Security-Policy
NET Nexus of Emerging Technologies

BRIEFING NOTES

# BN-28-COVID19-June2020

PRIVACY ISSUES IN AI-BASED COVID-19 CONTACT TRACING APPS AND DEVICES

Authors: Mehdi Taheri[1] and Kash Khorasani [2]

[1] Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

[2] Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

MINDS
MOBILISATION DES IDÉES NOUVELLES EN MATIÈRE DE DÉFENSE ET DE SÉCURITÉ

Security-Policy NET Nexus of Emerging Technologies

SUMMARY

- COVID-19 contact tracing apps have been developed and tested in several countries, such as South Korea and Singapore. The effectiveness of these apps in containing and monitoring the spread of COVID-19 has been proven in these countries.
- Contact tracing wearable devices that utilize Bluetooth signals to measure the proximity of individuals have also been introduced and developed for workplaces. Employees will be notified if their distance from one another becomes less than a standard amount or if they have close contact with a confirmed COVID-19 patient in their workplace.
- Since the above apps and devices measure the proximity of individuals and collect their personal information, concerns regarding violation of privacy have been raised. Hence, there is a need for having specific guidelines that can be utilized in developing contact tracing apps and devices.

CONTEXT

- The COVID-19 pandemic is a fact in our today's world that we should learn how to live with while trying our best to keep our society safe. Contact tracing apps and devices are among the most popular tools that have been developed to contain and track the spread of COVID-19 [1].
- The Smart Nation and Digital Government Office (SNDGO) of Singapore has introduced a digital contact tracing device for people who do not have access to smartphones and specifically, seniors who are not familiar with the digital world [2]. This device uses Bluetooth signals to communicate with nearby tracing devices and assigns a personalized QR code to each user [2].
- Moreover, keyrings and wristbands with unique user IDs that utilize Bluetooth signals to measure the proximity of workers in a workplace have been suggested for companies that are willing to remain operational during the COVID-19 pandemic [3]. As an advantage over smartphone contact tracing apps, these wearable devices can reduce employees' concerns regarding the violation of their privacy by their employers as they can leave the equipment at the workplace after finishing their shifts and working hours.
- Apple and Google have done the groundwork and developed an application programming interface (API) that can help contact tracing apps on iOS and Android to be able to exchange information with one another [4].
- In Canada, Public Health Ontario has progressed in its efforts towards developing a contact tracing app [5]. An app named COVID Alert has been developed by Ontario Digital Service [6]. This app does not use geolocational information of users and measures their proximity by utilizing Bluetooth signals. A user with prolonged close contact with a confirmed COVID-19 patient will be notified by the app, and they will be given proper public health advice [6]. One of the main objectives in developing this app is to contain the potential threat of the second wave of

infections. However, even before COVID Alert's launch, a ransomware masquerading this app was detected by ESET [7].

- Despite all advantages of COVID-19 contact tracing apps, they have raised concerns regarding the users' privacy. For instance, due to privacy concerns, the use of the Norwegian contact tracing app "Smittestopp" has been suspended, and users' information has been deleted after a reduction in infection rate [8]. This app was developed to save data on a central server and track users by utilizing their GPS data.
- A few US senators have expressed their concerns regarding the violation of privacy by using COVID-19 contact tracing apps by asking the US government that "[w]hat measures will the Administration put into place to ensure that the public health surveillance initiative protects against misuse of sensitive information?" [1].
- In response to this valid concern, an act named the COVID-19 Consumer Data Protection Act has been introduced in the US. According to this act, companies are required to be transparent on their collecting and processing users' information, and consent of individuals should be obtained in the first place. Moreover, service providers should "de-identify personally identifiable information" once the data is no longer needed and used. Furthermore, the act allows companies to use geolocation and personal information of users for proposes other than COVID-19 contact tracing [1].
- To address the COVID-19 contact tracing privacy concerns in Canada, privacy watchdogs have proposed joint guidelines that include measures to promote and urge transparency and accountability [9].
- Nine main principles have been considered in the guidelines, which include voluntarily use and obtaining the consent of users when the information is not needed it de-identification process should be started, individuals information cannot be used for purposes other than the intended public health issue and must not be accessible by other organizations, users should be informed about the information that will be collected from them, the usage of that information, the method of data storage and organizations who have access to it, the security of data and when it will be deleted, possible associated cyber risks.
- Moreover, an evaluation should be conducted by governments on the effectiveness of the app, and its results should be announced so that if the app is not useful, it should be decommissioned [9].

CONSIDERATIONS

The Office of the Privacy Commissioner of Canada has articulated its guidelines on "good privacy practices for developing mobile apps" [10]. Across Canada, except for Quebec, Alberta and British Columbia, service providers and developers are responsible for the collected personal information, its usage, and its disclosure according to the Personal Information Protection and Electronic Documents Act (PIPEDA). The following is a list of several key privacy considerations in developing mobile apps that are applicable to COVID-19 contact tracing apps.

- The developers are accountable for personal information that they collect, use, and disclose. In the planning stage, developers should inspect their practices by analyzing the process of data collection, data usage, and data flow to check for unauthorized access to data.
- In a clear and understandable way, users should be informed about privacy practices that have been carried out. Hence, entities are required to be transparent about their privacy practices so that users have a window into the data that has been collected, its usage, and its disclosure. Moreover, before updating an app, users should be notified about the changes that will happen in handling their personal information so that they can refuse the update. The mentioned actions that include before and after downloading an app lead to gaining the users' trust.
- Collecting personal information should be limited to the level that is needed for an app to carry out its intended task. There should be a justification for collecting and using personal information by an app. Also, apps should not collect any device-unique identifiers unless it is necessary in the function of apps. Moreover, both on the device and the backend servers, the collected information should be stored securely. Users should be able to deactivate and delete all the collected data from them.
- Meaningful consent should be obtained from users. The challenging step is to show users what will happen to their personal information without making them confused and exhausted. It can be achieved by showing only the most important details and providing links for the rest so that users' attention is drawn to the most critical information and "notice fatigue" is avoided. There also can be a user's privacy option in the setting so that users can adjust and tighten their settings. Moreover, graphic signs, different colors, and audible notifications can be utilized to draw the users' attention to specific privacy-related changes in apps.
- Timing for obtaining users' consent is essential. Users should be informed about an app's privacy policies, and the consent should be obtained when the app is downloaded. Hence, before deployment of an app or during its first use on the device, users will be informed about processes that will happen on their devices.

NEXT STEPS (If applicable)

- The importance and necessity of developing COVID-19 contact tracing apps and devices is evident as they can help us contain and monitor the second wave of infection in Canada while continuing with the reopening of workplaces and companies.
- Guidelines specifically designed to develop contact tracing apps and devices without violation of users' privacy are required. Hence, entities can build their products to comply with the law.
- Lessons can be learned from other countries with successful and failed contact tracing apps such as Singapore and Norway. For instance, the geolocation of users must not be utilized in the app, and information should not be stored in a central database.

- In addition to privacy, users' safety in cyberspace is of paramount importance and should be considered in the design step. Having a safe app that does not violate an individual's privacy helps to gain people's trust, which eventually leads to more usage of the app.

REFERENCES

[1] C. Shachar, "Protecting Privacy In Digital Contact Tracing For COVID-19: Avoiding A Regulatory Patchwork," 19 May 2020. [Online]. Available: https://www.healthaffairs.org/do/10.1377/hblog20200515.190582/full/. [Accessed July 2020].

[2] J. Guy, 29 June 2020. [Online]. Available: https://www.cnn.com/2020/06/29/asia/tracetogether-tokens-singapore-scli-intl/index.html. [Accessed July 2020].

[3] M. Hamblen, "COVID contact tracing for the workplace without smartphones, via LoRaWAN," 07 May 2020. [Online]. Available: https://www.fierceelectronics.com/electronics/covid-contact-tracing-for-workplace-without-smartphones-via-lorawan. [Accessed July 2020].

[4] D. Nield, "How Covid-19 Contact Tracing Works on Your Phone," 07 June 2020. [Online]. Available: https://www.wired.com/story/covid-19-contact-tracing-apple-google/. [Accessed July 2020].

[5] "COVID-19 Contact Tracing Initiative," 03 June 2020. [Online]. Available: https://www.publichealthontario.ca/en/diseases-and-conditions/infectious-diseases/respiratory-diseases/novel-coronavirus/contact-tracing-initiative. [Accessed July 2020].

[6] "New COVID-19 contact tracing app to be tested in Ontario starting in July," 18 June 2020. [Online]. Available: https://www.cbc.ca/news/canada/toronto/covid-19-coronavirus-ontario-june-18-contact-tracing-1.5617240. [Accessed July 2020].

[7] C. Osborne, "New ransomware masquerades as COVID-19 contact-tracing app on your Android device," 24 June 2020. [Online]. Available: https://www.zdnet.com/article/new-crycryptor-ransomware-masquerades-as-covid-19-contact-tracing-app-on-your-device/. [Accessed July 2020].

[8] "Norway ends virus tracing app, deletes data over privacy concerns," 15 June 2020. [Online]. Available: https://www.ctvnews.ca/world/norway-ends-virus-tracing-app-deletes-data-over-privacy-concerns-1.4984626. [Accessed July 2020].

[9] B.-J. MacKinnon, "Canada's privacy commissioners offer guidance on COVID-19 contact-tracing apps," 07 May 2020. [Online]. Available: https://www.cbc.ca/news/canada/new-brunswick/covid-19-contact-tracing-app-privacy-commissioners-new-brunswick-1.5557548. [Accessed July 2020].

[10] "Seizing opportunity: Good privacy practices for developing mobile apps," October 2012. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/mobile-apps/gd_app_201210/. [Accessed July 2020].