# SPNET: NOTE FOR NATIONAL DEFENCE:
# Privacy Issues in AI-Based COVID-19 Contact Tracing Apps


**SUMMARY**

a) One of the current challenges in the world is spread of COVID-19. To control the spread of this lethal disease a number of countries such as South Korea, Singapore, and Canada have launched monitoring mobile software contact tracing apps.
b) COVID-19 contact tracing apps utilize the Bluetooth and GPS signals to determine and log the proximity of users from one another. The log history can be used to locate individuals that have been in close contact with confirmed infected patients of COVID-19.
c) Despite their benefits, COVID-19 contact tracing apps can violate the privacy of users. Certain guidelines, such as obtaining consent of users for collecting, using, and disclosing their information should be provided to protect users' privacy.


## CONTEXT

- In response to the COVID-19 pandemic, mobile software applications that use Bluetooth and GPS signals have been developed and utilized in public. In South Korea, by using specific data banks and artificial intelligence (AI), the government has the capability of tracking and discovering a COVID-19 patient's routes in any given day in less than 10 minutes. Also, the government of South Korea monitors self-isolating individuals by using a mobile app that checks their GPS location and health condition. An alarm is embedded and included in the app to warn self-isolating individuals when they leave their designated locations.
- Singapore's Government Technology Agency (GovTech) has released the TraceTogether app that utilizes Bluetooth signals to determine the proximity of a user with other nearby users and stores the information for 21 days. Once a user contracts the virus or becomes part of a "contact tracing investigation" the Ministry of Health is granted the right to identify the suspected case.
- The Alberta Health Services (AHS) in Canada has launched a contact tracing mobile app named ABTraceTogether that utilizes Bluetooth signals. When someone tests positive for the virus, AHS contact them to ask if they consent to grant the right of sharing their app's history.
- In Canada, a federal law for the private sector named Personal Information Protection and Electronic Documents Act (PIPEDA) has been legislated that considers the consent of users as a fundamental element in collecting, using, and disclosing individuals' information.
- To protect the privacy of users, a guidance document on meaningful consent has been released by the Privacy Commissioner of Canada that sets some guiding principles such as emphasizing and explaining certain key elements of the system and providing explanations in a user-friendly manner, giving a clear option to the users to say yes or no, and being accountable and able to demonstrate the organization's compliance with law.

- The Privacy Commissioner of Canada has identified certain “no-go zones” in a guidance document on inappropriate data practices that are considered offside of PIPEDA.
- Certain “no-go zones” are indicated as any unlawful collection, use, and disclosure of individuals’ personal information, unfair and unethical categorization of individuals that are against human rights laws, collecting, using, and disclosing individuals’ information that are utilized for purposes that are known and might cause harm to the users, screening employees by asking and using their social media accounts’ passwords, and using video and audio functionality of the users’ devices with the purpose of surveillance.

## CONSIDERATIONS

The main concern in using contact tracing apps emanates from privacy considerations of users. Despite the challenging situations that the public has to endure during a pandemic, such as COVID-19, protecting individual’s privacy remains still of paramount importance. Consequently, there should be guidelines that provide various stakeholders with right directions and recommendations during emergency situations such as pandemics, earthquakes, floods, and wars. The following is a list of the proposed guidelines.

1) Instructions on methods and certain information used in developing the system should be given and clearly explained to the users.
2) Service providers should ask and obtain consent of the users to collect, use, and disclose their information.
3) Collected data should not be stored in a central database unless under exceptional circumstances.
4) Collected data should be deleted after a certain period of time.
5) Tracking data, such as GPS location, must not be used.
6) Disclosed information by service providers should not be to the extent that leads to disclosure of individual’s identity.
7) Existence of security breaches in the app should be investigated and discovered.
8) In Canada, the AI-based systems should comply with PIPEDA. Moreover, the system should be developed following the guidance documents on obtaining meaningful consent and inappropriate data practices.

## NEXT STEPS

- The key factor in success of COVID-19 contact tracing apps is the number of their users. As the number of users increases, the more practical the contact tracing apps become. Hence, it is crucial to protect and ensure individual’s privacy so that more people are willing to use the contact tracing apps.
- If service providers do not consider privacy of users, people would not trust and will not use these apps that could result in a higher number of COVID-19 infections and longer duration of the pandemic. Moreover, to gain user’s trust companies should inform their users about the steps that they have taken and their measures in protecting users’ privacy. This is a key factor in the success of contact tracing apps ultimate goals and purposes to combat the COVID-19 pandemic.