SciEn
Journal of Engineering Advancements Vol. 02(01) 2021, pp 35-40 https://doi.org/10.38032/jea.2021.01.005

Trust Concerns regarding Health-Related Smartphone Apps in collecting Personally Identifiable Information throughout COVID-19-like Zoonosis

Molla Rashied Hussein[1], Md. Ashikur Rahman[1], Md. Jahidul Hassan Mojumder[1], Shakib Ahmed[1], Ehsanul Hoque Apu[2]

[1]Department of Computer Science & Engineering (CSE), University of Asia Pacific (UAP), Dhaka, Bangladesh
[2]Department of Biomedical Engineering, Michigan State University, East Lansing, MI, USA

Received: November 19, 2020, Revised: February 10, 2021, Accepted: February 13, 2021, Available Online: February 22, 2021

ABSTRACT

Coronavirus disease 2019 or COVID-19 is a zoonosis, which means a disease that contaminates from the animals to the humans. Since it is very highly epizootic, it has forced the public health experts to implement smartphone-based applications to trace its swift transmission trajectory as well as the affected individuals. For this, the individuals' personally identifiable information is utilized. Nonetheless, these information may hamper privacy and cyber security, especially the trust concerns, if not handled properly. If the issues are not resolved at this very moment, the consequences will induce the mass level population to use the health-related applications in their smartphones inadequately. Therefore, a catastrophe will be imminent for another COVID-19-like zoonosis to come. So, to mitigate, an extensive study was required to address this severe issue, namely, trust concern. This paper has studied the needed by discussing the recently designed and developed health-related applications region by region across the world. Moreover, it has analyzed the benefits and drawbacks. The trust defiance is recognized and inspected from the perspective of an end-user. Some recommendations are advised in the later part of this paper to leverage and collaborate the awareness campaign between the Government, the App Developers and the common individuals.

Keywords: Trust, Smartphone Application, COVID-19, Personally Identifiable Information, Awareness, Privacy, Cyber Security, Recommendation.

1 Introduction

The zoonotic novel disease named coronavirus disease 2019 (COVID-19) has changed the course of the worldwide economy by putting constraints on individuals in daily commercial activities [1]. The highly contagious disease has potentially affected health facilities' capacity, even in first-world countries, where the healthcare systems are reliable with robustness [2]. To control and track the COVID-19 infection pattern, different administrations have utilized modern artificial intelligence (AI) based methods integrated with 5G technology as well as aerial drone machineries to track COVID-19 in real-time [3],[4]. As there is no definite medicine to prevent or cure the disease [5], the most effective way to avoid COVID-19 so far is not to get exposed [6]. Social distancing must be preserved between all, as recent studies [7] have shown that even an asymptomatic person may spread the disease inaudibly.

This social distancing induces the public health experts and professionals to collaborate with the technical researchers to deploy the health applications (apps) to monitor people digitally, as the manual process is quite tedious to execute. Instead of gathering the personally identifiable information (PII) of the affected individual along with contact information for the last couple of weeks through detailed interviews, the health-related apps in smartphones could be an effective substitute which have already been conceived, built, and even implemented in several countries [8].

Also, a majority of the people can use those apps using their smartphones not only in developed countries but also in the low- and middle-income countries (LMICs) [9]; proper app usability has to be guaranteed by comparing in terms of development as well as confidentiality along with popularity among the end-users, and last but not least, user-friendly interfaces.

However, as the PII is stored in those apps, potential exposure of the PII may violate the user's privacy. Moreover, the re-identification of a person could be executed by utilizing only a few demographic data of that PII. Therefore, an individual may become target for a potential cyber-attack or threat.

This paper enlightens the readers regarding the cyber security and privacy terminologies, reviews related apps through Google Play Stores, analyzes users' comments and views, suggests recommendations to mitigate trust concerns amongst the Governments, Developers and the End-Users. The studies in this paper will not only be beneficial for the authorities, but also for the mass population.

2 Definition of Terminologies

Before discussing the health-related apps and their features, fundamental trust issues concerning cyber security and privacy must be presented in short. The first one is the concept of the semi-honest model, the second one is the activity of a malicious actor, and the last one is the possibility of re-identification of a person to track and carry on cyber-attack or threat.

In a real world, when a user is using smartphone apps during any type of epidemic situation for public health activities, some PII is saved into the application storage. Those app data can indicate where the users are travelling or meeting with.

Now, after those epidemic situations go away, still the PII remains saved in that particular storage which is undesirable by the user. For this reason, the user may want the health app keeping the data for a specific timeframe, and removal of those data afterwards. Moreover, users may want a fully trustable

*Corresponding Author Email Address: mrh.cse@uap-bd.edu

model or a full honest model having no hackers or malicious actors to misuse the user data. However, it is quite impossible to create a full honest model because we cannot assume that all the actors in a security model behave in a completely honest manner [10].

But that necessarily does not imply that a vast number of malicious actors are always active to harm the unsuspecting users all the time. Because even though they may wish to harm or cheat, they in fact, act rather in a semi-honest way [10]. Therefore, we are proposing for a semi honest model to get rid of this problem of having trust.

In a malicious model, there is no an ideal stable condition. All participants are attacking each other and several kinds of malicious behaviors are present. It is quite hard to control and stop the malicious actors.

Moreover, there may be threat actors who want to create a security breach and hamper the safety of others, either intentionally or unintentionally. Those threat actors can be divided mainly in two types, malicious actors and nefarious actors. Malicious actors are the ones who try to hamper the system whenever they get the chance. Nefarious actors, on the other hand, are the ones who are always present online and try to break the systems. In real-life, nefarious actors present in a privacy model are quite rare. Some malicious actors can still be present in a privacy model. Some examples of threat actors in a privacy model are given below:

Cyber-terrorist: Threat actors who attack via technology in cyber-space are called cyber-terrorist. They may attack for political reason, creating public panic, spreading propaganda and so forth.

Cybercriminals: Cybercriminals are mainly profit-driven and represent a worldwide threat for a long time. The target of the Cybercriminals is to sell the sensitive data, such as PII, hold for ransom, and otherwise absorb for financial gain. Cybercriminals may work individually or in a group to achieve the target [11].

Now, a general misconception regarding tracking and tracing is eradicated as follows:

Tracking: The term indicates the way of travelling a path or location at the moment. Tracking gathers insights in real-time. A tracking app can detect an individual's exact location at any given moment by utilizing the geo-data through GPS coordinates or radio cell location. It can even build an extensive movement profile if it can track a person been where and when, in addition.

Tracing: On the other side of the coin, the term defines searching the path in reverse from its any given point to where it began. Tracing collects insights in retrospect. A tracing app can be employed to trace physical close contacts between individuals. Bluetooth technology makes digital devices communicating with one another over a minimal distance. It has the capability of measuring the distance between smartphones by sensing the strength of the radio signals, and therefore, sense the social encounters between individuals, also known as proximity tracing.

Finally, the demographic variables and the process of de-identification, and the data policies as well as laws are discussed as below:

Demographic variables: These are defined as the independent variables as these are immutable. Demographic variables could be either categorical, such as race, gender, psychiatric diagnosis, marital status, or continuous, such as age, income, years of education, family size and so forth [12].

De-identification:- It is the process of making datasets anonymized before being shared. It is a common practice in research and data sharing environments to preserve a person's privacy. However, from the numerous anonymous datasets, a person can be re-identified using a demographic variable, which create a big concern about the privacy and ethical use of those data. Recently the collection and subsequent sale of Facebook data to Cambridge Analytica has made an enormous trust issue.

Reporters have re-identified the political personnel in an anonymized web browsing history dataset, comprises three million German citizens, back in 2016. The incident revealed their medical information as well as their sexual preferences.

The Australian Department of Health publicly released de-identified medical records for 10% of the population exclusively for researchers few months ago, but those got re-identified one and half months later [13],[14]. Studies also had revealed that the de-identified hospital discharge data could be re-identified by utilizing the basic demographic attributes along with the year of birth, diagnostic codes, ethnicity and gender. Researchers also exclusively detect individuals in the anonymized subway data in Riga, bike sharing rides in London, taxi travelling patterns in New York City, and mobile phone as well as credit card datasets [13],[14].

To prevent such privacy hampering, the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) ensure that each individual in a dataset needs to be protected by being anonymous, as data protection laws around the world consider anonymous data as not PII.

3 Related Works

To secure their people from COVID-19, governments around the world have authorized the usage of a smartphone app designed and implemented by the local technical enterprises with/without the collaboration with the global tech giants. In this section, we will go by the regions, i.e., continents around the world.

The following Table 1 is going to summarize the merits and demerits of several health apps spread over the numerous countries under the regions/continents.

From Africa, the continent has seen its country Ghana implementing the GH COVID-19 Tracker [15] by crowd sourcing data. Crowd-sourced data collection is a sharing method of making a data-set with the support of a massive group of the crowd and using a more secured semi-honest model to improve Crowd-sourcing. Also, Nigeria and South Africa have developed their own apps [16],[17] with not enough documentation to be discussed.

Next from Asia, more specifically, South Asia, Bangladesh has built an app, namely, Corona Tracer BD [18], which has gathered mixed feelings from the end-users. The nicely constructed user interface has been appreciated, but the issue of heavy usage of Bluetooth along with redirection to web browser all the time have raised frown among the end-users.

On the other hand, India has developed an application named Aarogya Setu [19]. This application has got very good documentation [20]. Although there was no mention of disposal of data after the pandemic in the initial development, the updated privacy policy [21] states that all PII collected will be stored on the mobile device for one month from the date of the collection, and if it has not already been uploaded to the server, will be permanently deleted from the App. All PII uploaded to the server will be permanently deleted from the server after one and half

months being uploaded if not tested positive, two months in case of being positive and later tested negative for COVID-19.

Moreover, Aarogya Setu [19] app alerts the individuals while an infected person is nearby through Bluetooth as well as GPS. Several Data Mining techniques, namely, Classification, Association Rule Mining, and Clustering have been implemented to discover COVID-19 spreading patterns [20]. As PII of numerous users of the app is stored on one server, this design potentially allows the potential malicious actors to hack the PII of users.

Meanwhile, from Asia, more specifically from Southeast Asia, MySejahtera [22] in Malaysia needs to mention good documentation describing its data privacy. Another app from Malaysia, MyTrace [23] accepts a community-driven approach. The participating devices share the proximity information when the app can identify another device close by with the same app installed. As this app is based on the DP3T (Decentralized Privacy-Preserving Proximity Tracing) algorithm [24], it does not need any permission to access location.

From the Asia and the Pacific, Singapore has implemented TraceTogether app with an adequate privacy statement [25]. As the user given the required consent, the app shares Bluetooth signals with encryption and anonymity with devices close by having same app. The data regarding Bluetooth are automatically erased after 25 days to prevent hacking. Storing limited data, such as users' contact/mobile number, users' identification details, a random anonymized User ID, the app never shows those to the public. No GPS location is collected, nor any information regarding WiFi or mobile network. Data about devices near users do not reveal any personal identity, as whenever the users are close to another device with the same app installed, both devices utilize Bluetooth technology to share a momentary ID generated by encrypting the user ID with a private key maintained by the Ministry of Health (MOH), Singapore, which could be decrypted by the MOH only. The right to be forgotten as per GDPR is preserved. The Temporary ID inside the users' device being exchanged with other nearby devices are regularly refreshed to prevent tracking.

Next from Asia, particularly from the Middle-East area, Bahrain uses an application named BeAware [26]. This application needs to have good documentation mentioning the data privacy issue. Tetamman [27] in Saudi Arabia always uses GPS and Bluetooth to cause power leakage, i.e., battery drain. It takes much control over users' smartphones as well. In Israel, Hamagen (or "Protector" in Hebrew) [28] cross-validates the GPS chronology of the smartphones of the patients with a bona fide geographic data stored in the Ministry of Health (MOH).

Meanwhile, from Europe, Czech Republic is using an application named e-Rouška [29]. It has an adequate documentation [30] with videos which are self-explanatory. But, the medium of instruction is Czech language. Therefore, the linguistic barrier hampers the spreading of the vital information, which should rather be kept in an international language, namely, English. In Hungary, VírusRadar [31] is a mobile app which implemented for Apple iOS and also for Android. It provides the topmost security standards, total control over PII, and ensures privacy protection as well. It is generally using the Bluetooth Low Energy (BLE) protocol to detect faceless encrypted contacts [32] which are highly secured.

After that, from Northern Europe, in Iceland, the app called Rakning C-19 [33] gathers the GPS location of the individuals' smartphone and saves the PII locally inside the device. If an individual is diagnosed COVID-19 positive, then the Health Directorate asks to exchange the location data only for contact tracing and identifying the people need to be in quarantine. On the other hand, Smittestopp app [34] of Northern Europe, more specifically, from Denmark, always keeps GPS and Bluetooth turned on and empties the energy. The frequently asked questions (FAQ) section is quite useful, but it is not adequate in terms of proper documentation and the data usage policy. Linguistic barrier is a concern as well.

Meanwhile, from North America, USA has developed several apps for each state. Among those, DC CAN, COVID Alert NY and CA Notify are praiseworthy [35]-[37]. They lack efficient notification system or multi-app conjunction, but simple in design and break down data with high energy efficiency. On the other hand, Canada has built COVID Alert app [38] that preserves privacy by not tracking location via GPS. However, rapid drainage of battery makes it cumbersome to use.

Next, from South America, Brazil has made Coronavírus – SUS [39] and Colombia uses CoronApp [40]. The documentation of the CoronApp could be found in [41]. Nothing has been mentioned about data privacy and further disposal of data, so it needs to mention the data privacy of an individual. Also, both apps need to be built in English for documentation as well as tutorial videos to assist expatriates.

Finally, from Oceania, Australia is using an app, namely, COVIDsafe [42] with an excellent documentation [43]. New Zealand, on the other hand, employs NZ Covid Tracer App [44] to mitigate their pandemic situation. This is based on user interaction. Although it has a poor design, it empowers the users of not exchanging credentials and thus doing nothing. It has a better data privacy, but it is not that effective compared to other contact tracing apps.

Table 1 Trust in Health Apps: Merits and Demerits

Region	**App features by region, country and name**			
	Country Name	***App Name***	***Merits***	***Demerits***
Africa	Ghana	GH COVID-19 Tracker [15]	Crowd-sourcing	Security Model
	South Africa	COVID Alert South Africa [16]	No fake notification due to 6 digit pin	No explicit data policy, Tardy notification
	Nigeria	Rapid Trace [17]	Live COVID-19 News and Status Check	Not enough documentation
Asia	Bangladesh	Corona Tracer BD [18]	Nicely designed User Interface	Redirection to Web Browser
	India	Aarogya Setu [19]	Well documented privacy policy	Central server allows potential hacking of PII
	Malaysia	My-Sejahtera [22]	Not enough information	Data Policy

Region	App features by region, country and name			
	Country Name	***App Name***	***Merits***	***Demerits***
		MyTrace [23]	Community-driven approach, DP3T	State surveillance may go wrong
	Singapore	TraceTo-gether [25]	Secure Server	Users can delete the app anytime
	Bahrain	BeAware [26]	Not enough information	Not enough documentation
	Saudi Arabia	Tetamman [27]	Not enough information	Power leakage
	Israel	Hamagen [28]	Crosscheck GPS data with MOH data	Not enough documentation
Europe	Czech Republic	e-Rouŝka [29]	Self-explanatory	Linguistic barrier
	Hungary	VírusRadar [31]	High security	Not enough information
	Iceland	Rakning C-19 [33]	Supervised by Health Directorate	Not enough information
	Denmark	Smittestopp [34]	Helpful FAQ information	Battery drainage
North America	United States of America	DC CAN [35]	Energy efficient	App Location Service issues
		COVID Alert NY [36]	Breaks down data for the whole state as well as local county	Not usable in conjunction with other COVID-19 apps
		CA Notify [37]	Simple design	Notification issue
	Canada	COVID Alert [38]	Does not use GPS or track location	Fast drainage of batteries
South America	Brazil	Coronavírus – SUS [39]	Well documented terms and conditions	Language barrier
	Colombia	CoronApp [40]	Well documented	No English version
Oceania	Australia	COVIDsafe [42]	Well documented	Not enough information
	New Zealand	Covid Tracer [44]	Maximum security unless user misuse	User dependent action

4 Recommendations

The following recommendations have been made to assist the Governments, the App Developers and the End-Users.

For the Governments:

i. Linguistic barrier is a major concern in European and South American countries. Many foreign personals living in those countries may not speak or read the native language, so having app made in the native language causes inconvenience. This also applies for foreign volunteers working in developing countries.
ii. Aware mass level people regarding security model such that they know that not all actors are malicious and there are very few nefarious actors. Also, a pure honest model is not possible, so caveat emptor (Latin, meaning "let the buyer beware") is the best policy in a semi-honest model.
iii. Moreover, even though the re-identification is mathematically possible, proper data management can reduce the threat significantly. So, it is the duty of the Government to educate the population so that the panic reduces.

For the App Developers:

i. Applications which are being used in different countries are not creating documentations properly. If an application has proper documentation, then people will feel more comfortable to use that application because they already know how the application in exactly working.
ii. To increase the trust issues, the app developers should make a proper documentation and a self-explanatory video to let the people know about the working procedure of the application.
iii. Furthermore, as every contact tracing application is using a centralized database to store data, if the distributed ledger is used, it will be safer for the data stored. If done so, in case of malicious attacks, the actor will be able to retrieve maybe a part of the database rather than the whole database.
iv. Therefore, Blockchain technology can play a vital role in this regard. It ensures maximum security with a shared ledger system, which makes it the best match to address the issues raised by the centralized systems.

For the End-Users:

i. The end-users should learn regarding the cyber security and privacy terminologies explained by the Government and the App Developers.
ii. They should be aware of their rights, know the data usage policy, ask questions before being forced to use any app, read app documentations and demand if not provided. Overall, they need to be conscious, not gullible.
iii. Cooperate the Government to take decisions regarding apps by volunteering for the pre-release. Also, suggest the requirements to the App Developers, so that there is no gap between supply and demand.
iv. In Democracy, the people have the authority. Therefore, they should trust and get trust from the Government and the App Developers. There should be clarity in each step to enhance trust issues.

5 Conclusion

To conclude, the Governments need to educate their citizens regarding cyber security and privacy. Moreover, data policy should be explicit and available to all. The App Developers should work with the Government to publish the data usage policy and assure the End-Users. It is also highly essential to study an individual's trust issues using digital health monitoring technologies including health apps. If in the near future, the trust issues are not solved, it will cost more, as people will be reluctant to use health apps and make a pandemic to come a much worse one.

Further studies and implementations have to be carried out as per the suggestions presented in the recommendations section. Afterwards we can ensure a better strategy to prepare for a future zoonosis or such disease.

References

[1] Gvili, Y., 2020. Security analysis of the COVID-19 contact tracing specifications by Apple Inc. and Google Inc. *IACR Cryptol. ePrint Arch.*, *2020*, p.428.

[2] Pillai, S., Siddika, N., Apu, E.H. and Kabir, R., 2020. COVID-19: Situation of European countries so far. *Archives of medical research*, *51*(7), pp.723-725.

[3] Hussein, M.R., Apu, E.H., Shahabuddin, S., Shams, A.B. and Kabir, R., 2020. Overview of digital health surveillance system during COVID-19 pandemic: public health issues and misapprehensions. *arXiv preprint arXiv:2007.13633*.

[4] Hussein, M.R., Shams, A.B., Apu, E.H., Mamun, K.A.A. and Rahman, M.S., 2020. Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations. *arXiv preprint arXiv:2007.13182*.

[5] Lai, C.C., Shih, T.P., Ko, W.C., Tang, H.J. and Hsueh, P.R., 2020. Severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) and coronavirus disease-2019 (COVID-19): The epidemic and the challenges. *International journal of antimicrobial agents*, *55*(3), p.105924.

[6] Hussein, M.R., Shams, A.B., Rahman, A., Raihan, M.S., Mostari, S., Siddika, N., Kabir, R. and Apu, E.H., 2020. Real-time credible online health information inquiring: a novel search engine misinformation notifier extension (SEMiNExt) during COVID-19-like disease outbreak. DOI: 10.21203/rs.3.rs-60301/v2 *PPR: PPR257400*.

[7] Yu, X. and Yang, R., 2020. COVID-19 transmission through asymptomatic carriers is a challenge to containment. *Influenza and Other Respiratory Viruses*, 14(4), pp.474-475.

[8] Ahmed, N., Michelin, R.A., Xue, W., Ruj, S., Malaney, R., Kanhere, S.S., Seneviratne, A., Hu, W., Janicke, H. and Jha, S.K., 2020. A survey of covid-19 contact tracing apps. *IEEE Access*, 8, pp.134577-134601.

[9] Jalabneh, R., Zehra Syed, H., Pillai, S., Hoque Apu, E., Hussein, M.R., Kabir, R., Arafat, S.M. and Azim Majumder, M., 2020. Use of mobile phone apps for contact tracing to control the COVID-19 pandemic: A literature review. Doi.org/10.1016/j.arcmed.2020.05.015.

[10] Goldreich, O., 2009. Foundations of cryptography: volume 2, basic applications. *Cambridge University Press*.

[11] Ablon, L., 2018. Data thieves: The motivations of cyber threat actors and their use and monetization of stolen data. *RAND*.

[12] El Emam, K., Brown, A. and AbdelMalik, P., 2009. Evaluating predictors of geographic area population size cut-offs to manage re-identification risk. *Journal of the American Medical Informatics Association*, 16(2), pp.256-266. https://doi.org/10.1197/jamia.M2902

[13] Rocher, L., Hendrickx, J.M. and De Montjoye, Y.A., 2019. Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications*, 10(1), pp.1-9. https://doi.org/10.1038/s41467-019-10933-3

[14] Sweeney, L., 2000. Simple demographics often identify people uniquely. *Health (San Francisco)*, 671(2000), pp.1-34.

[15] GH COVID-19 Tracker, Available at: https://www.coronatracker.com/about, last accessed on: August 20, 2020.

[16] COVID Alert South Africa, *Department of Health – South Africa*, available at: https://play.google.com/store/apps/details?id=za.gov.health.covidconnect&hl=en_US&gl=US, last updated on: December 21, 2020 and last accessed on: January 26, 2021.

[17] Rapid Trace, *Cadnetwork Enterprise, Nigeria*, available at: https://www.rapidtrace.com.ng, last updated on: January 01, 2021 and last accessed on: January 21, 2021.

[18] Corona Tracer BD, *Mobile game & application project, ICT Division, Bangladesh*, available at: https://play.google.com/store/apps/details?id=com.shoho z.tracer&hl=en_US&gl=US, last updated on: July 21, 2020 and last accessed on: January 04, 2021.

[19] Aarogya Setu, NIC eGOV Mobile Apps. Available at: https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu&hl=en, last updated on: July 8, 2020 and last accessed on: August 23, 2020.

[20] Sharma, U., 2020. Understanding aarogya setu: navigating privacy during a pandemic proves to be tricky. *LSE Covid 19 Blog*.

[21] Aarogya Setu Privacy Policy, available at: https://web.swaraksha.gov.in/ncv19/privacy, last updated on: July 8, 2020 and last accessed on: August 28, 2020.

[22] MySejahtera, Government of Malaysia, available at: https://play.google.com/store/apps/details?id=my.gov.onegovappstore.mysejahtera&hl=en, last updated on: August 10, 2020 and last accessed on: August 29, 2020.

[23] MyTrace, Government of Malaysia, available at: https://play.google.com/store/apps/details?id=my.gov.onegovappstore.mytrace&hl=en, last updated on: April 26, 2020 and last accessed on: August 29, 2020.

[24] Nanni, M., Andrienko, G., Barabási, A.L., Boldrini, C., Bonchi, F., Cattuto, C., Chiaromonte, F., Comandé, G., Conti, M., Coté, M. and Dignum, F., 2021. Give more data, awareness and control to individual citizens, and they will help COVID-19 containment. *Ethics and Information Technology*, pp.1-6.

[25] TraceTogether Privacy Safeguards, A Singapore Government Agency Website, A collaboration between Ministry of Health, SG United and GovTech. available at: https://play.google.com/ store/apps/details?id=my.gov.onegovappstore.mytrace&hl=en, last updated on: July 20, 2020 and last accessed on: August 30, 2020.

[26] BeAware Bahrain, Information & eGovernment Authority, available at: https://play.google.com/store/apps/details?id=bh.bahrain.corona. tracker&hl=en, last updated on: August 17, 2020 and last accessed on: August 31, 2020.

[27] Tetamman, *Ministry of Health, Kingdom of Saudi Arabia*, available at: https://play.google.com/store/apps/details?id=com.tetamman.home&hl=en, last updated on: August 25, 2020 and last accessed on: September 15, 2020.

[28] Hamagen ("Shield" in Hebrew), The Health Ministry, Israel, available at: Ihttps://play.google.com/store/apps/details?id=com. hamagen&hl=en, last updated on: August 27, 2020 and last accessed on: September 12, 2020.

[29] eRouška - part of smart quarantine, *Ministry of Health of the Czech Republic*, available at: https://play.google.com/store/apps/details? id=cz.covid19cz.erouska&hl=en, last updated on: July 26, 2020 and last accessed on: September 9, 2020.

[30] eRouška, *Ministry of Health of the Czech Republic*, available at: https://erouska.cz/en, last accessed on: September 9, 2020.

[31] VírusRadar, *Government Informatics Development Agency*, Hungary, available at: https://play.google.com/store/apps/details ?id=hu.gov.virusradar&hl=en, last updated on: May 15, 2020 and last accessed on: September 6, 2020.

[32] Nextsense, "VirusRadar – a mobile app for Covid-19 contact tracing implemented in Hungary as a donation," available at: https://www.nextsense.com/ns-newsarticle-virusradar-a-mobile-contact-tracing-implemented.nspx, last updated on: May 14, 2020 and last accessed on: September 6, 2020.

[33] Rakning C-19, *The Office of the Medical Director of Health, Iceland*, available at: https://play.google.com/store/apps/details ?id=is.landlaeknir.rakning&hl=en, last updated on: July 19, 2020 and last accessed on: September 3, 2020.

[34] Smittestop ("Stop infection" in Danish), *Ministry of Health and the Elderly, Denmark*, available at: https://play.google.com/store/apps/ details?id=com.netcompany.smittestop_exposure_notification&hl=en, last updated on: August 14, 2020 and last accessed on: September 4, 2020.

[35] DC CAN, DC Exposure Notifications, *Washington DC, USA*, available at: https://play.google.com/store/apps/details?id=gov.dc.covid19.exposurenotifications, last updated on: January 13, 2021 and last accessed on: February 09, 2021.

[36] COVID Alert NY, *New York State Department of Health, New York, USA*, available at: https://play.google.com/store/apps/details?id=gov.ny.health.proximity, last updated on: November 30, 2020 and last accessed on: February 06, 2021.

[37] CA Notify, CA *Dept of Technology, California, USA*, available at: https://play.google.com/store/apps/details?id=gov.ca.covid19.exposurenotifications, last updated on: January 14, 2021 and last accessed on: January 31, 2021.

[38] COVID Alert - Let's protect each other, *Health Canada*, available at: https://play.google.com/store/apps/details?id=ca.gc.hcsc.canada.stopcovid&hl=en&gl=US, last updated on: January 20, 2021 and last accessed on: February 03, 2021.

[39] Coronavírus - SUS, *Governo do Brasil, Brazil*, available at: https://play.google.com/store/apps/details?id=br.gov.datasus.guardioes&hl=en&gl=US, last updated on: October 27, 2020 and last accessed on: February 07, 2021.

[40] CoronApp - *Colombia*, available at: https://play.google.com/store/ apps/details?id=co.gov.ins.guardianes&hl=en, last updated on: September 2, 2020 and last accessed on: September 7, 2020.

[41] A healthy isolation, Tips for being at home, *The Government of Colombia*, available at: https://coronaviruscolombia.gov.co/ Covid19/aislamiento-saludable/coronapp.html, last accessed on: September 12, 2020.

[42] COVIDSafe, *Australian Department of Health*, available at: https://play.google.com/store/apps/details?id=au.gov.health.covidsafe&hl=en, last updated on: August 14, 2020 and last accessed on: September 9, 2020.

[43] How COVIDSafe works, COVIDSafe app, *Australian Government: Department of Health*, available at: https://www.health.gov.au/resources/apps-and-tools/covidsafe-app#how-covidsafe-works, last updated on: August 24, 2020 and last accessed on: September 9, 2020.

[44] NZ COVID Tracer, *Ministry of Health NZ (New Zealand)*, available at: https://play.google.com/store/apps/details?id=nz.govt.health. covidtracer&hl=en, last updated on: September 7, 2020 and last accessed on: September 13, 2020.