An Infrastructure for Integrated Temperature Monitoring and Contact Tracing

J. Niehaus* and N. Caporusso*
* Department of Computer Science, Northern Kentucky University,
Louie B Nunn Dr, 41099 Highland Heights, United States
niehausj3@mymail.nku.edu, caporusson1@nku.edu

***Abstract* – The COVID-19 pandemic has urged national governments worldwide to recommend several health-safety measures, including social distancing, the use of face masks, and sanitization. In this paper, we focus on body temperature monitoring and contact tracing, and we introduce a novel infrastructure designed to provide National Healthcare Systems with a centralized repository for systematic data collection and analysis. To this end, our system enables aggregating body temperature monitoring and contact tracing information acquired from a distributed network of heterogeneous data collection nodes. By doing this, we aim at collecting more data using different types of existing measurement devices. Also, the information architecture of the proposed system supports analyzing data in a centralized fashion. In this regard, we highlight the components that render our approach more suitable than current solutions in supporting cohesive intervention protocols and we describe the advantages in terms of better response against the COVID-19 pandemic and other types of health-safety emergencies.**

Keywords – pandemics, big data, COVID-19, health-safety.

I. INTRODUCTION

The unanticipated outbreak of the Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2) has rapidly escalated into a global emergency that infected more than 100 million individuals and caused over 2 million deaths worldwide. Consequently, national governments have enacted drastic provisions such as shelter-in-place and lockdown orders, especially in the first phases of the Coronavirus disease 2019 (COVID-19) pandemic and in case of faster growth of the infection curve. Additionally, other types of preventive non-pharmaceutical practices, including social distancing and Personal Protection Equipment (PPE) requirements, have been implemented to ensure the safety of individuals while releasing restrictions. Recent research studies show a high acceptance and compliance rate, which contributed to render them more effective.

On the contrary, countermeasures such as temperature monitoring and contact tracing have been successful only in a few countries (e.g., China) due to several factors, including government adoption, user compliance, and availability of an information infrastructure. As the effectiveness of health-safety measures depends on their systemic deployment and use, contact tracing specifically requires the entirety of the population to use the system in order to capture potential situations of risk. Similarly, protocols for body temperature checking are less effective when they are not integrated with reactive measures that enable alerting individuals who are at risk because of their social interactions. Unfortunately, in addition to poor adoption from national governments and, consequently, limited individuals' adherence, the unprecedented nature of the COVID-19 emergency involved a lack of information infrastructures that support collecting, storing, analyzing, and using the aggregated data from temperature monitoring and contact tracing effectively. The most significant effort in this regard has been the partnership between Google and Apple, which resulted in a set of smartphone-based Application Programming Interfaces (API) that support detecting individuals' proximity using the Bluetooth protocol [1]. However, their infrastructure does not support data from other devices or information about other types of measurements, such as temperature monitoring or positivity tests. As a result, most countries utilized many different systems that did not exchange information with one another, which created additional data fragmentation. Moreover, the lack of systems for aggregating and exchanging information from different sources required human intervention and posed a significant burden on the National Healthcare Systems (NHS), which were already overwhelmed by the emergency.

In this paper, we introduce an infrastructure-based solution based on a centralized database and on a distributed network of acquisition nodes that leverages the combined use of body temperature monitoring and social tracking. By doing this, our system aims at offering a more comprehensive solution for filling the effectiveness gap (e.g., in the case of asymptomatic and presymptomatic individuals) as well as increasing the information available to limit potential virus transmission. We discuss the architecture of the system and its components, detail the advantages of its integration with the currently available infrastructures and systems, and address concerns related to users' privacy and data access.

II. RELATED WORK

In addition to the implementation of pharmaceutical and non-pharmaceutical health-safety measures, the COVID-19 pandemic has been tackled by several groups who have adopted different strategies in the design and development of solutions for collecting information useful to limiting the spread of the virus, preventing potential outbreaks, and minimizing the risk of infection and its

damage [2]. As a result, several types of systems have been introduced. Primarily, efforts have been spent in the direction of overcoming the initial lack of data about the spread of the pandemic, using systemic approaches based on centralized or distributed data collection. The former strategy has been utilized predominantly in governmental institutions, such as NHSs, for managing the progress of the pandemic. Simultaneously, other types of tools have leveraged personal technology, such as smartphones, wearable devices, and self-reporting websites, to collect data, inform individuals about their potential risk, and support tracing. For instance, the authors of [3] describe a mobile application that individuals could use to self-report symptoms that could be potentially associated with an ongoing infection. Also, different devices, including wearables, have been introduced to support remote monitoring of body temperature changes [4] [5]. As a result of the development and introduction of multiple systems collecting different data, using different protocols, and storing it in self-contained repositories, the availability of solutions has created the problem of fragmentation, which poses new challenges to the use of the data being collected as described in [6]. On the contrary, a more promising and successful avenue for tracing has been pursued by platforms that provide a more comprehensive approach to data collection and use.

Several studies have analyzed the effectiveness of centralized and distributed data collection infrastructures for fighting COVID-19 using proximity tracing [7]. In this regard, the most successful case was the partnership between Google and Apple, which has led to the development and deployment of a set of APIs that enable collecting information about individuals' proximity using the Bluetooth protocol [1]. Specifically, they use several components of the radiofrequency signal, such as strength and signal-to-noise ratio, to calculate and track social contact. Although some studies report an initial concern about privacy [8], further research has clarified the security of the application and its compliance with rules about the collection and use of individuals' personal information [9]. As a result, the APIs have been integrated into several mobile applications adopted by national governments worldwide. Furthermore, data from recent studies demonstrate that smartphone-based solutions for proximity tracing have been received positively by end-users when its adoption has been advertised effectively [10]. Particularly, data from the NHS show that this approach prevented 594000 infections in the United Kingdom alone [11] [12]. Moreover, data from Washington state demonstrated the effectiveness of contact tracing in the case of low adoption rates (e.g., 15% of the entire population) [13]. Although the APIs developed by Google and Apple offer a great platform for proximity tracing, there is still a lack of solutions that enable integrating and using data from multiple services, which would enable a more comprehensive view of the pandemic as well as more in-depth analyses about its evolution.

III. System Design

In a preliminary study, we analyzed individuals' adoption of health-safety measures with the objective of identifying strategies that were less effective in tackling the pandemic because of poor user adoption or adherence. To this end, we distributed a survey in which we asked to rank the most common health-safety practices based on their perceived effectiveness. Although the data collection is ongoing, we analyzed the results obtained from 514 individuals in one week during the progress second wave of the pandemic. Although participants showed overall compliance with most health-safety recommendations, their perceived effectiveness indicated a disparity between the countermeasures, as shown in Figure 1. Specifically, wearing face masks and Personal Protection Equipment (PPE), social distancing, and sanitization accounted for 25%, 24%, and 20% of the perceived health-safety, respectively. Conversely, other measures accounted for the remaining 31%. In particular, checking body temperature regularly, getting vaccinated, and adopting contact tracing measures, resulted in a lower perceived effectiveness, that is, 14%, 12%, and 4%, respectively. The results regarding vaccines could be explained by the fact that no vaccines were available when the survey was circulated. Conversely, participants' comments indicate a lower compliance with monitoring their body temperature and social interactions. Also, the perceived low effectiveness of body temperature checking could be motivated by the inefficacy of this type of measure against asymptomatic and presymptomatic individuals. Furthermore, individuals indicated the difference between measurement systems and the impossibility to retrieve a trace of their measurements as another source of distrust in this health-safety practice. Finally, as far as the perceived low effectiveness of contact tracing is concerned, respondents indicated a variety of possible motivations. Several people were not aware of social tracking measures or technology, others instead indicated that they considered this measure less effective due to a lack of universal adoption and the presence of false positives and true negatives, even if they installed mobile applications for contact tracing. Nevertheless, although our results indicate a low perceived effectiveness, respondents' comments and willingness to use monitoring and tracking technology are in line with findings in the literature, which indicate a high acceptance of app-based contact tracing [10] and, in general, of tracking technology [14]. Surprisingly, privacy concerns were mentioned in only a few instances, which may suggest that this would not be a major issue in the case this measure would be enforced as other health-safety practices, as realized in countries such as China and the United Kingdom.

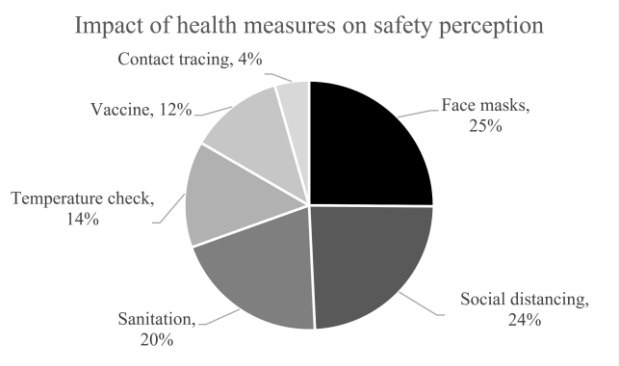

Figure 1. Users' perceived effectiveness of health-safety measures recommended against the spread of COVID-19.

As the goal of our work is to support fighting the pandemic by increasing the effectiveness of each health-safety measure, we focused on improving the less-performing ones. As a result, based on the analysis of the causes of non-compliance and on an evaluation of the limitations of current solutions, we designed a novel infrastructure for supporting body temperature monitoring and contact tracing. To this end, our approach was aimed at leveraging existing devices and systems already in use rather. Indeed, introducing new hardware or mobile applications with a one-size-fits-all strategy would not be effective due to the impossibility of adopting it universally, replacing current infrastructures, and adapting to specific use cases.

Our proposed solution is an information infrastructure that consists of a centralized data repository that enables many different stakeholders to collect, store, and access information related to body temperature monitoring and contact tracing. Particularly, the platform supports acquiring information about interactions between individuals, visits to private and public locations, and measurements of body temperature and other parameters. By aggregating information from multiple sources in a single database, we aim at solving the current data fragmentation and at offering a source of information for more accurate and comprehensive data analyses, which can be beneficial for fighting the COVID-19 pandemic as well as other health crises and emergencies. To this end, our infrastructure exposes a series of Application Programming Interfaces (API) served over HTTP that enable a variety of third-party stakeholders (TPS) to store their data in the centralized repository so they can contribute valuable information that can be accessed and analyzed for further use, as described in Figure 2. For instance, the data collected by the platform can be available to several the National Health Service and to other relevant organizations that are involved in individuals' health-safety. Specifically, as there are many different systems utilized for measuring individuals' body temperature and trace their social contacts, the APIs of our solution enable TPSs to share the data with our platform independently from the specific device being utilized for measuring individuals' body temperature or the contact tracing protocol, thanks to a data format specifically designed to render our infrastructure completely agnostic with respect to the data collection instrument and the specific type of information acquired from the user. For instance, as far as body temperature monitoring is concerned, the proposed platform supports receiving data from different types of thermometers (e.g., thermal scanners and kiosks), mobile applications for self-reporting, and even manual input. Similarly, in the case of contact tracing, the proposed platform supports data from social tracking software, infrastructure-based data collection, and paper-based forms. As long as TPSs adhere to a simple data protocol that enables capturing the information components relevant for our platform, they can use the proposed system. To this end, we designed a simple format and structure that is detailed in the API overview below. Consequently, the proposed infrastructure can leverage existing systems, software, acquisition devices, and tools as a distributed network of heterogeneous data collection nodes. In turn, by adhering to the API protocol, TPSs can benefit from an easy-to-integrate off-the-shelf data storage system.

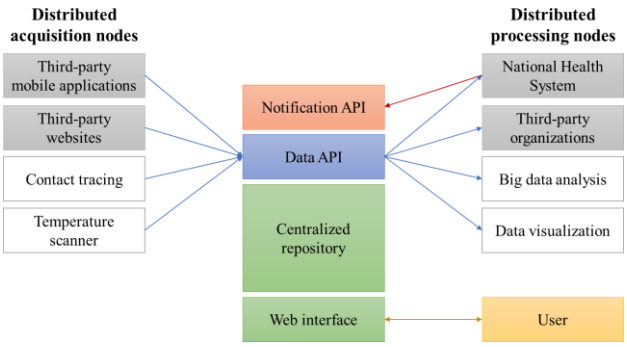

Figure 2. Overview of the platform structure, type of information exchanged via the Data and Notification APIs, and types of processing nodes.

A. *Main Entities*

The data repository of the proposed infrastructure consists of eight entities that represent the core information being collected and shared by the system. Additionally, the system includes other types of entities that are utilized for ensuring the operation of the platform. The main entities and their purpose are summarized in Figure 3, and they are as follows:

- User: this represents any single person who uses the platform directly (i.e., they created an account) or indirectly (i.e., because a TPSs stored data involving their contact information and, consequently, created a user entity). They are associated with an identifier that is globally unique. Also, their email and phone number are stored in the system. This has a three-fold purpose, that is, identification, contact in case of notifications and alerts, and two-factor authentication. As many social tracking systems collect contact information, they can be utilized in place of the numeric identifier or the token (as discussed below).
- Location: this represents a specific place, which can be a public venue or a private home. As in the case of users, they are associated with a globally unique identifier and with a flag that indicates whether the location is visible in the system or not. This enables users to prevent any of the stakeholders of the platform from accessing the information associated with their house. Additionally, public locations are identified by their GPS coordinates (i.e., latitude and longitude), name, and address. However, some of the values can be null, as shown in Figure 3. This is to include locations that are not associated with a specific latitude, longitude, or address. For instance, this is the case of flights, which can be identified by using their code as a name.
- Token: it is an alphanumeric string that identifies a user or location. Tokens can be utilized in place of the identifier for data collection and analysis purposes, and they enable abstracting from the numeric identifiers associated with users and locations. Also, tokens are generated with a new

request, and they expire as soon as they are consumed. Alternatively, an expiration date can be set to enable the acquisition of longitudinal data (e.g., the total duration of a visit to a location). Therefore, they can be utilized to render data collection completely anonymous, which, in turn, results in increased privacy for users.

- Measurement: it primarily refers to body temperature checks. Their value is stored together with information that enables identifying the user, the location, and the date and time in which the measurement was taken. However, either the user identifier or the location identifier can be null. Although this is counterintuitive, by doing this, the proposed infrastructure supports situations in which individuals' body temperature is checked, but it is not associated with their identity. For instance, this is the case of temperature scanners in high-traffic areas or other types of equipment that does not support identifying the person being monitored. Nevertheless, storing a body temperature measurement without the information about the person enables evaluating situations of risk and notify users who were in the location around the time in which the alert was generated. Conversely, the identifier of the place where the measurement was taken can be set to null in case a user wants to monitor their body temperature in their home or in a location that is not in the system. To this end, the proposed infrastructure supports data collection from self-monitoring applications while preserving users' privacy. In addition to the value, which can represent an individual's body temperature in case of this type of monitoring, the system collects the measurement type. This enables using the platform for different measurement purposes. For instance, in addition to body temperature, the proposed infrastructure can be utilized to aggregate information about diagnostic tests (e.g., PCR) as well as antibody tests (e.g., serological tests). In this case, the measurement type can represent the type of test, whereas the value can indicate the positivity of the subject. Consequently, the use of the proposed system can be extended to incorporate other relevant indicators that may help fight the spread of the pandemic or identify new outbreaks early.
- Visit: it represents a known location of an individual in a specific time window. In contrast to measurements, which are associated with body temperature checking or other parameter monitoring uses, visits are utilized for contact tracing purposes. Specifically, they enable tracking individuals' location over a timeline. This, in turn, combined with measurements, can be useful for identifying situations of potential risk involving a specific venue and alerting users in the case they have been in the same place in the same time window. In addition to the identifier of the location, the data repository enables storing the beginning and the end of the visit. However, either value can be null in the case the data acquisition node does not capture it, such as most venues in which the exit is not regulated.
- Interaction: this entity is utilized for contact tracing purposes and enables to explicitly indicate situations in which two or more individuals are in close proximity. The data repository stores information about the users (their identifier) and about the location, if this is available. Also, the platform supports specifying the date or the time frame of the interaction. By doing this, if an individual tests positive, all the people who have been in contact with them in a time compatible with the incubation and development of the virus will be able to receive a notification about their potential the risk of infection.
- Alert: this entity represents situations in which one individual is at risk, and they can be generated either by a data acquisition node in the case of a measurement value that is non-compliant with the standard, or by a data processing node that identifies a concern based on the analysis of the information in the repository. In the former case, the alert is immediate, whereas in the latter scenario the alert appears when it is found by the DPN. Alerts are stored in the entity sandbox and visible to the user they are associated with, based on the data access rules described below. However, stakeholders with higher permissions can process alerts and issue notifications to the user or to other stakeholders.
- Notification: this type of entity is utilized to inform a user that they may have been exposed to potential risk due to past interactions or visits that involved the co-presence of individuals who have been confirmed as being at risk. They differ from alerts in that their purpose is to notify one or more individuals that someone they have been in contact or shared a location with has tested positive or has been confirmed as a case. Notifications are issued by the NHS or by an authorized organization based on the information on the platform or other data. The notification type indicates the severity of the notification, whereas the message is utilized to detail the actions that they need to take next.

Figure 3, as well as the list above, presents the key attributes of the entities, details the relationships between the entities, and explains how they are exchanged between the stakeholders. The main advantage of this approach is the possibility of maintaining a low complexity of the data design so that TPSs can seamlessly integrate it in their system. Also, the minimal set of entities and attributes required to contribute to the data repository, renders it interoperable with a multitude of acquisition systems and with different types of relevant information, in addition to the measurements indicated here. Nevertheless, the data repository of our platform utilizes a document-oriented database management system, which supports a more flexible structure and enables including additional detail, if needed. For instance, the system can be utilized to store users' names. However, this information is not shared with other stakeholders, unless they already had access to it or

own the data based on the data access permissions, ownership, and history rules defined below.

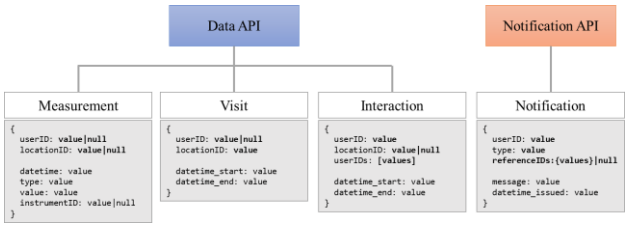

Figure 3. Key information acquired and shared by the Data API and by the Notification API

B. *Data Access Permissions, Ownership, and History*

Data APIs enable stakeholders registered with an API key to insert information measurements, visits, and interactions. To this end, there are two types of Data API permissions, that is, write-only (W) and read-write (RW), as described in Figure 4. Write-only permissions enable organizations to only insert data in the repository. This is the case of stakeholders contributing to the system with their data collection nodes. By doing so, they will be able to acquire information from their users and store it in the repository, but they will not be able to view or access data inserted by other entities. Therefore, the proposed platform provides a third-party entity having a W permission in the system with a sandbox that acts as a dedicated storage space in which the entity can insert and access its own data. However, write-only permission does not enable entities to access information outside their sandbox, that is, collected by other stakeholders. As a result, organizations will be able to use the data repository of the system to read and write information they collect and own without tampering with others' data. On the contrary, RW permissions enable authorized stakeholders to read the data acquired from other entities, in addition to writing information in their own sandboxes. This is the case of organizations affiliated with or authorized by NHSs. By doing this, they can access the data to realize analyses and research studies and share the results with other stakeholders by inserting them into the platform.

As far as data ownership is concerned, the permission structure enables stakeholders to own the information they contribute. Therefore, TPSs maintain ownership of the data they submit to the platform, and they can access it completely. Moreover, an organization that has RW permissions is not able to modify or delete the information stored outside their sandbox (i.e., in others' sandboxes) to guarantee the integrity of the data. Furthermore, TPSs with RW permissions are only able to view the information of the main entities detailed in Figure 3 unless the owner of the data gives explicit permission to get access to additional details. In addition to stakeholders, all the data involving a single user is shared with them, so they can review it and even flag it as private information. By doing so, their information regarding measurements, visits, or interactions will not be visible outside the sandbox of the stakeholder who contributed it unless the NHS service would issue a request related to a major health-safety emergency.

Finally, as TPSs with RW permissions can read others' data, access is tracked so that owners and users can view the log and be informed about how their information is utilized, in compliance with privacy regulations.

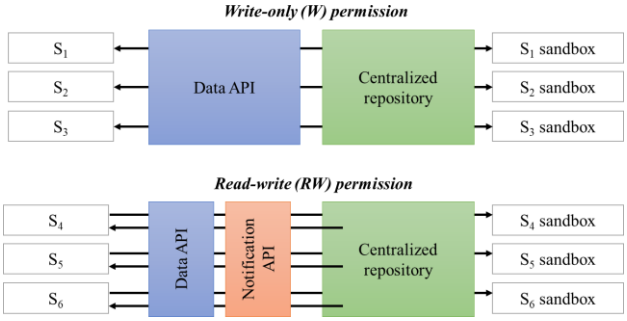

Figure 4. Permission structure of the platform.

C. *Data and Notification APIs*

The core APIs of our proposed infrastructure shown in Figure 3 are divided into two types of interfaces, one for data and one for notifications. The former set of interfaces is available to TPSs for storing the information they directly collect about one or more individuals or locations, including measurements that are non-compliant with the expected values. This enables TPSs to acquire data and raise alerts if needed. Conversely, notification APIs can be utilized by higher-level TPSs, such as NHSs or their affiliated and authorized organizations, to contact users in case they have been exposed to potential contagion, based on the analysis of the information from the sandboxes of one or more TPSs. In addition to separating their different purposes and the separate permission levels required for using them, the distinction between Data and Notification APIs marks the type of TPS that can access the latter type of interfaces. Additionally, each API has a different set of security measures that enable protecting the data as well as users' privacy, such as decoupling the user identifier and preventing potential attempts of sending unsolicited messages.

D. *Information Assurance*

The proposed infrastructure has the purpose of providing multiple TPSs with an easy-to-integrate system for aggregating information that can be useful for analyzing the evolution of the pandemic and tackling specific issues, such as the presence of an outbreak in a location, or for addressing broader challenges thanks to the combined availability of different types of data. To this end, the platform is designed to collect information from many different sources, such as users and TPSs. Both must register and create an account to be able to access the system. Specifically, TPSs are required to enter additional information when they request the use of APIs. Nevertheless, the information entered in the system may include untrusted sources or incorrect data. Furthermore, the decentralized nature of data collection processes based on self-reporting introduces several concerns regarding the authenticity of the data. Furthermore, as the system collects information from a variety of measurement devices and data acquisition systems, the different sensitivity of instruments (e.g., thermometers) and accuracy of measurement processes may affect the quality of the information stored in the data repository. However, this can

be addressed with a trust score system, so the data from each TPS can be ranked in terms of reliability.

IV. Conclusion

The pandemic scenario generated by the COVID-19 emergency has required the development and implementation of urgent strategies for limiting the risk of new outbreaks, flattening the contagion curve, and reducing the damage caused by the virus. To this end, in addition to health-safety measures, technology has been an important ally for deploying solutions that tackle the multifaceted aspects of the emergency, including body temperature monitoring, contact tracing, and early detection of symptoms. Thus, the data acquired by personal devices, scanners, kiosks, self-reporting forms, websites, and other systems may contain relevant information for identifying risk proactively or for addressing it reactively. In this paper we have proposed a centralized information infrastructure that enables aggregating the data collected by a multitude of heterogeneous acquisition nodes and using it for analyses that could help identify potential situations of risk or generate new and useful knowledge about fighting the pandemic.

The proposed information infrastructure has several differences with respect to other types of APIs such as the ones introduced by Google and Apple, which are specifically designed for supporting proximity tracking on mobile devices. Conversely, although our approach is less platform- and purpose-specific, it is more comprehensive as far as the supported devices and type of information that TPSs and individuals can share. Furthermore, the proposed system has several advantages compared to existing solutions. It can be utilized to collect real-time data as well as historical data. Consequently, TPSs can contribute the information they acquired during the early stages of the pandemic and share it with other stakeholders, such as research institutions, who can analyze the data and contribute to finding new evidence and generate knowledge about the pandemic and its countermeasures. Moreover, although the proposed infrastructure was specifically designed for fighting COVID-19, it can be suitable for managing other types of health crises or emergencies.

The specifications of the platform, its API documentation, and its implementation details are shared in a public repository that is available at the URL http://ush.to/uXXXuT. Currently, we are finalizing implementation details related to the compliance with healthcare regulations in terms of data collection and storage. Also, we are working with stakeholders to test different the platform in different scenarios and make the necessary changes. As a next step, we will integrate the system in some of the existing solutions and we will realize implementation and stress tests with selected TPSs that will enable us to evaluate the correctness of the design, the robustness of the system, and its performance. Subsequently, we will publish the system and make it available for integration and use to the public.

References

[1] Michael, K. and Abbas, R., 2020. Behind COVID-19 contact trace apps: the Google–Apple partnership. IEEE Consumer Electronics Magazine, 9(5), pp.71-76.

[2] Whitelaw, S., Mamas, M.A., Topol, E. and Van Spall, H.G., 2020. Applications of digital technology in COVID-19 pandemic planning and response. The Lancet Digital Health.

[3] Menni, C., Valdes, A.M., Freidin, M.B., Sudre, C.H., Nguyen, L.H., Drew, D.A., Ganesh, S., Varsavsky, T., Cardoso, M.J., Moustafa, J.S.E.S. and Visconti, A., 2020. Real-time tracking of self-reported symptoms to predict potential COVID-19. Nature medicine, 26(7), pp.1037-1040.

[4] Mondal, M.S., Roy, K. and Sarkar, S., 2020. Design and Development of Wearable Remote Temperature Monitoring Device for Smart Tracking of COVID-19 Fever. Available at SSRN 3735919.

[5] Yamanoor, N.S. and Yamanoor, S., 2020, September. Low-Cost Contact Thermometry for Screening and Monitoring During the COVID-19 Pandemic. In 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) (pp. 1-6). IEEE.

[6] Li, J. and Guo, X., 2020. Global deployment mappings and challenges of contact-tracing apps for COVID-19. Available at SSRN 3609516.

[7] Troncoso, C., Payer, M., Hubaux, J.P., Salathé, M., Larus, J., Bugnion, E., Lueks, W., Stadler, T., Pyrgelis, A., Antonioli, D. and Barman, L., 2020. DP-3T: Decentralized Privacy-Preserving Proximity Tracing. Retrieved September, 1, p.2020.

[8] Baumgärtner, L., Dmitrienko, A., Freisleben, B., Gruler, A., Höchst, J., Kühlberg, J., Mezini, M., Miettinen, M., Muhamedagic, A., Nguyen, T.D. and Penning, A., 2020. Mind the gap: Security & privacy risks of contact tracing apps. arXiv preprint arXiv:2006.05914.

[9] 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.

[10] Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, F., Nosenzo, D., Toussaert, S. and Abeler, J., 2020. Acceptability of app-based contact tracing for COVID-19: Cross-country survey study. JMIR mHealth and uHealth, 8(8), p.e19857.

[11] Kendall, M., Milsom, L., Abeler-Dörner, L., Wymant, C., Ferretti, L., Briers, M., Holmes, C., Bonsall, D., Abeler, J. and Fraser, C., 2020. Epidemiological changes on the Isle of Wight after the launch of the NHS Test and Trace programme: a preliminary analysis. The Lancet Digital Health, 2(12), pp.e658-e666.

[12] Chidambaram, S., Erridge, S., Kinross, J. and Purkayastha, S., 2020. Observational study of UK mobile health apps for COVID-19. The Lancet Digital Health, 2(8), pp.e388-e390.

[13] Abueg, M., Hinch, R., Wu, N., Liu, L., Probert, W.J., Wu, A., Eastham, P., Shafi, Y., Rosencrantz, M., Dikovsky, M. and Cheng, Z., 2020. Modeling the combined effect of digital exposure notification and non-pharmaceutical interventions on the COVID-19 epidemic in Washington state. medRxiv.

[14] Georgieva, I., Beaunoyer, E. and Guitton, M.J., 2021. Ensuring social acceptability of technological tracking in the COVID-19 context. Computers in Human Behavior, 116, p.106639.