal Institute of Technology (EPFL) and ETHZ.</td>
<td>SwissCovid smartphone application uses Google and Apple’s API, Bluetooth</td>
<td>SwissCovid is the first application to use Google and Apple’s Exposure Notifications API. One of the developers of SwissCovid stated: “in our design, information is processed locally and all data is automatically deleted after 21 days. In addition, no user personal data is stored centrally, and contact tracing data even leaves the phone unless authorized by the user. “The SwissCovid app is also open sourced, as that’s how it works and implementation will be available for public inspection” (Forrest, 2020). Through the amended Epidemic Act, public health authorities will be able to change SwissCovid. It is voluntary and will be the first such case within Switzerland. (Forrest, 2020).</td>
<td></td>
</tr>
</tbody>
</table>

References:
- "The NHS COVID-19 app is centralized, compared to the decentralized approach of other contact tracing applications. Like the other applications, Bluetooth technology is still used to store proximity data exchanged between smartphones. The application will not be able to use Google and Apple’s API framework due to its centralized approach.,” (Hamilton & Ghosh, 2020)
<table>
<thead>
<tr>
<th>Country</th>
<th>Contacting</th>
<th>Government/Agency/Service</th>
<th>Application/Device</th>
<th>Feature/Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Western Australia</td>
<td>Tracking, quarantine enforcement</td>
<td>Western Australia State Emergency Coordinator (law enforcement)</td>
<td>TraceSafe, smartphone application</td>
<td>Proximity data</td>
<td>The Emergency Management Amendment (COVID-19) Bill 2021 allows the State Emergency Coordinator of Western Australia to enforce wearable electronic monitoring devices and other forms of home surveillance devices for individuals who are in containment or self-isolation orders. The power of the State Emergency Coordinator of Western Australia can only be activated in a state of emergency, however, the enforcement of wearable electronic home surveillance does not have a real-time capability corresponding to the containment of the COVID-19 pandemic, which has caused concerns among privacy advocates and health officials (Fernandes, 2020). The only amendment that has a real-time capability is the traceSafe, which is a state of emergency contains individuals to answer questions from law enforcement to that officials may gather contact tracing information (Fernandes, 2020).</td>
</tr>
<tr>
<td>Australia</td>
<td>Contacting</td>
<td>Australian Government Department of Health, residents of Australia, Amazon Web Services</td>
<td>TraceSafe, smartphone application</td>
<td>Proximity data</td>
<td>Without collecting location data, the TraceSafe application is able to identify other devices using COVIDSafe using Bluetooth technology and records proximity data that is encrypted and securely stored on the user's mobile device (Department of Health, 2020). The encrypted information is inaccessible to the user and can only be viewed by health officials if they receive permission from the user. When a user grants health officials permission to the encrypted information it is uploaded to a highly secure informatie storage system hosted by Amazon Web Services (AWS) (Nicholls &amp; Bassett, 2020). The encrypted contact information is retained for 21 days after which it is permanently deleted, keeping in line with the COVID-19 isolation period and testing time estimates. The Health Minister issued a Determination under the Emergency Act protecting people's privacy and restricting access to information from the app. The Australian Government will introduce self-regulation in Parliament to work towards centering the privacy protections outlined in the determination into primary legislation (Attorney-General's Department, 2020). As a result, it is a critical offensive to use the application which is not regulated by the app. Meaning, healthcare officials can only access information for contact tracing purposes. The determination states that the data must remain in Australia, and in terms of legislation that data cannot cross borders will ease the concerns of those worried data is a critical offense being shared through AWS and therefore being subjected to U.S. legislation under the CLOUD Act (Nicholls &amp; Bassett, 2020).</td>
</tr>
<tr>
<td>New Zealand</td>
<td>Contacting</td>
<td>New Zealand Government National Contact Service (NCDS)</td>
<td>NZ COVID Tracer, smartphone application, QR codes</td>
<td>Previously visited public location data</td>
<td>Users will create a “digital diary” of the locations they have visited by scanning QR codes posted at the entrances of businesses and public spaces. The information is stored in the app for 21 days after which it is automatically deleted. NZ COVID has gone through independent security testing and the Ministry of Health has consulted with the Privacy Commissioner. The digital diary entries are stored on the user’s phone and the user has the choice to share their data with the NCDS. The next update of the app will be able to notify individuals who have been at the same location at the same time as someone who tested positive for COVID-19, allowing them to avoid their digital diary contact traces.</td>
</tr>
</tbody>
</table>

References: