Mobile apps for health surveillance: Balancing public health needs with the privacy of personal data

Journal of Infrastructure, Policy and Development 2024, 8(11), 5703.
https://doi.org/10.24294/jipd.v8i11.5703

Article

Mobile apps for health surveillance: Balancing public health needs with the privacy of personal data

Abba Amsami Elgujja[1,*], Augustine Arimoro[2], Fatimah Saad Alshahrani[1,3], Ahmad Salah Hersi[4,5], Aisha A. Elgujja[6], Salah Ezreqat[1]

[1] Infection Prevention and Control Department, King Saud University Medical City, Riyadh 11472, Saudi Arabia
[2] Law Department, University of Roehampton London, London SW15 5PJ, UK
[3] Division of Infectious Diseases, Department of Internal Medicine, College of Medicine, King Saud University, Riyadh 11451, Saudi Arabia
[4] College of Medicine, King Saud University, Riyadh 11472, Saudi Arabia
[5] King Saud University Medical City, Riyadh 11472, Saudi Arabia
[6] Eye Hospital, HMB, Maiduguri 600252, Nigeria
*** Corresponding author:** Abba Amsami Elgujja, abelgujja@ksu.edu.sa

CITATION

Elgujja AA, Arimoro A, Alshahrani FS, et al. (2024). Mobile apps for health surveillance: Balancing public health needs with the privacy of personal data. Journal of Infrastructure, Policy and Development. 8(11): 5703. https://doi.org/10.24294/jipd.v8i11.5703

ARTICLE INFO

Received: 7 April 2024
Accepted: 24 July 2024
Available online: 18 October 2024

Abstract: The privacy of personal information is aimed at protecting human rights both under the international human rights regime and the Saudi Arabian constitution and other statutes and regulations, subject only to some exceptions that include the protection of public health. The coronavirus disease 2019 (COVID-19) pandemic has brought about certain challenges that necessitate strategies to augment the conventional surveillance of infectious diseases, contact tracing, isolation, reporting and vaccination. Several governments institutions, and agencies presently adopt mobile applications for collecting, analyzing, managing, and sharing critical personal data of individuals infected with or exposed to COVID-19. While the benefits of sharing private information for achieving public health needs may not be disputed, the risk of breach of personal privacy is enormous. This had forced the national governments into a dilemma of either succumbing to public health needs, strictly respecting and protecting the privacy of individuals, or alternatively, balancing the two conflicting demands. There is a massive body of literature on the security and privacy of such mobile applications, but none has adequately explored and discussed public interest justifications under Saudi Arabian laws for alleged privacy breaches. We examined the health surveillance mobile app technologies currently in use in Saudi Arabia with the aim of determining the potential risks of data breaches under extant data protection laws. The paper recommends, among others, that any potential risk of breach to right to privacy of personal information under the law must be (justified by) the public health needs to protect society during the COVID-19 pandemic.

Keywords: Tawakkalna; Sehaty; Taba'ud; Tatamman; data protection; Anat; public health; COVID-19; covid apps; contact tracing

1. Introduction

Mobile apps for health surveillance have emerged as powerful tools in public health, offering real-time data collection and analysis capabilities. These apps can track disease outbreaks, monitor population health trends, and facilitate rapid response to health emergencies. However, their use raises important questions about the balance between public health benefits and individual privacy rights. As these apps collect sensitive personal health data, there are concerns about data security, consent, and potential misuse. Policymakers and health officials must navigate complex ethical and legal terrain to ensure that public health surveillance needs are met while also safeguarding personal privacy.

Conversely, it has already settled that the privacy and confidentiality of private information is a fundamental human right that is protected by international human rights law as well as the domestic law of Saudi Arabia. Privacy is essential for the protection of human autonomy and dignity, serving as the foundation upon which many other human rights are built (Zhang, 2021). Privacy protections guard individuals against wrongful government repression, especially that which is targeted against marginalized people (e.g., religious or ethnic minorities), against harms that stem from identity theft, fraud, extortion, and other criminal activities, and against the risk of reputational, economic, or social harms that might arise if personal practices or beliefs are made public (Boudreaux et al., 2020).

Ever since COVID-19 was first reported and later declared a pandemic, human life has changed in many respects, including conventional physical business transactions/interactions. The use of e-meeting technology became more prevalent to the extent that physical board meetings, classroom teaching, shopping, and family meetings, to mention but a few, are now done mainly online. Accordingly, around the peak of the pandemic, the hitherto existing infrastructure needed to mitigate and handle the pandemic could not adequately support the rapidly increasing number of confirmed cases of COVID-19 infection (Alharbi and Abdur Rahman, 2021). In light of this, evolving technologies for COVID-19 detection, monitoring, diagnosis, screening, surveillance, mapping, tracking, and creating awareness have become more prevalent (Mbunge et al., 2021).

Contact-tracing applications (apps) have emerged as reliable tools for public health communication and the promotion of public health (Duc Tran and Trung Nguyen, 2021). Hence, many countries have developed and deployed contact tracing technologies to curb the spread of the disease by locating and isolating people who have been in contact with coronavirus carriers (Toch and Ayalon, 2021). Contact tracing applications have flooded the marketplace, especially during the peak of the first wave when governments and authorities struggled to contain its spread domestically and internationally (Krehling and Essex, 2021). With the absence of a standardized approach used by authorities, policymakers, and developers, many of these apps were unique, and they varied by function and the underlying technology (Elkhodr et al., 2021). Some mobile apps are used for retrospective identification of people who had contact with persons who test positive for the COVID-19 virus and for prospective collection of pertinent information required for controlling the spread of the disease. The key challenge is how to maintain the confidentiality of the collected data (LI and Guo, 2020).

On the other hand, mobile apps are also used for mobilizing, registering, following up and maintaining a database of COVID-19 vaccinations. As traditional immunization cards or certificates are vulnerable to forgery, corruption, alterations, and difficulty read by non-health experts, they can easily become lost and are also susceptible to weather conditions such as rain. There is a need to develop secure COVID-19 electronic-based vaccination certificates or passports to counter the limitations of traditional vaccination cards. However, such technological interventions should be guided by ethical guidelines (Mbunge et al., 2021).

However, digital tools, though looking promising with great potential, were developed rather too quickly, resulting in the production of different apps with varying

levels of success. (Nasereddin et al., 2021) The swift development of half-finished contact tracing apps dented public trust and negatively impacted perceptions of app efficacy (Hogan et al., 2021). Moreover, the effectiveness of the apps depended highly on their level of acceptability and use by the general public; the broader the acceptance, the more effective the associated interventions were (Wirth et al., 2020). However, due to its associated privacy concerns, the apps were not well received by the users (Tahir et al., 2021). Furthermore, the perceived lack of trust in the government's intention seems to affect the people's acceptance of installing a contact tracing app on their phones, especially in countries where the use is not mandatory (Akinbi et al., 2021). Advances in modern information technology have created a potential risk to this right of confidentiality that the patient has always enjoyed, as protected by the laws (Elgujja, 2019, p. 379). The destruction of citizen privacy could also hinder public health by weakening trust and promoting dissent (Ada Lovelace Institute, 2020).

Although several studies have explored and discussed the privacy risks associated with mobile apps for COVID-19 surveillance, only a few, e.g., Househ et al. (2018), Seto et al. (2021b), have attempted to examine the balancing of public health needs and the protection of privacy, and only Sarabdeen (2021) has one with a particular focus on European, Canadian and Saudi Arabian data protection laws and regulations with a proposal of standards for acceptable use of health data for public health while ensuring acceptable protection of personal health data privacy. Building on those proposed standards, this paper explored the surveillance mobile app technologies in use in Saudi Arabia for their potential risks of data breaches under the prevailing data protection laws and regulations with a view to understanding if such breaches are obligated, allowed, or justified under the laws.

1) Aim of the study:

To optimize the utility of mobile apps for health surveillance by striking a balance between its benefits and the risk of confidentiality breach.

2) Statement of problem:

The widespread adoption of mobile health surveillance apps presents a critical challenge in balancing the urgent need for effective public health monitoring and disease control with the fundamental right to personal data privacy. As these apps collect sensitive health information and location data, they raise significant concerns about data security, user consent, and potential misuse. The key problem lies in developing a framework that allows for robust health surveillance to protect population health while simultaneously ensuring strong safeguards for individual privacy and preventing unauthorized access or exploitation of personal data.

3) Research questions:

This research question addresses the key aspects of your topic:

(1) It focuses on mobile apps specifically designed for health surveillance.
(2) It acknowledges the public health needs these apps aim to serve.
(3) It highlights the critical issue of personal data privacy.
(4) It implies the need to find a balance between these potentially competing interests.

This question could lead to an exploration of various subtopics, such as:

(1) Current mobile health surveillance technologies and their effectiveness.

(2) Legal and ethical frameworks surrounding health data collection.
(3) User perceptions and concerns regarding privacy in health apps.
(4) Policy recommendations for balancing public health and privacy concerns.

4) Methodology:

This is a review article that reviews the existing literature and legal tools to find answers to the research questions, and achieve the objective of the study. The review includes the follow:

(1) Utility and benefits of mobile apps in public health.
(2) Privacy concerns of contact tracing technologies.
(3) Geospatial technologies for contact tracing and impact on privacy.
(4) Centralized versus decentralized databases and impact on privacy.
(5) Tawakkalna: Saudi Arabian core contact tracing app.
(6) Balancing public health needs against privacy protection, and.
(7) Conclusions and recommendations for ensuring the protection of private data.

2. Contact tracing app uses and benefits in public health

Contact tracing mobile apps are used by public health authorities to augment traditional epidemiological interventions, such as by using technology-based data collection (e.g., automated signaling and record-keeping on mobile phone apps) (Boudreaux et al., 2020) to determine the chain of contacts of an infected person to identify them and get them to self-isolate or undergo institutional quarantine (Ross, 2021). Effective contact tracing allows public health authorities to break the chains of transmission and shift policy to case-based interventions such as selective individual quarantines rather than population-wide interventions such as social distancing (Kedron and Trgovac, 2021). Notwithstanding the possible breach of privacy, these apps prove to be beneficial in tracking and investigating infected persons and preventing further spread through unknown contact by actively warning healthy individuals and enabling the quarantining of positive individuals (Khan et al., 2021).

Apps are used to automate the traditional manual contact tracing (CT) process, which includes symptom tracking tools, dashboards, and analytical tools to support the comprehensive digital CT program (Nekvi and Haque, 2021). There is a large potential for future solutions supporting multiple uses by combining different technologies (e.g., Bluetooth and GPS) (Wirth et al., 2020). In a study to verify whether the use of WhatsApp facilitates communication, improves health information, perceptions of safety and security, and reduces emotional stress during the COVID-19 emergency, the satisfaction questionnaire showed good reliability and a high percentage of satisfaction of patients and their families with the adopted communication tool, reassurance, privacy protection and reduction of emotional stress (Nardo et al., 2021).

In the time of the COVID-19 epidemic, Italy was found unprepared to manage lockdown patients with chronic diseases due to the limited availability of resources necessary for running an integrated and efficient telemedicine, the heavy privacy regulations, and lack of clear guidelines, all hinder the implementation of effective telemedicine solutions for long-term patient management. The COVID-19 pandemic

seems to be a good opportunity to help promote better use and a larger integration of telemedicine services in the armamentarium of health care services. Telemedicine must no longer be considered an option or add-on to react to an emergency (Omboni, 2020).

The proliferation of electronic data within the modern health information infrastructure presents significant benefits for medical providers and patients, including enhanced patient autonomy, improved clinical treatment, advances in health research and public health surveillance, and modern security techniques (Hodge et al., 1999). These technologies use health data, symptom monitoring, mobility, location and proximity data for contact tracing, self-isolation, and quarantine compliance (Mbunge et al., 2021). Analysis has shown that the applications collected data related to demographics, contact identification, type of contact made with COVID-positive individuals, user symptoms, etc. (Tahir et al., 2021). Contact tracing is helpful during the pandemic (in rapid identification of cases and their contacts (Zhang et al., 2020). Apps are instrumental in mitigating the transmission of COVID-19, but there have been concerns among users about the data collected by these apps and their management (Zhang et al., 2020).

3. Privacy concerns of contact tracing technologies

Current developments in several countries show that conventional preventive measures can be augmented technologically by mobile apps, although privacy concerns are significant (Kaspar, 2020). These privacy concerns stemmed from the fact that to be efficient, mobile apps may need access to users' personal information (e.g., identity, location, system settings, voice and text), which raises concerns about potential wrongful data disclosure, misuse and social surveillance (Duc Tran and Trung Nguyen, 2021). The significant privacy concerns with using contact-tracing apps (Carlsson Hauff and Nilsson, 2021) may not be unconnected from the massive collection of private data and lax attitudes towards privacy protection during the pandemic. The apps collect personal data on a vast level, which could potentially result in a gross violation of user privacy (Tahir et al., 2021).

In general, the degree of these concerns and their effectiveness varied globally (Nasereddin et al., 2021) depending on the societal norms and values attached to privacy in each particular country (Seto et al., 2021a). However, during the COVID-19 crisis, governments had to make a fast and effective decision or choice to protect and promote public health. Unfortunately, such emergency decisions may potentially result in loosening regulations of digital private data privacy and regularizing the deployment of what would seem like social surveillance (Duc Tran and Trung Nguyen, 2021). There is also a potential risk of users' personal information and sensitive data being stolen should hackers that are within the vicinity of these devices (Zhang et al., 2020). Mobile apps are a target of malicious and phishing attacks with ransomware that can compromise patient records confidentiality and integrity. Therefore, privacy concerns are not insignificant (Khan et al., 2020). If not tested and validated rigorously, the room may be left for hacking devices and, once installed, such tracking software may be able to open the user's phone up to commands which may then permit the movement of data, 'including all passwords, contacts, reminders, text and voice

calls. In addition, the operator could turn on the phone's camera and microphone and use its GPS to track the target' (Van Zyl and Mclean, 2021, p. 516) Therefore, their use has become contentious because of the potential violation of ethical values such as security and privacy, among others (Mbunge et al., 2021).

A misuse of technologies could, if unchecked, lead to an erosion of privacy rights and hurt public trust in digital technologies (Kato, 2021). Opponents have argued that it is a viable means of targeted control in countries across the globe that creates significant ethical challenges for vulnerable communities (Van Zyl and Mclean, 2021). They further insisted that:

> "Reports from many countries that the government is requiring or asking people to install mobile phone apps that use location data for contact tracing. While some measures of surveillance are sophisticated and reliant on tech, others are about marking the bodies of COVID-19 patients with stamps. Routinely, privacy is being compromised and violated, and we are all frightened enough to let this happen" (Van Zyl and Mclean, 2021, p. 516).

Those in the race to adopt and embrace digital contact tracing—while a timely response to the pandemic—did not consider 'putting laws and policies in place to address the stigma surrounding the epidemic, and to protect the rights of those most marginalized, risks undermining the goal of epidemic control' (Chair, 2020).

The serious privacy concerns raised could have arisen with the several experiences we had with similar technologies in the past. Despite their privacy policies, many similar surveillance apps have been implicated in serious privacy breaches. For instance, a North Dakota app Care19 shared information, the unique advertising identifier used for targeted advertisements in other apps. Additionally, Google collected location data with its "privacy-preserving" contact-tracing application programming interface. Furthermore, Facebook performed similarly in the Cambridge Analytica scandal (Lo and Sim, 2021).

Mobile apps provide a convenient source of tracking and data collection to fight against the spread of COVID-19. However, their access to personally identifiable information can present challenges to ensuring that the right to privacy and civil liberties are protected (Sharma and Bashir, 2020). Therefore, this technology presents a trade-off between increased privacy measures and the effectiveness of the app. The right balance between privacy and effectiveness, while critical, is challenging because it is highly context-specific (Seto et al., 2021a). Often, users engage in health risk-privacy risk tradeoffs when evaluating and deciding to use the apps. This seems to support prior studies linking health risk and privacy risk perception with the adoption of healthcare technologies (Duc Tran and Trung Nguyen, 2021). This is further compounded by the realization that there is a perceived lack of clarity regarding related legal frameworks for dealing with new technologies used for managing private health information (Kaliyadan et al., 2020). Consequently, some researchers have raised concern that since the utility of these apps has not yet been proven, they should probably not be used as a preventive tool until the bioethics and legal issues related to their use are resolved (Cioffi et al., 2020).

Notwithstanding these concerns, such technology and devices are rapidly proliferating, prompting studies on their acceptability and ethical issues in their use (Abuhammad et al., 2020). As the security and privacy of people's health information

are not guaranteed (Mbunge et al., 2021). However, the degree of vulnerability to data breaches seems to depend on the type of tracking technology (WiFi versus Bluetooth) and, to a large extent, on the domicile of the database (centralized versus decentralized databases).

4. Geospatial technologies for contact tracing and impact on privacy

Today, large volumes of geospatial data are generated at high velocity from satellite sensors and unmanned aircraft systems, citizen sensors, geolocation-based data services, global navigation satellite systems, and so on (Tullis and Kar, 2020). Geographic information systems (GISs) have significant potential in planning to slow the spread, surveillance, contact tracing, and identify the trends and hotspots of breakdowns. Potentially, it could be used in future public health emergencies along with statistical and other socioeconomic modelling techniques (Ahasan et al., 2020).

Geospatial detection technologies use either geolocation-based, proximity-based or mixed approaches. In geolocation-based detection, the GPS feature of smartphones is used to trace users' geolocation to determine if two phones stay at the same location. However, in the proximity-based detection method, two smartphones exchange wireless message keys using Bluetooth technology whenever they come close enough (i.e., less than two meters) for a prolonged period. Hence, the users' geolocation is not collected. A mixed approach uses both the technology (GPS and Bluetooth). Another alternative is to supplement the proximity-based method with prior collection of users' area code and venue check-in capabilities, which, unlike GPS, does not collect users every movement but can still collect key location-related information (Kedron and Trgovac, 2021). Although geospatial data can be integrated and linked with contextual information to identify individuals' movements, steps taken to ensure privacy can complicate the multiuser development of high-quality geospatial workflows. In the era of big data and deep learning, GI scientists and associated institutions bear greater responsibility both for geospatial workflow quality and for location privacy (Tullis and Kar, 2020).

GPS technology could be used for crowd mapping to track infected persons by detecting other devices for a certain amount of time and a range of distances and anonymously notifying the devices of their affinity to the devices held by a reported infected person (Li and Guo, 2020). Bluetooth technology may improve tracing efficiency while alleviating privacy concerns by shifting data collection away from personal devices (Shelby et al., 2021).

The United States has the highest number of contact tracing apps, followed by Italy, where both Bluetooth and GPS technologies are used (Elkhodr et al., 2021). Similarly, geospatial technologies were successfully employed in Ghana (Sarfo and Karuppannan, 2020) and in several other countries to control the spread of COVID-19 (Tahir et al., 2021). Examples include Health Code (China), StayHomeSafe (Hong Kong), Stopp Corona (Austria), NHS CV19 (UK), Healthy Together (State of Utah, US) and Care19 (State of Dakota, US). Others are TraceTogether (Singapore), COVIDSafe (Australia), Hamagen (Israel), BlueZone (Vietnam) and Corona Data Donation (Germany) (Li and Guo, 2020). Additionally, the Norwegian, Singaporean,

Georgian, and New Zealand apps were among those that collected the most personal information from users, whereas some apps, such as the Swiss app and the Italian (Immuno) app, did not collect any user information (Elkhodr et al., 2021). Apple and Google partner on COVID-19 privacy-preserving contact tracing framework that is Bluetooth based, decentralised, free of GPS.

While GPS technology can track the movement of and map the location of infected persons more accurately, it is more intrusive and privacy breach prone. On the other hand, the Bluetooth tech does not take information on locations and movement but communicates with nearby devices and exchanges information about the holders of the devices. It would seem to be less prone to privacy breaches than GPS technology. This distinction is even more so when seen from the perspectives of whether the data collected are domiciled locally or centrally.

5. Centralized versus decentralized databases and impact on privacy

The installed mobile tracking applications use the mobile phone's GPS, cameras, Bluetooth, etc. to collect private data and either store them in users' smartphones (decentralized approach) and/or send it to and store them on a central server (centralized approach) controlled by government agencies and healthcare providers (Tahir et al., 2021). It is also possible to store exposure data either in an unidentifiable or anonymous form to maintain the confidentiality of users (Nekvi and Haque, 2021). Usually, government authorities use centralised data collection apps, while individuals control decentralised data on their devices, which largely reduces the risk of a privacy breach. Data from noninfected individuals' data are usually decentralised, while those of infected individuals are anonymized and kept in a secure centralized database (Li and Guo, 2020).

Generally, the decentralised framework with no GPS solution has the highest level of data protection in which no personal data of the healthy individual are collected. However, GPS tracking is needed to collect data and trace the population's movements geographically. In the decentralised framework, data are collected locally, and they cannot be driven into a centralised database for future analysis, i.e., less information for controlling self-quarantine and the movement of the disease among the population (Li and Guo, 2020). Decentralised tracing apps such as Austria's Stopp Corona are issuing a static unique digital ID to each user with rolling public and private keys (keeping the message encrypted and increasing the data protection standard).

However, decentralized storage does not necessarily eliminate the risk of a data breach. If the digital ID is unique and static, it runs the risk that certain digital IDs could be hacked and paired with a mobile device, thus compromising individual privacy (Li and Guo, 2020). Another drawback of decentralized tracing apps is where a malicious party running accounts on multiple phones can deduce the identity of a case by triangulating the notifications (Lo and Sim, 2021). Therefore, a rolling base digital ID to mitigate this vulnerability would be a better practice (Li and Guo, 2020).

The section also identified the risks of privacy breaches associated with the use of those applications to determine if such potential disclosures are actually protected by, pursuant to or justified under a law. Despite its benefits in suppressing the spread

of the virus, publicizing contact trace data raises concerns about individuals' privacy and thus the tug-of-war between one's privacy and public safety (Jung et al., 2020). With the foregoing in mind, the next section examines some of Saudi Arabia's mobile applications that are used to collect, manage and share private information for tracking movements of suspected confirmed cases of COVID-19.

6. Tawakkalna: Saudi Arabian core contact tracing app

Tawakkalna, developed by the Saudi Data and Artificial Intelligence Authority (SDAIA), is the key central data collection and sharing focal point that is used to support government efforts aimed at countering COVID-19 and to 'preserve the health and safety of citizens and residents on its soil from the risk of the spread of novel coronavirus' (Tawakkalna, 2021).

The central identifier that is used to link Tawakkalna to other related apps and databases is the civil registry number (Iqama and national ID numbers) that individuals use to register and provide their address using GPS. The app was used during the curfew period to map one's location, monitor one's movements, and determine violations of curfews, as well as provide the ability to notify the Ministry of Health in the event of a suspected case. Currently, it features COVID-19 vaccination appointments and records, national address updates, a health passport that shows the immunity status of the holder, and displays and keeps records of public violations and health conditions of the holder and his/her family members. Other features include an appointment for COVID-19 tests, displays of COVID results, and connections with the Taba'ud app, through Bluetooth, to alert users when they are around an infected, exposed or suspected person.

Tawakkalna also enables family heads to request providing care for their dependents who are under 15 years of age and gives access to online educational resources. Other relevant features include requesting for and providing gatherings, umrahs (lesser pilgrimage), and other public permits. It also enables QR and color codes that must be shown to security and receptionists of organizations and institutions upon entry. A user may be required to scan a QR to register at a gathering, public place or restaurant. Such information is collected in a central database and shared with relevant authorities such as the Ministry of Health for COVID-19 surveillance.

Tawakkalna is also linked to other related mobile apps such as Sehaty that, among other functions, gathers and shares with Tawakkalna COVID results, clinical information, vaccination appointments and status, among others. Other collateral apps linked to Tawakkalna include Absher (the Unified National Platform), Tatamanna, Sehaty (for booking clinic appointments, gathering clinical information, COVID-19 status, vaccination status, etc.), Taba'ud (through Bluetooth), alerts Tawakkalna users of the presence of a suspected or confirmed case of COVID-19 close to them so that they can take appropriate steps to protect themselves., Anat (identifies and prioritizes booking for licensed health care practitioners for COVID-19 vaccine), Etmarna (uses users' status to issue Umrah and visit permits to worshipers in the Holy Mosques in Makkah and Madinah), etc.

Tawakkalna is mandatory for every adult citizen or resident to install on his/her smartphone to enable them to move around and have access to health facilities,

shopping malls, and other public places. So, one has no right of consent, or of opting out. You do not have to supply your private information, but the apps gather your location and other private information and collates users' information from other sister apps that gather information about you. However, the app's privacy policy has made some promising commitments to protecting the privacy and confidentiality of collected private data.

- Tawakkalna privacy policy: (Tawakkalna-Privacy, 2021).

As alluded to above, the app has access to GPS location, Bluetooth, BLE, camera and can read external storage devices to upload PDF files. Therefore, the app gathers critical private information, maps users' location and monitors movements, and connects to other apps through Bluetooth to alert the user of his/her proximity to a suspected or confirmed COVID-19-positive person. Instructively, the app has made strong commitment to protect the privacy of personal data and to disclose only to those that are authorized by policy to receive such information for an approved purpose. The application's data protection policy is largely consistent with international standard practices. Some of its features include:

1) Data collection: it collects only specified information, such as personal information used for registration, location details, contact details and updates (including device language and system type used issue exit permits and notifications), other such information like requests for permits, answers to questionnaires, objections etc.
2) Restricted data disclosure for legitimate purposes: The app shares information with the Ministry of Health for facilitating the containment of COVID-19 transmission and to facilitate the access of citizens and residents (in the Kingdom of Saudi Arabia) to leave permits and to receive notifications sent by the application. Only authorized workers have access to the user's information for the purposes and uses determined by approved policies.
3) Data retention: All information entered by users is stored in a central server for 21 days only, after which the app undertakes to delete such information.
4) Users' responsibilities: The app implores users to protect their login details, not to share their private information and to secure their phone from unauthorized access.

These privacy policies are, by design/default, common for most data collecting apps, as most of them are built with a proactive commitment to privacy-preserving technological features (privacy by design) and only use strictly necessary data (privacy by default). However, no privacy-preserving system is perfect, and there is always the risk of (intended or unintended) disclosure of private information to third parties. (Alessandro and Effy, 2020) The question, therefore, is are such disclosures justified in public health interest under the laws?

7. Balancing public health needs against privacy protection

Electronic health information systems or surveillance apps have made not only human social interaction easier but also the way that individuals and healthcare professionals interact with each other within the purview of confidential professional relationships. However, advances in modern information technology have created a

potential risk to this right of confidentiality, which the patient has always enjoyed, protected by laws (Elgujja, 2019). Adherence to privacy is just not a norm but a legally binding obligation (Nekvi and Haque, 2021). Consequently, data privacy laws are becoming an increasingly important consideration in almost every jurisdiction around the world. These laws regulate how, when, where, and for what purpose any entity may collect, transfer, and process data about individuals (Seto et al., 2021a).

Protecting privacy has 3 interconnected impacts on the usability of the application: privacy of identifiable health information, reliability and quality of health data, and legal liability. It is argued that protecting health information privacy (by giving individuals control over health data without severely restricting warranted communal uses) directly improves the quality and reliability of health data (by encouraging individual uses of health services and communal uses of data), which diminishes tort-based liabilities (by reducing instances of medical malpractice or privacy invasions through improvements in the delivery of health care services resulting in part from better quality and reliability of clinical and research data) (Hodge et al., 1999).

While public health authorities can conduct manual contact tracing, many cannot identify and trace infected individuals at the scale or speed needed to respond to the COVID-19 pandemic. To improve and expand the reach and effectiveness of contact tracing, introducing digital contact tracing technologies has become imperative (Kedron and Trgovac, 2021). However, major concerns about its efficacy and privacy affect mass acceptance amongst a population (Akinbi et al., 2021). However, justification for privacy infringements of users may be permissible in the public interest if such apps can potentially help save lives and reduce enormous suffering associated with total population lockdown (Akinbi et al., 2021).

Digital health technologies can be highly effective and preserve privacy at the same time, but in the case of contact tracing and exposure notification apps, there is a trade-off between increased privacy measures and the effectiveness of the app (Seto et al., 2021a). This is because the delicate interplay between data protection on the one hand and the protection of public health on the other presents several challenges. During a crisis such as COVID-19, striking a balance between private rights to health data protection and public rights to data usage is critical (Sarabdeen, 2021) and therefore offers several opportunities and challenges (Househ et al., 2018).

Unfortunately, there is no clear guidance on how the user can strike the balance against competing these interests (Sarabdeen, 2021). Governments and users have been left without a standard metric to weigh these protocols and compare their assurances to know which are more private and secure (Krehling and Essex, 2021) and hot to strike a balance between one's privacy and the public benefits of data disclosure (Jung et al., 2020). Maintaining such a balance, especially between user privacy and societal benefit, is a huge challenge (Akinbi et al., 2021).

Data protection aspects are a critical factor for the adoption of any contact tracing apps, which must often be balanced against their functionalities to provide an optimal balance between privacy protection and pandemic control (Wirth et al., 2020). In times of crisis, some civil liberties may have to be suspended by governments, and "the sharing of sensitive data like one's health status and location can contribute to containing the spread of the virus" Digital contact tracing introduces different risks to

the recording of data as opposed to recording data on paper, for instance. When the technology is built at speed and rushed to market without the rigorous analysis and testing that may usually be afforded to software, there is a greater risk of vulnerabilities in the software. (Van Zyl and Mclean, 2021, p. 516)

However, the variety of digital CT solutions, especially CT apps, contain different levels of privacy threats and technical capabilities that are directly linked with effectiveness. Sometimes, the choice of a particular method of digital CT has an opposite effect to privacy and effectiveness, only to add uncertainty to decision making regarding digital CT (Nekvi and Haque, 2021). Despite the increase in the use of these applications, there is an ongoing research challenge concerning data protection, guaranteeing security, and the availability of CC applications (Alashhab et al., 2021).

Researchers have developed a variety of evaluation criteria for assessing compliance with public health requirements and privacy protection. For instance, a study used a total of 11 criteria but reported that the three most frequently adopted types of functions in the group reviewed were information about geographical coverage, contact alerting, and governmental responsibility. On the other hand, 12 criteria were defined to verify to what extent digital technologies comply with data privacy guidelines. The three most frequently met conditions were user consent, voluntary basis, and adoption of anonymization techniques. In balancing the efficiency versus privacy domains, it was found that the balance was best achieved by the COVID Safe app and worst by the Alipay Health Code app (Kolasa et al., 2021).

Evaluation of the apps' compliance with data privacy standards and their fulfilment of public health interests showed that apps with high levels of compliance with standards of data privacy tend to fulfil public health interests to a limited extent. Conversely, digital technologies with a lower level of data privacy protection allow for the collection of more data (Kolasa et al., 2021). It is our submission, therefore, that the focus should not be on 'if the whole essence of apps' efficiency can be balanced with its level of privacy protection, but on if any associated risk of a privacy breach can be justified by the need, under the particular situation, for achieving the protection and promotion of public health needs.

As part of its efforts to contain the coronavirus disease (COVID-19) pandemic, Saudi Arabia has launched a set of different applications and improved some existing applications to provide various health care services to its residents (Obaid, 2020). Saudi Arabia has protected personal data in addition to the limitation of such protection in the case of national and international crises (Sarabdeen, 2021). Saudi Arabian laws provide for the protection of privacy and confidentiality except as are necessary in the public interest to protect, among others, public health (Elgujja, 2020). Contemporary Muslim jurists have explained such exceptions based on various juristic rules. These include choosing the lesser evil or greater good is always the priority and the notion that the public interest overrides individual interest (Elgujja, 2020, pp. 12–13). In a fatwa (a religious ruling), for instance, the jurists affirmed that a breach of confidentiality may become justifiable if, the harm of maintaining confidentiality overrides its benefits by allowing the commission of lesser evil to avoid the greater one and for an overriding public interest, which favours enduring individual harm to prevent public harm or safeguard the public interest (Elgujja, 2020, pp. 12–13).

Such justification for the infringement of privacy rights is acceptable even under international human rights laws (IHRLs). Even in other climes, mandatory reporting of infectious diseases (MRID) is an essential practice to prevent disease even during nonpandemic periods for the protection of public health, conducting scientific research and planning health policy. In this context, the relevant information benefits public health, health systems and scientific work (Sert et al., 2021). However, such reporting should be conducted within ethical and legal boundaries with due regard to balancing potential benefits between all individuals, as well as between the individual and the rest of society. Disease notification systems that are not designed with a balancing and harm-reductionist approach may lead to stigmatization and discrimination (Sert et al., 2021).

There is no doubt that these apps possess many aims of protecting individual privacy. Nevertheless, by their very nature, they must reveal some otherwise protected personal information. Therefore, digital contact tracing has endemic privacy risks that cannot be removed by technological means alone and that may require legal solutions, among others (Hogan et al., 2021). Apart from the need for the laws to keep tabs on such challenges, there may also be the need for 'bringing about a fundamental shift in our thinking about privacy.' Additionally, individuals must be better educated on and be aware of the privacy risks of their communications in the digital spheres in terms of increased sensitivity to the privacy of others and, hence, more alert to the requirement to prevent privacy invasions (Elgujja, 2020, p. 198).

8. Saudi Arabian privacy laws and regulations

Saudi Arabia has no dedicated statutory law, particularly for data protection. There are, however, snippets of data protection provisions that can be found fragmented in different laws and regulations (Elgujja, 2020). Generally, it has been argued that laws are not able to keep a tab with the revolution going on in the information technology sector. Such an ensuing gap potentially gives way to unresolved gray areas. Additionally, the lack of clear regulations and legal frameworks for regulating health data security and consumer privacy were identified as the major challenges (Alanzi, 2021). Until recently, the increasingly new ways in which privacy and confidentiality rights are at risk of violation in a technological age had not been sufficiently integrated into most legal systems, thus necessitating the adoption of a contemporaneous approach (Elgujja, 2020).

In the next two sections, the paper examined the fragments of privacy protections that are embedded in some unrelated legislation and the efforts made to supplement the laws with regulations to adequately deal with the evolving new technologies.

8.1. Saudi Arabian statutory protection of privacy of confidential data

From the foregoing, it can be seen that the complexities of contact tracing mobile apps bear inherent privacy risks, and even the safest technologies do not eliminate such privacy risks. Hence, technological solutions can only go so far, resolving the impact of many of these attacks is thus a matter of policy and law. Currently, there are dedicated data regulations and snippets of laws on data protection in Saudi Arabia. Some privacy protection provisions can be found in unconnected laws that include the

Basic Law of Government (the Saudi Constitution), the Anti-cybercrime law, Telecommunication Law, the Law of Practicing Healthcare Professions, and the Mental Health Law, among several others. For instance, under the Basic Law, privacy is protected under Article 39, which provides the following:

> "Mass and publishing media and all means of expression shall use decent language and adhere to State laws and that whatever is injurious to the honour and rights of man, shall be prohibited."
>
> It also broadly provides, under Article 40, for privacy and confidentiality:
>
> "Correspondence by telegraph and mail, telephone conversations, and other means of communication shall be protected. They may not be seized, delayed, viewed, or listened to except in cases outlined in the Law."

This provision has encompassed both the positive and negative duties of protecting privacy and confidentiality. It undertakes to ensure the protection of confidential information and will not (or allow others to) breach this right except under certain circumstances as provided by laws. Although the Basic Law itself does not state what these exceptions are, other statutes have stated certain exceptions under which infringements of human rights may be justified.

> Accordingly, the Anti-Cybercrime Act provides the following:
>
> "Producing and distributing content that ridicules, mocks, provokes and disturbs public order, religious values and public morals through social media will be considered a cybercrime" (Barnes, 2018).

The Anti-Cyber Crime Law (BOE,2007), enacted by Royal Decree no. M/17, imposes heavy civil and criminal sanctions on the encroachment of personal data privacy, including the interception of data transmitted through an information network without legitimate authorization and the illegal access of bank data or computers to modify, delete, damage, or redistribute private data. Penalties upwards of SR 3,000,000- and four years' imprisonment may apply (see, e.g., Arts. 3–5).

Another similar law is the Saudi Telecom Act, 2001 (CSTC, 2001) which is intended to regulate the telecommunication industry with the goal, among others, of 'safeguard(ing) the public interest and the user interest as well as maintain the confidentiality and security of telecommunications information.' Article 3 prescribes sanctions for the breaches of privacy in the telecommunications sector. Consequently, it is a violation of the Act to engage in an interception or intentional disclosure (other than during duty) of any telephone call or data carried on the public telecommunications networks in violation of the provisions of Article 37 of the Telecommunications Act. A violation of its provisions may attract a fine of up to five million Saudi Riyals, and any party who is unsatisfied with the decision of the Commission may appeal to the Minister. An opportunity for a further appeal lies to the Board of Grievance.

Similarly, the Ministry of Health (2016) provides for a broad spectrum of rules on the duty of health care practitioners (HCPs). HCPs, among their many other duties, are obligated to maintain their patients' confidentiality in the following words:

> "A healthcare professional shall maintain the confidentiality of information obtained in the course of his practice and may not disclose it except (as provided by the law)" (See Article 21, (Ministry of Health. (2016)))
>
> Under Article 30, a violation of the Law constitutes a crime that attracts a fine of

not more than 20,000 Riyals. In addition, Article 31 of the Law provides for disciplinary liability for defaulting in any professional duty created under the law or for violating the relevant code of professional conduct or ethics. The disciplinary penalties may include a warning, a fine not exceeding 10,000 Riyals or revocation of the license for practice and a further ban from re-registration for two years from the date of revocation. Similarly, a breach of this duty confidentiality under the Mental Health Act could attract a penalty of imprisonment for a period not exceeding three months or a fine not exceeding fifty thousand riyals, or both, according to Article 25 (4) Mental Health Law.

8.2. Legal justifications for privacy breaches under the Saudi Laws

The state has undertaken to protect human rights according to Shari'ah (see Article 6 and shall look after public health under Article 31. (Ministry of Health. (2016)). Accordingly, it commits to protecting the privacy of individuals, the law, under Article 40, but subject to certain exceptions (under a law) that are necessary for the protection of public health and some other named public interests. Ordinarily, exceptions to a human right may only be considered justified if they meet the three conditions: they are under or according to a law, it is necessary for achieving a legitimate aim, and it is applied proportionately for achieving such a legitimate aim (Elgujja, 2020).

Hence, a violation of the protection of personal data or privacy may be excused under Saudi Arabian laws if the violation happens to be for the greater good (Sarabdeen, 2021). For instance, under Article 31 (a) (2) of the Law of Practicing Healthcare Professions, the duty of maintaining confidentiality is subject to certain exceptions that include reporting communicable or epidemic diseases. For example, a health emergency during the COVID-19 pandemic caused health authorities to widely collect, store, transmit, and use individuals' private data for research and public health purposes. Although such may impact the right to data privacy, it is a justifiable attempt to prevent the spread of infectious diseases and protection of public health provided that such limitation of data privacy is appropriately balanced. (Sarabdeen, 2021) Where the exceptions apply, the right of consent, opt-in/out would seem to be dispensed with.

Given that the Saudi Arabian legal protection of privacy is not encoded in dedicated statutory law for dealing with emerging intrusive apps, is there any hope? The next sections reviewed the novel interim regulation recently milled out for just this purpose.

8.3. Personal data protection under the National Data Governance Interim Regulations

Unfortunately, most of the laws prevailing at the onset of the COVID-19 pandemic were not robust enough to address the automatic tracing app context (Hogan et al., 2021), and under Saudi Arabia's legal protection of privacy and confidentiality of private information was not an exception. With the technological advancement and ease of access and sharing of data, personal data protection is becoming increasingly critical, which has instigated most countries around the world to release laws and

regulations for collecting, processing, and sharing personal data to protect individuals' right to privacy and to govern national data sovereignty. Pending the legislation of data protection, pursuant to its power under Council of Ministers resolution No. (292) of 27/04/1441H, authorizing it to develop regulations, standards, and controls related to data protection as the national regulator of data in the Kingdom, the National Data Management Office created the National Data Governance Interim Regulations (NDGIR).

The noble goals of the NDGIR include increasing the level of public scrutiny standards against the performance of public entities, enhancing transparency, and fostering integrity and removal of unnecessary secrecy on public entities activities. This requires data classification against defined levels of confidentiality to balance the benefits and risks associated with data sharing among entities in the public, private, or third sector. Data classification is a prerequisite for identifying and publishing open data, making publicly classified information available, and exchanging protected data that includes personal data.

Under the NDGIR, official data in developmental sectors are, by default, open and public unless otherwise warranted, and data from the security or political sector are considered top secret unless otherwise warranted. Data are classified, upon creation or receipt, based on the potential adverse impact as a result of unauthorized disclosure, subject to the nature and sensitivity of the data. Access to data is granted to the least number of persons who need to know, for a legitimate purpose and according to the access control for limited access necessary for achieving the legitimate purpose as stated under para 4.3, (SDAIA, 2020).

The private data of individuals could be classified as confidential, secret or top-secret depending on whether the disclosure could affect the data user's privacy right or affect the health or safety of other individuals. In the latter case, the information is considered top-secret (with high impact) if it could lead to the disclosure of identity or location of security personnel leading to massive loss of lives. If it causes significant harm that can impact the life of another individual (medium impact), it is considered secret, but if it causes minor harm with no risk to life (low impact), it is still considered confidential. See para. 4.4, (SDAIA, 2020).

However, if the disclosure of private data affects only the individual data subjects, the classification would depend on whether it would infringe on the data subject's privacy right or intellectual property right and if it also affects the national interest. If the data are for a VIP and the disclosure of private data could impact the national interest (high impact), it is top-secret, but if the VIP's data disclosure does not affect the national interest, it is still considered secret. However, for other individuals (low impact), the private date is considered confidential. However, any private data that bears no impact on the individuals, whether the data subject or other third parties, is classified as public data unless at a point in time, it is determined otherwise (SDAIA, 2020).

8.4. Personal Data Protection Interim Regulations (PDPIR)

- Scope

  The Personal Data Protection Interim Regulations (PDPIR) is a segment of the

NDGIR, and it applies to all entities in the Kingdom that process personal data in whole or part, as well as all entities outside the Kingdom that process personal data related to individuals residing in the Kingdom using any means, including online personal data processing. However, the PDPIR does not apply to mandatory data collection of personal data (usually without the consent of the data subject) that is collected by a government entity if it is required for, among other public interests, protecting public health or safety or protecting the vital interests of other individuals. We will come back to discuss this further, infra. It is noteworthy that although the PDPIR would not apply to personal data collected for mobile contact tracing, it would be sensible to conceptualize it and appreciate it if it could be borrowed as part of the solutions to any identified loopholes in the contact tracing processes.

- Data protection principles

The PDPIR incorporated all the classical data protection principles of accountability and transparency (approved clear and understandable policies and procedures), consent (data subject offers and informed permission), and data quality (maintenance of accuracy, completeness, and timeliness). Other principles include data collection and disclosure limitations, data access limitations and data security, and restrictions on use, purpose, and retention. The regulation also requires that the data control monitor the data collection and management process for compliance and address any privacy-related inquiries about complaints and disputes (SDAIA, 2020), at Para 5.2

- Data subject rights under the PDPIR

The PDPIR recognizes three main rights of data subjects under the regulation: the right to be informed of the legal basis and the purpose concerning the collection and processing of their personal information, the right to withdraw his consent – at any time – unless statutory or judicial requirements require otherwise and the right to access his data within the possession of the data controller, including access to, request to correct, complete or update personal data, and request to destroy unnecessary data, and obtain a copy of such data in a clear format.

- Data management under the PDPIR
    - Usage: Classified information shall be used as per the classification level usage requirements and should be used within specified locations whether physical (e.g., offices) or virtual (e.g., using cryptography or special applications).
    - Storage: Classified information, or a mobile device that processes, stores or communicates classified information shall not be left unattended or be protected while in storage either physically or electronically through National Cybersecurity Authority approved encryption mechanisms.
    - Data Sharing: Entities shall decide on the physical and digital means of data sharing that ensure security, minimization of risk and compliance with Data Sharing regulations, and on the delivery model for data sharing, whether entities will utilize existing sharing mediums, e.g., Government Service Bus, National Information Center Network, or Secured Government Network, or will set up a new direct connection through the wire, removable storage media, Wi-Fi, remote access / VPN, API, etc.
    - Retention: A schedule defining the retention period of all data shall be

maintained based on the applicable business, contractual, regulatory and legal requirements and reviewed periodically—not less than annually—or when there are changes in applicable requirements.

- Disposal: All data shall be securely disposed of—in conformance with applicable Data Disposal Regulations—according to the retention schedule only after approval from the relevant Business Data Executive.
- Archival: in secure storage locations in the format recommended by the relevant Business Data Executive. Backed up. With access control
- Declassification: Data must be declassified or downgraded when classification duration expires, or protection is no longer required at the original level.

The PDPIR seems to have incorporated most, if not all, of the standard personal data protection definitions, principles and data subject rights as contained in contemporary data protection laws globally. However, the PDPIR does not apply to data collection that the government embarks on to protect public health, which would presumably include contact tracing apps. Therefore, is there any consolation for individuals whose private data are collected and shared by government agencies? What controls exist to protect those data subjects from unjustified disclosure to, and potential misuse by third parties, including businesses e.g., hotels, airlines etc.

The massive data primarily collected for combating COVID-19 may potentially become available to the government for other purposes, e.g., for combating security risk, and to private businesses, e.g., airlines, tourism and hotels, for possible commercial purposes. It would be arguably within the law (it is legal) for the government to use the data collected for the COVID-19 pandemic for a secondary use int eh public interest, e.g., for security-related purpose. However, is there a control mechanism applied to prevent misuse of personal data so collected? NDMO has taken a significant big step in this direction by including another interim regulation, in addition to NDGIR, for regulating data sharing among all data controllers of personal data.

8.5. Data Sharing Interim Regulations

The Data Sharing Interim Regulations (DSIR) applies to all government data that are shared with other public entities, the private sector, or individuals – regardless of its source, form, or nature. Unfortunately, for our discussion, the DSIR does 'apply to sharing of private sector or individuals' data or data requests made by a governmental agency for security or judicial purpose' See Para 6.1 (SDAIA, 2020). It is noteworthy that the usual clumping of public health interests with other public interests like security is conspicuously missing here, and it is not clear if the generalization of 'individual's data' also includes data collected by the mobile contact tracing app. In other words, is the DSIR applicable to the sharing of private information shared on mobile apps or by any other apps for whatever reason?

The confusion is further compounded by the statement: "if the classification level is assigned as 'Confidential'… then the Business Data Steward must assess conformance to the Data Sharing principles" See Para 6.3.3.c (SDAIA, 2020). This is because a piece of private information under the custody of the government agency

may also be classified as 'confidential' if disclosure can negatively impact the life of the data subject or other individuals. This confusion can provide an opportunity to argue that the DSIR can be applied to protect the unjustified sharing of personal information.

Had the DSIR applied, it would have subjected such third-party disclosure to balancing of public benefit and risks of harm against national interests, organizations, individuals, or the environment. See para 6.2 (SDAIA, 2020). This could have precluded third-party businesses, e.g., airlines and hotels, from taking advantage of any collected information or private laboratories from selling their databases. This would have been in line with one of the general purposes for which the NDGIR's data classification was made, to wit, for 'balancing between the benefits and risks associated with data sharing among entities in the public, private, or third sector' See para 5, (SDAIA, 2020). Furthermore, if the DSIR applied, 'entities involved in Data Sharing must find the appropriate balance between the need to share data and protect data confidentiality against the potential risks to an individual or society' See para 6.6.11, (SDAIA, 2020).

As promising as the NDGIR has robust regulations on data collection, management, sharing, storage, and disposal, it is unclear if its data-sharing regulation is applied to data collected by mobile contact tracing apps in use in Saudi Arabia, although it is clear that the PDPIR does not apply thereto. If the DSIR applied, it would have put an appropriate check on potential unjustified sharing with third parties.

9. Conclusions and recommendations for ensuring the protection of private data

9.1. Conclusions

The COVID-19 pandemic has changed the whole world in many ways, including even how we interact with our families, at work, in shops, at recreational places, and in schools to mention but just a few. Investigating and managing outbreaks/epidemics of infectious diseases is not an exception.

Mobile apps for health surveillance represent a powerful tool in modern public health efforts, offering unprecedented capabilities for data collection, disease tracking, and rapid response to emerging health threats. However, their implementation requires careful consideration of the delicate balance between public health benefits and individual privacy rights.

Mobile contact tracing apps have come to stay similar to virtual meeting apps that have transformed how we conduct important meetings, studies, and even worshipping in some quarters. As much as they have tremendous potential to augment conventional contact tracing methodologies, they are also infested with high risks to privacy and confidentiality of private data.

Privacy of private data is a fundamental right that is fully recognized and protected both by national and international human rights laws, and the Saudi jurisdiction is not an exception. However, privacy rights worldwide are not unfettered. The right to privacy may be justifiably infringed on for the purpose of achieving public interests, provided that it is under law, done for the purpose of achieving a legitimate

aim, and is proportionate to achieving that aim.

But privacy risk is inherent in all such apps. The more intrusive the app is into an individual's privacy, the more that public health can benefit from the data. Moreover, it seems that a high level of privacy protection corresponds to an obstacle in terms of the use of data for public health (Kolasa et al., 2021). Thus, there is a trade-off between its benefits and its risks.

The fragments of legal provisions and the recently created data protection interim regulation have collectively made enormous attempts to ensure that private data are fully protected subject to public health needs.

Under certain circumstances, some rights of the data subjects, e.g., the right to consent and to opt-out, are dispensed with in the public interest. This may be justified in the public interest because for the apps to be fully efficient, there has to be high uptake and downloads by the majority of the population so that the maximum benefit of protecting public health may be fully achieved.

The paper submits that technology alone cannot completely eliminate the risks of privacy breaches. The legal framework should be updated to ensure that it fully protects the privacy of personal data and to provide stringent conditions for their justifiable infringement, as needed for public health purposes, among others.

As we move forward, it is crucial that policymakers, health organizations, and technology developers work together to create frameworks that maximize the public health benefits of mobile surveillance apps while rigorously protecting individual privacy. This may involve developing privacy-preserving technologies, establishing clear legal guidelines for data use, and fostering open dialogue with the public about the risks and benefits of health surveillance.

Ultimately, the success of mobile apps in health surveillance will depend on striking the right balance—one that harnesses the power of technology to protect public health while respecting the fundamental right to privacy. As these technologies continue to evolve, ongoing evaluation and adjustment of our approaches will be necessary to maintain this delicate equilibrium.

9.2. Specific recommendations

The NDGIR should be updated and upgraded to a full-fletched dedicated data protection law, as is found in most other jurisdictions.

The applicability of the DSIR to data from mobile contact tracing apps should be clarified. We suggest that the DSIR should be made applicable to sharing of data obtained from mobile contact tracing apps to become fully protected by the regulation.

The role of private sector data controllers should be reviewed, and any chances of data misuse should be plugged to prevent them from potentially using the data for business purposes or to stigmatize previous COVID-19 infected persons.

There is a need to create awareness among Saudi citizens, residents and visitors of the importance of ensuring the security and safety of their devices.

9.3. General recommendations

Augmentations to existing legal frameworks may help to protect user privacy against legitimate central authorities, such as public health agencies, and deter private

sector organizations, such as hotels, that might be tempted to leverage such privilege (Hogan et al., 2021).

Encouraging collaboration between different stakeholders, such as developers, health ministries, data protection authorities, experts, and the involvement of the lay public, is a key element for an efficient adaptive governance approach.

- Technical:

Assess app penetrance, accuracy, and effectiveness in reducing the health and social burden of the infection (Alessandro and Effy, 2020).

Regular monitoring of technical parameters about the use and reliability of such apps would inform specific strategies to be adopted to increase the rate of downloads and actual use of the apps and to improve their functioning.

- Ethical:

Advocate for people who are missed out of the technological arena, either because they do not have a smartphone, have contracts for limited data use, or are not proficient users, e.g., the elderly, the poor etc. (Alessandro and Effy, 2020).

Author contributions: Conceptualization, AAE (Abba Amsami Elgujja) and AA; methodology, AAE (Abba Amsami Elgujja); validation, FSA, ASH and AAE (Abba Amsami Elgujja); formal analysis, SE; investigation, AAE (Aisha A. Elgujja); resources, FSA; data curation, SE; writing—original draft preparation, AAE; writing—review and editing, AA and ASH; visualization, AAE (Aisha A. Elgujja) and SE; supervision, FSA; project administration, ASH. All authors have read and agreed to the published version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

References

Abuhammad, S., Khabour, O. F., & Alzoubi, K. H. (2020). Covid-19 contact-tracing technology: Acceptability and ethical issues of use. Patient Preference and Adherence, 14, 1639–1647. https://doi.org/10.2147/PPA.S276183

Ada Lovelace Institute. (2020). Exit through the App Store? Rapid evidence review. Available online: https://www.adalovelaceinstitute.org/case-study/exit-through-the-app-store/ (accessed on 2 June 2023).

Ahasan, R., Alam, Md. S., Chakraborty, T., et al. (2020). Applications of GIS and geospatial analyses in COVID-19 research: A systematic review. F1000Research, 9, 1379. https://doi.org/10.12688/f1000research.27544.1

Akinbi, A., Forshaw, M., & Blinkhorn, V. (2021). Contact tracing apps for the COVID-19 pandemic: a systematic literature review of challenges and future directions for neo-liberal societies. Health Information Science and Systems, 9(1), 18. https://doi.org/10.1007/s13755-021-00147-7

Alanzi, T. M. (2021). Gig Health vs eHealth: Future Prospects in Saudi Arabian Health-Care System. Journal of Multidisciplinary Healthcare, 14, 1945–1953. https://doi.org/10.2147/JMDH.S304690

Alashhab, Z. R., Anbar, M., Singh, M. M., et al. (2021). Impact of Coronavirus Pandemic Crisis on Technologies and Cloud Computing Applications. Journal of Electronic Science and Technology, 19(1), 25–40. https://doi.org/10.1016/j.jnlest.2020.100059

Alessandro, B., & Effy, V. (2020). What's next for COVID-19 apps? Governance and oversight. Science, 370(6518), 760–762. https://doi.org/10.1126/SCIENCE.ABD9006

Alharbi, A., & Abdur Rahman, M. (2021). Review of Recent Technologies for Tackling COVID-19. SN Computer Science, 2(6). https://doi.org/10.1007/s42979-021-00841-z

Barnes, T. (2018). Saudi Arabia prosecutor says people who post satire on social media can be jailed. Available online: https://www.independent.co.uk/news/world/middle-east/saudia-arabia-social-media-satire-jail-sentences-twitter-facebook-censorship-a8523781.html (accessed on 2 June 2023).

BOE. (2007). Available online: https://www.wipo.int/wipolex/en/legislation/details/14570 (accessed on 12 September 2024).

Boudreaux, B., DeNardo, M., Denton, S., et al. (2020). Strengthening Privacy Protections in COVID-19 Mobile Phone-Enhanced Surveillance Programs. Available online: https://www.rand.org/pubs/research_briefs/RBA365-1.html (accessed on 2 June 2023).

Communications, Space and Technology Commission (2001) Available online: https://www.cst.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA%20_001_E_%20Telecom%20Act%20English.pdf (accessed on 2 June 2023).

Carlsson Hauff, J., & Nilsson, J. (2021). Individual costs and societal benefits: the privacy calculus of contact-tracing apps. Journal of Consumer Marketing, 40(2), 171–180. https://doi.org/10.1108/jcm-03-2021-4559

Cioffi, A., Lugi, C., & Cecannecchia, C. (2020). Apps for COVID-19 contact tracing: Too many questions and few answers. Ethics, Medicine and Public Health, 15, 100575. https://doi.org/10.1016/J.JEMEP.2020.100575

CSTC, Saudi Telecom Act. (2001). Available online: http://www.citc.gov.sa/English/RulesandSystems/CITCSyste/Documents/LA _001_E_ Telecom Act English.pdf (accessed on 2 June 2023).

Duc Tran, C., & Trung Nguyen, T. (2021). Health vs. privacy? The risk-risk tradeoff in using COVID-19 contact-tracing apps. Technology in Society, 67, 101755. https://doi.org/10.1016/j.techsoc.2021.101755

Elgujja, A. (2020). Adequacy of the legal safeguards of the patients' confidentiality right under the Saudi Arabian laws. Available online: http://usir.salford.ac.uk/id/eprint/60188/1/Thesis %4000343621.pdf (accessed on 2 June 2023).

Elgujja, A. A. (2019). Impact of Information Technology on Patient Confidentiality Rights. In: Impacts of Information Technology on Patient Care and Empowerment. IGI Global. pp. 365–387. https://doi.org/10.4018/978-1-7998-0047-7.ch018

Elkhodr, M., Mubin, O., Iftikhar, Z., et al. (2021). Technology, Privacy, and User Opinions of COVID-19 Mobile Apps for Contact Tracing: Systematic Search and Content Analysis. Journal of Medical Internet Research, 23(2), e23467. https://doi.org/10.2196/23467

Hodge, J. G., Gostin, L. O., & Jacobson, P. D. (1999). Legal Issues Concerning Electronic Health Information. JAMA, 282(15), 1466. https://doi.org/10.1001/jama.282.15.1466

Hogan, K., Macedo, B., Macha, V., et al. (2021). Contact Tracing Apps: Lessons Learned on Privacy, Autonomy, and the Need for Detailed and Thoughtful Implementation. JMIR Medical Informatics, 9(7), e27449. https://doi.org/10.2196/27449

Househ, M., Grainger, R., Petersen, C., et al. (2018). Balancing Between Privacy and Patient Needs for Health Information in the Age of Participatory Health and Social Media: A Scoping Review. Yearbook of Medical Informatics, 27(01), 029–036. https://doi.org/10.1055/S-0038-1641197

Jung, G., Lee, H., Kim, A., et al. (2020). Too Much Information: Assessing Privacy Risks of Contact Trace Data Disclosure on People With COVID-19 in South Korea. Frontiers in Public Health, 8. https://doi.org/10.3389/fpubh.2020.00305

Kaliyadan, F., A. Al Ameer, M., Al Ameer, A., et al. (2020). Telemedicine Practice in Saudi Arabia During the COVID-19 Pandemic. Cureus, 12(12). https://doi.org/10.7759/CUREUS.12004

Kaspar, K. (2020). Motivations for Social Distancing and App Use as Complementary Measures to Combat the COVID-19 Pandemic: Quantitative Survey Study. Journal of Medical Internet Research, 22(8), e21613. https://doi.org/10.2196/21613

Kato, H. (2021). Development of a Spatio-Temporal Analysis Method to Support the Prevention of COVID-19 Infection: Space-Time Kernel Density Estimation Using GPS Location History Data. In: Urban Informatics and Future Cities. Springer. pp. 51–67. https://doi.org/10.1007/978-3-030-76059-5_4

Kedron, P., & Trgovac, A. B. (2021). Assessing Connections and Tradeoffs Between Geospatial Data Ethics, Privacy, and the Effectiveness of Digital Contact Tracing Technologies. In: Urban Informatics and Future Cities. Springer International Publishing. pp. 115–136. https://doi.org/10.1007/978-3-030-72808-3_7

Khan, A., Alahmari, A., Almuzaini, Y., et al. (2021). The Role of Digital Technology in Responding to COVID-19 Pandemic: Saudi Arabia's Experience. Risk Management and Healthcare Policy, 14, 3923–3934. https://doi.org/10.2147/rmhp.s317511

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. Available online: https://www.techrxiv.org/articles/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792 (accessed on 2 June 2023).

Kolasa, K., Mazzi, F., Leszczuk-Czubkowska, E., et al. (2021). State of the Art in Adoption of Contact Tracing Apps and Recommendations Regarding Privacy Protection and Public Health: Systematic Review. JMIR MHealth and UHealth, 9(6), e23250. https://doi.org/10.2196/23250

Krehling, L., & Essex, A. (2021). A Security and Privacy Scoring System for Contact Tracing Apps. Journal of Cybersecurity and Privacy, 1(4), 597–614. https://doi.org/10.3390/jcp1040030

Li, J., & Guo, X. (2020). Global Deployment Mappings and Challenges of Contact-tracing Apps for COVID-19. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3609516

Lo, B., & Sim, I. (2021). Ethical Framework for Assessing Manual and Digital Contact Tracing for COVID-19. Annals of Internal Medicine, 174(3), 395–400. https://doi.org/10.7326/M20-5834

Mbunge, E., Akinnuwesi, B., Fashoto, S. G., et al. (2021). A critical review of emerging technologies for tackling the COVID -19 pandemic. Human Behavior and Emerging Technologies, 3(1), 25–39. https://doi.org/10.1002/hbe2.237

Mbunge, E., Dzinamarira, T., Fashoto, S. G., et al. (2021). Emerging technologies and COVID-19 digital vaccination certificates and passports. Public Health in Practice, 2, 100136. https://doi.org/10.1016/j.puhip.2021.100136

Mbunge, E., Fashoto, S. G., Akinnuwesi, B., et al. (2021). Ethics for integrating emerging technologies to contain COVID-19 in Zimbabwe. Human Behavior and Emerging Technologies, 3(5), 876–890. https://doi.org/10.1002/hbe2.277

Ministry of Health. (2016). Law of Practicing Healthcare Professions. Available online: https://www.moh.gov.sa/en/Ministry/Rules/Documents/Law-of-Practicing-Healthcare-Professions.pdf (accessed on 2 June 2023).

Nardo, B., Lugaresi, M., Doni, M., et al. (2021). WhatsApp video call communication between oncological patients and their families during the COVID-19 outbreak. Minerva Surgery, 76(2). https://doi.org/10.23736/S2724-5691.20.08454-0

Nasereddin, M., Glantz, E. J., Grimes, G. A., et al. (2021). Digital Contact Tracing and Privacy. Journal of Cybersecurity Education, Research and Practice, 2021(1). https://doi.org/10.62915/2472-2707.1098

National Data Management Office. (2020). Available online: https://sdaia.gov.sa/ndmo/Files/PoliciesEn.pdf (accessed on 2 June 2023).

Nekvi, M. R. I., & Haque, A. (2021). Evaluating Contact Tracing Apps for Privacy Preservation and Effectiveness. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9484522 (accessed on 2 June 2023).

Obaid, R. (2020). The apps that helped keep Saudis safe from COVID-19. Available online: https://www.arabnews.com/node/1738016/media (accessed on 2 June 2023).

Omboni, S. (2020). Telemedicine During the COVID-19 in Italy: A Missed Opportunity? Telemedicine and E-Health, 26(8), 973–975. https://doi.org/10.1089/tmj.2020.0106

Ross, G. M. (2021). I use a COVID-19 contact-tracing app. Do you? Regulatory focus and the intention to engage with contact-tracing technology. International Journal of Information Management Data Insights, 1(2), 100045. https://doi.org/10.1016/j.jjimei.2021.100045

Sert, G., Mega, E., & Karaca Dedeoğlu, A. (2021). Protecting privacy in mandatory reporting of infectious diseases during the COVID-19 pandemic: perspectives from a developing country. Journal of Medical Ethics, 48(12), 1015–1019. https://doi.org/10.1136/medethics-2021-107372

Sarabdeen, J. (2021). Health Data Privacy During Pandemic: Benefiting from Health Data Without Compromising Health Data Privacy. SSRN Electronic Journal. https://doi.org/10.2139/SSRN.3878672

Sarfo, A. K., & Karuppannan, S. (2020). Application of Geospatial Technologies in the COVID-19 Fight of Ghana. Transactions of the Indian National Academy of Engineering, 5(2), 193–204. https://doi.org/10.1007/s41403-020-00145-3

SDAIA. (2020). National Data Governance Interim Regulations. Available online: https://sdaia.gov.sa/en/SDAIA/about/Pages/RegulationsAndPolicies.aspx (accessed on 2 June 2023).

Seto, E., Challa, P., & Ware, P. (2021a). Adoption of COVID-19 Contact Tracing Apps: A Balance Between Privacy and Effectiveness. Journal of Medical Internet Research, 23(3), e25726. https://doi.org/10.2196/25726

Sharma, T., & Bashir, M. (2020). Use of apps in the COVID-19 response and the loss of privacy protection. Nature Medicine, 26(8), 1165–1167. https://doi.org/10.1038/s41591-020-0928-y

Shelby, T., Caruthers, T., Kanner, O. Y., et al. (2021). Pilot Evaluations of Two Bluetooth Contact Tracing Approaches on a University Campus: Mixed Methods Study. JMIR Formative Research, 5(10), e31086. https://doi.org/10.2196/31086

Tahir, S., Tahir, H., Sajjad, A., et al. (2021). Privacy-preserving COVID-19 contact tracing using blockchain. Journal of Communications and Networks, 23(5), 360–373. https://doi.org/10.23919/jcn.2021.000031

Tawakkalna. (2021). Available online: https://ta.sdaia.gov.sa/en/index (accessed on 2 June 2023).

Tawakkalna-Privacy. (2021). Available online: https://ta.sdaia.gov.sa/en/privacy-en (accessed on 23 June 2023).

The Embassy of the Kingdom of Saudi Arabia. (1992). Available online: http://www.saudiembassy.net/print/about/country-

information (accessed on 2 June 2023).

Toch, E., & Ayalon, O. (2021). How Mass Surveillance Can Crowd Out Installations Of COVID-19 Contact Tracing Apps A Preprint. Available online: http://toch.tau.ac.il (accessed on 12 June 2023).

Tullis, J. A., & Kar, B. (2020). Where Is the Provenance? Ethical Replicability and Reproducibility in GIScience and Its Critical Applications. Annals of the American Association of Geographers, 111(5), 1318–1328. https://doi.org/10.1080/24694452.2020.1806029

Van Zyl, I., & Mclean, N. (2021). The Ethical Implications of Digital Contact Tracing for Lgbtqia + Communities. In: Proceedings of the Virtual Conference on Implications of Information and Digital Technologies for Development.

Wirth, F. N., Johns, M., Meurers, T., et al. (2020). Citizen-Centered Mobile Health Apps Collecting Individual-Level Spatial Data for Infectious Disease Management: Scoping Review. JMIR MHealth and UHealth, 8(11), e22594. https://doi.org/10.2196/22594

Zhang, M., Chow, A., & Smith, H. (2020). COVID-19 Contact-Tracing Apps: Analysis of the Readability of Privacy Policies. Journal of Medical Internet Research, 22(12), e21572. https://doi.org/10.2196/21572

Zhang, Q. (2021). Workplace surveillance and protection of worker's privacy in Covid-19. Available online: https://www.who.int/goe/publications/goe_mhealth_web.pdf (accessed on 12 June 2023).