# Data privacy during pandemics: A systematic literature review of COVID-19 smartphone applications

**Amany Alshawi** [Corresp., 1] , **Muna Al-Razgan** [2] , **Fatima H AlKallas** [2] , **Raghad Abdullah Bin Suhaim** [2] , **Reem Al-Tamimi** [2] , **Norah Alharbi** [2] , **Sarah Omar AlSaif** [2]

[1] King Abdulaziz City for Science and Technology (KACST), Riyadh, Saudi Arabia

[2] King Saud University (KSU), Riyadh, Saudi Arabia

Corresponding Author: Amany Alshawi
Email address: aalshawi@kacst.edu.sa

**Background.** On January 8, 2020, the Centers for Disease Control and Prevention officially announced a new virus in Wuhan, China. The first novel coronavirus (COVID-19) case was discovered on December 1, 2019, implying that the disease was spreading quietly and quickly in the community before reaching the rest of the world. To deal with the virus' wide spread, countries have deployed contact tracing mobile applications to control viral transmission. Such applications collect users' information and inform them if they were in contact with an individual diagnosed with COVID-19. However, these applications might have affected human rights by breaching users' privacy.

**Methodology.** This systematic literature review followed a comprehensive methodology to highlight current research discussing such privacy issues. First, it used a search strategy to obtain 808 relevant papers published in 2020 from well-established digital libraries. Second, inclusion/exclusion criteria and the snowballing technique were applied to produce more comprehensive results. Finally, by the application of a quality assessment procedure, 40 studies were chosen.

**Results.** This review highlights privacy issues, discusses centralized and decentralized models and the different technologies affecting users' privacy, and identifies solutions to improve data privacy from three perspectives: public, law, and health considerations.

**Conclusions.** Governments need to address the privacy issues related to contact tracing apps. This can be done through enforcing special policies to guarantee users privacy. Additionally, it is important to be transparent and let users know what data is being collected and how it is being used.

1 # Data privacy during pandemics: A systematic
2 # literature review of COVID-19 smartphone
3 # applications

5 Amany Alshawi[1], Muna Alrazgan[2], Fatimah Alkallas[2], Sarah AlSaif[2], Raghad Bin Suhaim[2],
6 Reem Altamimi[2], Noura Alharbi[2]

8 [1] Communication and Information Technology Institute, King Abdulaziz City for Science
9 and Technology (KACST), Riyadh, Ar Riyad, Saudi Arabia

10 [2] College of Computer and Information Sciences, King Saud University (KSU), Riyadh, Ar
11 Riyad, Saudi Arabia.

12 **Corresponding author**

13 Amany Alshawi, PhD.

14 King Abdulaziz City for Science and Technology (KACST).

15 King Abdullah Rd, Al Raed, Riyadh, Ar Riyad, 12354, Saudi Arabia

16 Email address: aalshawi@kacst.edu.sa

## Abstract

**Background.** On January 8, 2020, the Centers for Disease Control and Prevention officially announced a new virus in Wuhan, China. The first novel COVID-19virus (COVID-19) case was discovered on December 1, 2019, implying that the disease was spreading quietly and quickly in the community before reaching the rest of the world. To deal with the virus' wide spread, countries have deployed contact-tracing mobile applications to control viral transmission. Such applications collect users' information and inform them if they were in contact with an individual diagnosed with COVID-19. However, these applications might have affected human rights by breaching users' privacy.

**Methodology.** This systematic literature review followed a comprehensive methodology to highlight current research discussing such privacy issues. First, it used a search strategy to obtain 808 relevant papers published in 2020 from well-established digital libraries. Second, inclusion/exclusion criteria and the snowballing technique were applied to produce results that are more comprehensive. Finally, by the application of a quality assessment procedure, 40 studies were chosen.

**Results.** This review highlights privacy issues, discusses centralized and decentralized models and the different technologies affecting users' privacy, and identifies solutions to improve data privacy from three perspectives: public, law, and health considerations.

**Conclusions.** Governments need to address the privacy issues related to contact-tracing apps. This can be done through enforcing special policies to guarantee users privacy. Additionally, it is important to be transparent and let users know what data is being collected and how it is being used.

## Introduction

At the end of December 2019, a new COVID-19virus appeared in Wuhan, China. The novel virus severe acute respiratory syndrome (SARS-CoV-2), a COVID-19virus family member, produces an infectious disease known as COVID-19, causing illnesses that vary from the common cold to more severe diseases (Sharma et al., 2020; Skoll, Miller & Saxon, 2020).

The rapid global spread of COVID-19virus overwhelmed health sectors and caused a significant worldwide public health crisis, prompting the World Health Organization (WHO) to declare COVID-19 a global pandemic (Whaiduzzaman et al., 2020). The virus has affected human life in many different aspects: travelling, education, business, entertainment, and others (Mbunge, 2020).

Due to the virus' spread, many countries have taken measures and imposed restrictions like lockdowns, limiting activities requiring human gathering and interactions (De, Pandey & Pal, 2020). Consequently, national governments seek solutions to minimize infected cases, which results in employing digital surveillance technologies to contain the virus. A few countries have managed and controlled the pandemic using such technologies and developing smartphone apps and information system technologies to control the virus' spread (Dwivedi; 2020). Specifically, when an individual is diagnosed with COVID-19, anyone close to them during the contagious period must quarantine for two weeks (Cho, Ippolito & Yu, 2020). This solution requires individuals to download the app and access their sensitive data; therefore, it raises significant privacy issues.

Contact-tracing apps (Vitak & Zimmer, 2020) collect a wide range of data, including personal, location, and health and fitness data. In many countries, individuals avoid using these apps due to privacy concerns. Debates about the COVID-19 app's ethics have been largely preoccupied with privacy concerns, as these data is shared with governments, health ministries, and organizations (Hendl, Chung & Wild, 2020). It is an individual's right to understand what data these apps have access to, who has privileges to obtain them, and how their data is used (Vitak & Zimmer, 2020). Digital solutions must comply with confidentiality requirements (privacy and security) to ensure personal data protection. Examples of these actions could be obtaining users' consent, transparency, voluntary self-reporting, and anonymization. Moreover, clear and ethical principles must be stated (Hendl, Chung & Wild, 2020). When designing and deploying these apps and any other solutions, it is necessary mitigating privacy concerns.

There are a few literature reviews focused on apps developed for contact-tracing, prevention, surveillance measures, and mapping disease spread. In (Jalabneh et al., 2020) were identified 17 primary studies whose current application is to monitor and diagnose infected individuals. However, the authors only share their view concerning data privacy regarding how users' information is not necessarily accurate, which affects data analysis. Golinelli et al. identified 52 articles classified into seven categories covering public health needs addressed by recognized

78  digital solutions (Golinelli et al., 2020) in the COVID-19 pandemic context. The authors address
79  privacy in two of their identified categories, mentioning only that it would preferable the
80  applications do not collect personal data (Golinelli et al., 2020; Verma & Mishra, 2020) provides
81  a systematic review of smartphone technology applied in the fight against COVID-19.

82  Regarding the collection of users' information, there is only mention of an app developed in the
83  United Kingdom, where the data are stored in various places. Zimmermann et al. provided a set
84  of population perceptions about contact-tracing apps regarding authority trusting and individual
85  privacy, among others (Zimmermann, 2021). However, the context of such work only considers
86  the three main German-speaking countries: Germany, Austria, and Switzerland. Finally,
87  (Hussein, 2020) provides a review of several digital health surveillance systems where
88  regulations and data protection are only approached from the perspective of the pressure on users
89  to share their personal information to access such systems and apps.

90  As evident, several studies have been conducted focusing on contact-tracing apps developed
91  during the COVID-19 pandemic. Some of those studies discussed such apps about privacy and
92  ethical concerns. Nevertheless, there is an important window of opportunity for how such
93  information technologies can help health ministries and other parties contain the virus' spread.
94  Our overarching goal is to provide a better study of privacy concerns in the context of COVID-
95  19 apps. Toward this goal, we examined and analyzed the existing studies on COVID-19 apps
96  and privacy concerns and their findings, and summarized this research's efforts.

97  The remainder of this paper is as follows: Section 2 introduces our methodology for paper
98  selection and data collection, Section 3 represents our collected studies' analysis, Section 4
99  highlights implications, Section 5 discusses future work and limitations, and Section 6
100  concludes.

101  **Survey Methodology**
102  To ensure the accuracy of our systematic literary review results, we adapted and modified Liao's
103  methodology, proposed in (Liao, 2020). The methodology goes through six stages as shown in
104  Figure 1.

105  **RESEARCH QUESTIONS**

106  We aim to answer, at the end of this systematic literary review, three research questions:

107              1- What techniques are proposed to protect users' privacy in digital surveillance?

108              2- How does the law protect users' privacy in COVID-19 applications?

109              3- How do different entities contribute to preserving individuals' health privacy?

110  **SEARCH STRATEGY**

111  The search strategy consists of three steps, as defined below.

112    **Finding Keywords**

113    To find keywords related to our topic, we used Nails Project (Knutas, 2015; Salminen, 2020).
114    We then chose the words that we deemed to be the most relevant to the systematic literary
115    review topic and those most accurate from among the candidate words.

116    **Forming Search Strings**

117    From the selected words, we formalized two strings to use in the search process:

118        2.1 "Privacy" AND ("mobile application" OR "apps") AND ("COVID-19" OR "COVID-
119        19" OR "COVID-19virus" OR "COVID-19 pandemic").

120        2.2 "Privacy" AND ("mobile application" OR "apps") AND ("COVID-19" OR "COVID-
121        19" OR "COVID-19virus" OR "COVID-19 pandemic") AND ("contact-tracing" OR
122        "location privacy" OR "data protection" OR "privacy protection").

123    This systematic literary review focuses on three subjects: "COVID-19" and "privacy" in "mobile
124    applications." To ensure coverage of all papers across the field, we chose synonyms for each
125    term. In the first string, the results will be general, including any papers mentioning the three
126    main subjects. In the second string, we narrowed the results to papers related to "contact-tracing"
127    and combined it with keywords related to this term.

128    **Selecting Sources**

129    For the research process, we selected ten libraries. They are the most reliable and provide the
130    highest quality of research: Microsoft Academic (https://academic.microsoft.com/home), Wiley
131    (https://onlinelibrary.wiley.com/), IEEE (https://ieeexplore.ieee.org/Xplore/home.jsp), Sage
132    Journals (http://us.sagepub.com), Taylor & Francis (https://taylorandfrancis.com/online/),
133    Springer Link (https://link.springer.com/), Science Direct (https://www.sciencedirect.com/),
134    Scopus (https://www.scopus.com/home.uri), ACM (https://www.scopus.com/home.uri), and
135    Web of Science (https://www.webofknowledge.com/).

136    **INCLUSION AND EXCLUSION CRITERIA**

137    After exploring all the libraries' engines, we obtained 808 papers, which decreased to 565 papers
138    after duplication removal. We then filtered the papers by reading titles, keywords, and abstracts.
139    This process yielded 60 papers. We used the inclusion and exclusion criteria to filter the papers
140    as shown in Table 1.

141

142    **QUALITY ASSESSMENT CRITERIA**

143    The 60 papers from the previous step were read thoroughly and checked against quality
144    assessment questions as in Table 2. All questions were weighted to 1 point for Yes, 0 for No, and

145  0.5 for partial. Papers that scored 2 points or more were included in the final collection as shown
146  in Figure 2. Papers scoring less than 2 points were reviewed by a team member and re-scored.
147  Papers still scoring less than 2 were excluded.

148  **DOCUMENT SEARCH STRATEGY**

149  After assembling the final collection of papers, we assigned each paper to its origin library. As
150  shown in Table 3, some libraries have no papers in the final collection.

151  **SNOWBALLING**

152  For better comprehensiveness of papers, we conducted forward snowballing to cover all the
153  papers related to our topic. After reading the titles of the papers' references, we obtained 13
154  papers in the first stage. After reading the abstracts, the number decreased to 6 papers. We then
155  read the papers in their entirety and performed quality assessment, yielding 5 papers. This
156  process was repeated until no more results were produced; resulting in 40 papers. Figure 3 shows
157  the total number of papers from each data source and figure 4 illustrates the selection process.

158  **DISCUSSION**
159
160  In January 2020, WHO declared the newly-identified COVID-19 virus as a global pandemic
161  (Whaiduzzaman, 2020). When a COVID-19 patient has face-to-face contact with another person
162  for 15 minutes or more and the distance between them is less than 1.5 meters, there is a high
163  possibility the other person will become infected with the virus (Garg, 2020). Therefore, when an
164  individual is in close contact with a person diagnosed with COVID-19, the individual is advised
165  to quarantine themselves for approximately two weeks (Cho, Ippolito & Yu, 2020).

166  This process was easy to manage at the pandemic's beginning. However, with the virus'
167  widespread, it became difficult and time-consuming (Whaiduzzaman, 2020), necessitating the
168  tracing of infected, suspected, and contact persons in relation to COVID-19 patients.

169  Unlike vaccines, requiring time for development and approval (Joo & Shin, 2020), population-
170  wide contact-tracing applications can more immediately control viral spread and enable the
171  successful containment of COVID-19 or any future infectious disease (Skoll, Miller & Saxon,
172  2020; Dwivedi, 2020; Riemer et al., 2020). Many COVID-19-affected countries look at these
173  technology-based solutions, facilitating and automating limiting infection and minimizing viral
174  spread. These can be deployed following different approaches and adapting multiple
175  technologies, such as a global positioning system (GPS), Wireless Fidelity (Wi-Fi) technology,
176  and Bluetooth (Mbunge, 2020).

177  Contact-tracing refers to identifying an individual and their contacts (Vitak & Zimmer, 2020). In
178  addition to administering infected cases, contact-tracing apps trace the infection route from the
179  diagnosed individual to those with whom they have been in close contact. Traditional contact-
180  tracing is a strategy proposed more than 80 years ago. It was used as a part of the response to any

181  disease outbreak and has been implemented to control infectious diseases like the severe acute
182  respiratory syndrome (SARS) epidemic, since it is easy to adopt at any time (McLachlan et al.
183  2020; Fahey & Hino, 2020; Trang et al., 2020).

184  Different approaches exist to develop contact-tracing. The first order app identifies only the
185  individuals in direct contact with the patient. The single-step app was the enhanced version of the
186  first step. It identifies any individual in contact with an infected patient and any who became
187  infected, along with their contacts, and so on. Different apps, such as iterative and retrospective,
188  have many limitations and have failed to achieve their purpose. To bridge the gap, modern
189  contact-tracing apps were proposed, which rely on technologies like wireless and Bluetooth.
190  These apps have many features: live maps of confirmed cases, location-based tracking, and
191  quarantine and isolation monitoring. Even with these applications, from a public health
192  viewpoint, this tactic might not be ethically effective (Rowe, 2020).

193  Countries worldwide have taken different approaches and applied different technologies and
194  models to develop and roll out contact-tracing applications. Table 4 summarizes contact tracing
195  applications developed in different countries during the COVID-19 pandemic along with their
196  privacy concerns. A distribution of contact-tracing applications around the world is illustrated in
197  Figure 5.

198  Contact-tracing apps collect sensitive personal data like phone numbers, MAC addresses, and
199  GPS location data (McLachlan, 2020; Cao, 2020). Individuals' perceptions of these applications
200  vary; however, users' primary concern while using these apps is privacy, which is the key factor
201  motivating many to refrain from downloading them (Sharma, 2020; Goggin, 2020; O'Leary,
202  2020).

203  Contact-tracing raises significant privacy concerns and questions about user privacy
204  (Whaiduzzaman, 2020; Cao et al., 2020). Some considerations to bear in mind are: Are
205  individuals willing to share their contacts and locations with governments and health authorities?
206  What will happen to these data once the pandemic ends? What is this data's lifespan? For what
207  purpose will this data be used? (Dwivedi, 2020; Vitak & Zimmer, 2020; O'Leary, 2020). Privacy
208  risks can be mitigated by obtaining consent and safeguarding individuals' privacy by giving
209  them control over how their data are collected and used to encourage the continued voluntary use
210  of these apps (Mbunge, 2020; Trang, 2020; Nanni et al., 2020; Wang & Liu, 2020; Klar &
211  Lanzerath, 2020)

212  Countries worldwide have developed and deployed contact-tracing apps and adapted different
213  approaches to mitigate privacy concerns (Wang & Liu, 2020). Two technology-based solutions,
214  namely Bluetooth and GPS, are used to implement these apps. Bluetooth-based apps identify
215  whether two individuals are in the same place and whether there is a distance of at least 1.5
216  meters between them. It does not collect exact location information, but, ironically, is more

217  accurate. Users may feel they have a greater degree of privacy and may be less concerned about
218  being monitored 24/7. In contrast, GPS-based apps collect individuals' data on a 24/7 basis.

219  **Proposed techniques to protect users' privacy in digital surveillance**

220  Based on how applications collect and share information, app architecture is classified into two
221  different models: centralized and decentralized. These models differ in their approaches to
222  protecting users' privacy and the anonymity degree. In the centralized model, health authorities
223  and governments collect data from individuals regardless of whether they are healthy or
224  diagnosed with COVID-19, mapping the collected information to everyone uniquely in a central
225  server. This approach effectively controls cases if it is widely used, as it provides a
226  comprehensive view. However, the model does not ensure users' privacy because there is no
227  control over data sharing. In contrast, the decentralized model does not offer public control, as it
228  does not have a central server for data storage. Instead, individuals who tested negative or did not
229  test at all store their data locally on their devices and can check whether they were in touch with
230  infected people through public platforms that have already gone through a data anonymization
231  cycle. The sections below discuss the models in detail (Wang & Liu, 2020).

232  **Centralized Contact-tracing**

233  As abovementioned, there are two different technologies to collect individuals' information used
234  in centralized and decentralized models. This section will discuss the differences between using
235  GPS and Bluetooth technologies in the centralized model from a privacy perspective. In
236  centralized GPS-based applications, the user's places are collected and shared with the
237  authorities' servers (Joo & Shin, 2020). In centralized Bluetooth-based applications, data are
238  collected by creating random tokens at different times and exchanging with other users if they
239  happen within 6 feet. Later, each user's phone number and token are sent to health authorities,
240  informing the people that person has countered within the past two weeks if the user is found to
241  be infected. A centralized application using both GPS and Bluetooth technologies to collect
242  users' information has been deployed in India (Wang & Liu, 2020).

243  The main examples of centralized contact-tracing applications are Alipay Health Code used in
244  China and Self-Quarantine Safety Protection used in South Korea (Joo & Shin, 2020), both of
245  which are GPS-based, and TraceTogether, a Bluetooth-based app used in Singapore (Wang &
246  Liu, 2020). These apps have helped governments limit the spread of COVID-19. In the
247  centralized model, control is vested in governments and authorities, since they can trace all
248  users' health status and the number of infected people; this makes such apps more accurate and
249  efficient in quickly understanding the situation. Thus, they allow for better control of the virus
250  (Riemer, 2020).

251  When comparing Asian countries with some European countries to adopt centralized contact-
252  tracing apps, Asia have shown better control over the virus' spread than Europe. The reason can
253  be attributed to Asian citizens' willingness to sacrifice privacy in the interest of public health

254   (Cha, 2020), whereas in some European countries, such as France with the Stop-COVID app,
255   citizens refused to use contact-tracing, triggering a massive virus spread and losing control
256   (Rowe, 2020). In other words, using the most effective approach does not guarantee the best
257   results because civic readiness for and app's acceptance are crucial influencing factors.

258   Centralized applications have shown great potential to limit viral spread; however, users'
259   concerns about privacy and how their data are exposed and controlled by government and health
260   authorities have caused stress and motivated them to avoid using contact-tracing apps. This stress
261   is known as technostress: technology-caused anxiety and negative emotions. The Alipay Health
262   Code used in China is a great example of how collecting users' information increases stress and
263   anxiety. Considering its different information collection methods, like drones, GPS, QR codes,
264   and CCTV (Joo & Shin, 2020), it can be agreed it is difficult to trust the government and health
265   authorities when they do not state how they protect and process the collected information (Vitak
266   & Zimmer, 2020; Nabity-Grover, Cheung & Thatcher, 2020) .

267   Moreover, using centralized techniques has raised some privacy risks associated with each
268   technology. For GPS-based applications, the authority collects information from all users
269   regardless of infection status and broadcasts all the locations the user has visited recently when
270   someone tests positive, making it hard to maintain infected users' confidentiality. Bluetooth-
271   based applications are also vulnerable to these stated risks. Besides, there is a risk the authorities
272   will connect with another database via users' phone numbers and access sensitive information if
273   deemed necessary (Wang & Liu, 2020). Furthermore, some people think the centralized contact-
274   tracing approach infringes freedom and carries long-term risks like records of the information
275   collected during the pandemic even after ending (Rowe, 2020).

276   However, one study suggests forcing citizens to use contact-tracing apps regardless of privacy
277   concerns applying a framework complete with rules and policies punishing non-users will
278   enhance control and limit the virus' spread (Riemer, 2020).

279   **Decentralized Contact-tracing**

280   Based on the aforementioned problems with centralized contact-tracing apps, the importance of
281   using decentralized platforms offering a higher degree of privacy regarding individuals' data has
282   emerged (Cho et al., 2020). Decentralized contact-tracing provides more privacy because, unlike
283   in the centralized model, it has mechanisms to verify privacy and use public and private keys and
284   digital signatures (Skoll, Miller & Saxon, 2020)

285   The solutions provided in the distributed approach can utilize either GPS or Bluetooth, both
286   offering a degree of privacy. With Bluetooth, data are transferred in a phone-to-phone
287   transaction: location data are sent directly without an HTTP connection. Compared to GPS,
288   Bluetooth is more private, as GPS applications share data via HTTP protocol. However, both can
289   offer more privacy when used with blockchain (Garg et al., 2020).

290    BayesCOVID is a GPS approach combining contact-tracing, symptom tracking, and Bayesian
291    network. This approach gives the user a choice, since it provides a user contract that enhances
292    the application's utility (McLachlan, 2020).

293    One important solution is the Apple/Google Bluetooth approach that prioritized individuals'
294    privacy by using Privacy-Pre-Serving Proximity Tracing (DP-3 T) with both the SARS and the
295    Middle East Respiratory Syndrome (MERS) outbreaks. This method provides a high degree of
296    privacy, since it uses Bluetooth, which offers more location privacy than GPS (Fahey & Hino,
297    2020; Wang & Liu, 2020) and avoids storing data (location, users' identities, contacts) in
298    archives. This approach is very secure and provides a high degree of privacy. Unfortunately, it
299    taxes on smartphones' battery life, which is a drawback for users (Fahey & Hino, 2020).

300    However, offering users control is encouraging. Specifically, users can control which data are
301    being transferred and which are not. This approach uses two models: simple data transfer and
302    distributed computation. It also ensures self-awareness, which will encourage users to risk
303    sharing data (Nanni et al., 2020).

304    Furthermore, the decentralized technique provides a high degree of privacy because it uses two-
305    factor authentication blockchain. It also uses personal data without storing it in a database. It
306    accomplishes this with encoded data storage, which can be accessed with users' consent. This
307    approach cryptographically signs user data and stores it. When the data are deleted, the hash will
308    redirect to a null reference called "orphan hash." This approach has the advantage of
309    encouraging users to trust contact-tracing applications, which will help restore normal life sooner
310    (Eisenstadt et al., 2020).

311    Based on the outcome of this SLR and our findings, we present the following future
312    considerations and directions for contact tracing apps and related technologies in the fight
313    against COVID-19 and future pandemic outbreaks that are worth investigating and implementing
314    to encourage adoption by the wider population:

315    Utilizing privacy-protecting technologies such as Artificial Intelligence (AI) and Machine
316    Learning (ML) is suggested to help analyze the level of infection by viruses through
317    identification of infected areas, tracing, and monitoring infected people (Vaishya, et al., 2020;
318    Ahmed et al., 2020). Other researchers (Yang et al., 2020; Ting et al., 2020) propose the use of the
319    Internet of Things (IoT) and thermal imaging devices (Chamberlain et al., 2020; Mohammed et
320    al., 2019) to track positive cases and control the wide spread of COVID-19 virus. Additionally,
321    some studies proposed use of a privacy-preserving contact-tracing scheme through blockchain-
322    based medical applications (Zhang et al., 2020; Chang et al., 220).

323    Governments, decision makers, and public health authorities must implement a proper feedback
324    system throughout contact tracing apps deployment phases to gain public trust and increase
325    adoption levels. It must be very clear to users what data is being collected, who is accessing the
326    data, and how it is being used. It is key to study and understand human behavior throughout the

327  design and development phases of the apps before their actual implementation. Authorities could
328  implement multiple models and theories, such as the technology acceptance model, diffusion of
329  innovation model, and motivation theory, to study the acceptance and usage level of future
330  contact tracing technologies (Lucivero et al., 2020; He et al., 2021; Sharma et al., 2020).

331  Lastly, it is necessary to focus on privacy and data transformation while minimizing data
332  collection and access to reduce contact-tracing privacy concerns (Fahey & Hino, 2020).

333  **Privacy protection laws for COVID-19 applications**

334  Data privacy, also known as information privacy, is a subset of data security that focuses on data
335  management while complying with data security guidelines. The essence of data privacy is how
336  data should be collected, stored, managed, and shared. Practical data privacy issues often revolve
337  around whether or not data is shared with third parties, how it is shared, and how data is lawfully
338  collected and preserved. With the rise of the digital economy, one of the most difficult issues for
339  organizations to address is data privacy. As a result, adhering to a data privacy policy and
340  managing the data that is required is crucial in order to gain users' confidence.

341  With the individual as the major character, data privacy involves not only the proper handling of
342  data but also the public expectations about privacy. Individuals are entitled to privacy and
343  control over their personal information. Procedures for safely and securely keeping, processing,
344  acquiring, and sharing personal data must be implemented at all times.

345  Consumers' data protection and privacy are vital in today's technology era, therefore
346  governments, healthcare providers, and business groups have been using digital tracking to keep
347  COVID-19 outbreaks under control. Although this method has the potential to minimize
348  pandemic transmission, it has significant privacy implications (Sharma 2020; Callie 2021).

349  There is tension between privacy and information disclosure, and the data's privacy managed by
350  digital health apps must be maintained to limit the virus spread. There are two types of COVID-
351  19 data. The first type consists of cases and special medical data, such as disease statistics,
352  medical sources, and the history of cases in contact with the disease. The second type is data
353  related to government-imposed containment policies and health measures, such as social
354  distancing and quarantine.

355  A problem has emerged in the data managed in COVID-19 applications and on social media:
356  data and information are released from various sources, confusing the public about what
357  information is true and which sources are credible. The main sources of COVID-19 data and
358  information are government agencies, local governments, health authorities, and international
359  organizations such as the World Health Organization (WHO). The data and information
360  administered by COVID-19 digital health apps has helped limit the epidemic spread through
361  disclosure, specifically facilitating people's understanding of the containment measures. This has
362  been effective because people are more willing to comply with containment measures when they

363 understand the issues raised around the virus. Additionally, this will result in raising awareness
364 and acceptance of policies, and an enhanced sense of safety.

365 Finally, information disclosure reshapes people's perceptions of the epidemic and containment
366 measures, enabling the public to overcome difficulties and limit the virus' spread. However,
367 disclosure should be performed only with individual consent (Fu et al., 2020).

### 1. Protection Law:

369 COVID-19 is the most recent danger posing a threat to the world's health and economic sectors.
370 Tracing the main and secondary contacts of confirmed COVID-19 cases using contact-tracing
371 technologies and devices is one of the most effective approaches to reduce the spread of the
372 virus. The European Union (EU) emphasized the importance of data protection and privacy in
373 digital measures, stating that data must be used exclusively for the intended purpose, that is, to
374 prevent the spread of disease. Strategies to contain the pandemic include the use of technology to
375 contain and warn those who have been in contact with people infected.

376 The benefits gained by tracking people are greater than the potential of losing users privacy
377 because of its desired benefits to eliminate virus outbreaks (Gallaway, 2020; Schneble, 2020).
378 The EU, which has a robust data protection system, requires that all states share personal data
379 that has been collected through contact-tracing applications.

380 The US Government and the public sought to develop consumer data privacy protection laws.
381 The value of privacy was stressed by multiple entities including elected leaders, members of
382 congress, and others by emphasizing a myriad of possible harms connected with its violation.
383 Privacy protection also helps guard against fraudulent or economic damage caused by identity
384 theft, fraud, extortion, or other acts of crime. Guaranteeing information privacy is also important
385 to reduce public fears of divulging details of their private lives, such as their personal contacts or
386 behavioral habits, in the context of health-related data.

387 Most mobile phone applications that track symptoms or trace contacts require widespread use
388 among the population, which is only achieved if users trust these apps. Some of the common
389 privacy protection criteria of smartphone apps are transparency, purpose, anonymity, informed
390 consent, time limits, and data management.

391 Transparency requires straightforward software reporting policies, which help to create public
392 confidence in governments and health organizations, all of which are important to promote
393 informed and voluntary use of COVID-19 related services.

394 Anonymization is the use of a series of mechanisms to prevent data from being associated to a
395 specific person. Informed consent ensures that consumers have the information they need to
396 make informed decisions about willingly releasing confidential personal data in order to respond
397 to public health requirements. Time limits means ensuring that the data obtained about contacts,
398 location tracking, and mobile device proximity can only be used in the scope of the crisis. Data

399  management means applying all protections measures throughout the life cycle of data-collection
400  systems for contact-tracing mobile apps (Boudreaux, 2020).

401  COVID-19 apps should be free from security and privacy problems because these aspects are
402  important to users. Legal protection must also be provided because a lack of privacy will lead to
403  application failure if users shy away from using these applications due to a lack of trust (Hendl,
404  Chung & Wild, 2020; Culnane, Leins & Rubinstein, 2020; Islam et al., 2020).

405  **2. Ethical**

406  In addition to privacy concerns, there are many ethical issues related to the data collection
407  processes and algorithms of contact-tracing apps. During the COVID-19 pandemic, governments
408  and healthcare organizations rely on location and health data to assess infection rates,
409  effectiveness of social distancing measures, and disease transmission rates. As COVID-19
410  spreads, several COVID-19 tracking applications were developed to aid in the containment of the
411  pandemic. A framework has been established to validate COVID-19 apps' ethics. It is intended
412  to assist designers and publishers of contact-tracing apps in determining the application's ethical
413  justification. If used properly, the apps should be a major component of disease management,
414  proportional to the severity of the public health threat and scientifically sound and time-bound
415  ethical design. Following the COVID-19 breakout, these groups must utilize this data in an
416  ethical, robust, and transparent manner to prevent widespread skepticism and any breaches of
417  privacy rights (Klar & Lanzerath, 2020).

418  **3. Values**

419  When viruses start to cause safety issues, the balance between the need to fight the virus and the
420  obligation to uphold individual rights often changes. COVID-19 tracing apps illustrates how
421  close monitoring and contact-tracing compromises privacy rights around the world. In response
422  to the epidemic, the Australian government created COVID-19 Safe, a mobile phone app for
423  contact-tracing. Governments around the world have also been using technology to help maintain
424  social distancing, isolation, and contact-tracing.

425  Moreover, with privacy as a major concern, COVID-19 apps must be built explicitly based on
426  values including fairness, equality, solidarity, and user benefit. Due to the high privacy impact,
427  data sharing is only possible when there are serious health conditions. There are cases in which
428  governments receiving personal data must be identified. All population groups should be able to
429  use COVID-19 surveillance technology which respects their privacy (Lodders & Paterson, 2020;
430  van Kolfschooten & de Ruijter, 2020; Lee & Lee, 2020).The use of the contact-tracing process is
431  unprecedented and could have serious consequences for public health. It is necessary to
432  implement public-interest digital technology practices that are in line with values (Lodders et.
433  Al, 2021; Kolfschooten & Ruijter, 2020; Lee & Lee, 2020).

434

### 4. Issues

435

436 As mentioned before, employing digital surveillance technologies to contain the virus raised
437 several privacy issues related to the use, storage, and manipulation of collected personal
438 information. Individuals' concerns about their privacy prevented them from using such apps,
439 which obviously affected the tracing process considerably. Those individuals questioned the
440 integrity of the data collection and utilization processes and whether the data will be anonymous,
441 temporarily stored, or open to public use. Figure 6 illustrates the most important privacy issues
442 of contact-tracing apps.

443 To fulfill privacy guidelines to the highest degree, tracing apps should clearly reveal for which
444 purpose the data will be used, and whom will have access to it and control it. In addition, the data
445 should only be stored by authorized agencies. Health care agencies must clarify what will
446 happened to the data in the future after the pandemic is over. All tracing apps must comply with
447 the international privacy standards to minimize public privacy concerns.

448 On the other side, these issues can be eliminated from technological perspective by applying
449 more secure and private models. Two popular models have been used in designing tracing apps,
450 which are centralized and decentralized. After comparing these two models, the decentralized
451 model proved to be more secure and reliable, especially when used with Bluetooth technology.

### 5. Entities contributing to preserving privacy of healthcare applications

452

453 In 1996, a law obliged the health authorities to protect patients' privacy, disclosing their data
454 only in high-risk cases and guaranteeing information privacy even during data exchange.
455 Furthermore, integration between citizens' data and the health authorities will help identify
456 infected patients and restrict their interaction with healthy people. Patients' privacy is one of the
457 most important topics raised during the COVID-19 pandemic.

458 COVID-19's proliferation has created unique circumstances that have prompted a change toward
459 telemedicine infrastructure adoption. Telemedicine has become an important part of clinical care
460 delivery, and many medical institutions report a significant increase in the use of telemedicine.
461 For example, One Medical Center in New York City, witnessed a major increase in urgent care
462 virtual visits from 102 per day pre-COVID-19, to 802 per day post-COVID-19. As the transition
463 to telemedicine progresses, new problems and dangers have emerged, especially in the areas of
464 information security and privacy.

465 The Privacy Rule, issued in December 2000 by the US Department of Health and Human
466 Services (HHS), protects the privacy of individually identifiable health information. In addition,
467 The European Union, passed a data privacy legislation to protect patient's personal health
468 information, and has one of the most effective data protection and privacy policies in the world.
469 However, government agencies around the world have warned that the risk of cyberattacks

470 against healthcare departments and institutions researching COVID-19 is increasing since the
471 pandemic started (Jalali et al., 2021)

472 There are many applied methodologies when it comes to the type of data health officials are
473 sharing with the public. In the US, the local government in Los Angeles County provides an
474 estimated age distribution of patients, and a breakdown of the number of cases in more than 140
475 cities and communities. However, residents in Florida are given much more information,
476 including the cities affected, the number of people tested, the age distribution of cases, and the
477 number of cases in nursing homes.

478 In response to the Covid-19 pandemic, the Indian Ministry of Health and Family Welfare issued
479 guidelines for the mandatory notification of information for COVID-19 patients, allowing the
480 government to enact any regulations it deems necessary to prevent the outbreak or spread of such
481 epidemics. The Indian government requires doctors to report COVID-19 cases and suspected
482 cases to designated government agencies, and the government agencies can then respond
483 appropriately to limit the disease spread based on the information provided by the health care
484 professionals (Fu et al., 2020 and Shekhawat et al., 2020)

485 Digital health apps are available in Apple Store and Google Play App Store that contain more
486 than 318,000 available applications which are updated daily, to comply with the latest policies
487 announced by the health authorities [42].

488 The Federal Data Protection Act (FADP) provides a comprehensive framework dealing with data
489 protection using defined principles. It insists on securing individuals' privacy and provides
490 protection measures. According to FADP, patient data are considered sensitive and require
491 additional privacy. Each user has to give consent for the health authorities to use their data for
492 health purposes. Therefore, the applications have to grant the user the right to revoke, update,
493 and remove the data (Vokinger et al., 2020).

494 The COVID-19 pandemic has shed light on digital health applications but ignored their data
495 privacy. Blockchain technology appears to be an ideal solution to secure and authenticate
496 certificates, health and medical records, and prescriptions, while preserving privacy (De, Pandey
497 & Pal, 2020) Doctors may disclose patients' information to competent authorities under specific
498 circumstances for society's greater interest. Quarantine and social isolation measures imposed by
499 the health authorities have effectively limited viral spread. Thus, it is important to collect
500 individuals' information via contact-tracing apps (Labs & Terry, 2020; Shekhawat et al., 2020).f

501 In conclusion, tracing applications help to control the speared of COVID-19 pandemic.
502 Governments and health authorities developed these apps based on many technologies and
503 different models. The aim of these apps is to monitor the infected individuals and keep track of
504 the public status. Some countries had followed international laws and local regulations to protect
505 users' privacy while designing and developing these apps. However, other countries did not
506 comply with these requirements, which resulted in privacy breaches. Nevertheless, there was no

507 clear guidelines regarding the disclosure of using the personal data in tracing apps. However,
508 even with the privacy limitation in tracing apps, WHO stated that they had effectively helped in
509 containing the pandemic and slowing down its spread.

510 COVID-19 has put forward privacy concerns in many fields, and this systematic literature review
511 has discussed it from three perspectives: the public's privacy in using contact-tracing apps, laws
512 and policies that should be followed to protect users' privacy and digital authorities' strategies
513 for dealing with data privacy. The classifications of the included literature is illustrated in Figure
514 7.

515 **IMPLICATIONS**
516

517 Many persons avoid using COVID-19 apps due to privacy concerns about location and health
518 data (De, Pandey & Pal, 2020; Fahey & Hino, 2020). To prevent this issue, governments should
519 develop policies ensuring individual data privacy rights, encouraging people to trust these apps
520 and provide their information voluntarily (Lee & Lee, 2020).

521 Another implication: not all citizens have internet access. The solution is providing universal
522 internet so that everyone can access COVID-19 apps. Moreover, some individuals do not have
523 their own devices, raising the issue these apps may not cover all citizens. This challenge can be
524 surmounted by assigning one account per family to reach the highest number of users (De,
525 Pandey & Pal, 2020; Rowe, 2020).

526 Lastly, COVID-19 problems are widespread since it is a new virus, but researchers are trying to
527 address each concern to reduce the virus' effects and minimize its spread (De, Pandey & Pal,
528 2020; Hendl, Chung & Wild, 2020)

529 **LIMITATIONS AND FUTURE WORK**
530

531 COVID-19 has revealed many limitations in many areas such as information management and
532 data privacy; therefore, digital surveillance has become more important than ever. Artificial
533 intelligence, big data, the internet of things, and GPS have been recognized as paramount
534 technologies in developing COVID-19 contact-tracing apps (Mbunge, 2020; Joo & Shin, 2020;
535 Fahey & Hino, 2020).

536 Privacy protection is an important issue. In the context of digital health and the COVID-19
537 epidemic, within a framework for evaluating applications from epidemiological and legal
538 perspectives, solutions are designed to obtain useful information with several limitations,
539 including preventing sharing sensitive personal information (Sharma, 2020, Nanni et al., 2020;
540 Vokinger, 2020).

541  The studies did not cover all classifications of COVID-19 research's keywords, and they are also
542  restricted to specific countries' cultures and policies. Moreover, the studies did not consider the
543  differences in values and cultural and political aspects of the countries using tracking
544  applications. Additionally, no study has discussed contact-tracing applications developed after
545  April 30, 2020 (Garg at al., 2020; Trang et al., 2020; Islam et al., 2020; Kumar, Shahrabani &
546  Das, 2020). For the future, Garg expects to develop an RFID solution and aims to reduce the cost
547  of scaling the RFID range (Garg et al., 2020)

548  The COVID-19 pandemic is a recent one, hence applications in this field are limited. The study
549  found that a limited number of mobile applications were developed, which will be used as a
550  benchmark for future applications' specifications and learn more about users' interactions on
551  different national app platforms. That result makes a significant contribution to health institutes
552  and health practitioners (Trang et al., 2020; Islam et al., 2020).

553  During epidemics, it has been suggested it is prudent to allow for some loss of privacy and place
554  trust in smart technologies to help fight deadly, invisible creatures. With the continuing spread of
555  COVID-19, Singapore will continue to deploy technological tools and interventions (Lee & Lee,
556  2020).

557  A limitation of future research on an ultimate dependent variable is the adoption of COVID-19
558  applications recommendations for pre- and post-testing in future studies. Emphasis should be
559  placed on collecting data about infectious diseases, ensuring public health and that
560  epidemiological surveillance technology features are ethical and reflective of fair values, and
561  reducing the vulnerability of at-risk individuals (Sharma et al., 2020; Skoll, Miller & Saxon,
562  2020; Whaiduzzaman et al., 2020; Hendl, Chung & Wild, 2020).

563  Moreover, developing and improving the efficiency and effectiveness of information systems
564  and technology in organizations as well as monitoring people's safety and privacy in the fight
565  against COVID-19 (Mbunge, 2020; O'Leary, 2020; Wang & Liu, 2020) are essential.
566  Additionally, expanding anti-snooper privacy safeguards, imposing usage restrictions in contact-
567  tracing, and adding a private messaging system will enhance overall privacy. There have been
568  discussions about creating an application to track contacts directly using Bluetooth (Cho, ; Vitak
569  & Zimmer, 2020).

570  ## Conclusion

571

572  The effect of the COVID-19 pandemic represents an enormous challenge to public health
573  authorities and governments around the world. The pandemic put major pressure on health
574  systems and resulted in fundamental changes to everyday life for individuals and organizations.
575  Public health authorities introduced contact-tracing systems which include the use of digital
576  contact-tracing mobile apps. Contact-tracing apps are promising technologies for rapid tracing
577  and tracking of infected persons, and they can support manual contact-tracing and tracking
578  methods to control the COVID-19 virus. However, some people avoid using digital surveillance

579 apps altogether since they are concerned about their privacy. Governments and health authorities
580 should address this issue and try to preserve the rights of those who do not wish to waive their
581 privacy.

582 In most countries, the use of these apps is not mandatory, which makes it challenging to predict
583 their acceptance and participation levels. It is significant for governments and health officials to
584 gain the trust of their citizens and show suitable transparency by clarifying what personal data is
585 collected and how it is being used. The efficiency of contact-tracing apps is highly dependent on
586 how authorities address all related privacy challenges and concerns. Their efforts will surely
587 determine the role of digital contact-tracing technologies in future pandemic occurrences and
588 lessons learned from similar errors.
589
590 The challenges facing contact-tracing apps include, in addition to privacy, technical, usability,
591 and addressing additional requirements reported by some users. A considerable number of
592 contact-tracing apps were not welcomed by the public and suffered low acceptance levels, which
593 dramatically affected their efficiency. As an example, only the Singaporean app had a
594 penetration level of a little over 30%, the Australian and Swiss apps had a penetration level
595 below 20%, and the penetration values for the majority of other apps around the world were less
596 than 5%.
597
598 The volume of personal data contact-tracing apps collected varied considerably, some apps
599 collected absolutely no data while others collected a significant amount of highly private
600 personal data. The majority of the surveyed apps did not give users an option to deactivate the
601 app, such as logging out, without uninstalling them. Additionally, the lack of standardization for
602 contact-tracing technologies resulted in fragmented non-interoperable apps. As countries are
603 coming out of lockdown and reopening borders, there is an essential need for a unified and
604 interoperable contact-tracing app that can easily be implemented globally without compromising
605 users' privacy.
606
607 A possible solution to the privacy issues and concerns can be implemented through a
608 comprehensive government-mandated data privacy policy in the context of digital health
609 applications. Another option is for governments to deploy fully decentralized and highly accurate
610 applications, which do not keep any records of sensitive personal information and provide the
611 same level of accuracy as the centralized approach. One suggestion for a decentralized approach
612 is to use a blockchain-based app algorithm balancing users' privacy and public health
613 requirements. Moreover, internet intermediaries must work with governments and civil society to
614 address privacy and surveillance issues to improve new contact-tracing technology adoption
615 levels in the future.

## Acknowledgements

617 We thank King Abdulaziz City for Science and Technology (KACST) and King Saud University
618 (KSU) for providing all the necessary technical tools for data collection and analysis.

# References

620 **References**

621 ACM Digital Library. Available at: https://dl.acm.org/ (accessed 25 December 2020)

622 Ahmed N, Michelin RA, Xue W, Ruj S, Malaney R, Kanhere SS, Seneviratne A, Hu W, Janicke
623     H, Jha SK. A survey of COVID-19 contact tracing apps. IEEE Access. 2020;8:134577–
624     601. https://doi.org/10.1109/ ACCESS.2020.3010226.

625 Boudreaux, Benjamin, Matthew A. DeNardo, Sarah W. Denton, Ricardo Sanchez, Katie Feistel,
626     and Hardika Dayalani. 2020. Data Privacy During Pandemics: A Scorecard Approach for
627     Evaluating the Privacy Implications of COVID-19 Mobile Phone Surveillance Programs.
628     Santa Monica, CA: RAND Corporation.
629     https://www.rand.org/pubs/research_reports/RRA365-1.html.

630 Cao Y, Takagi S, Xiao Y, Xiong L, Yoshikawa M. 2020. PANDA: Policy-aware location
631     privacy for epidemic surveillance. Proceedings of the VLDB Endowment 13(12):3001–
632     3004. DOI: 10.14778/3415478.3415529 (accessed 15 November 2020)

633 Cha V. 2020. Asia's COVID-19 lessons for the West: public goods, privacy, and social tagging.
634     The Washington Quarterly 43:1–18. DOI: 10.1080/0163660X.2020.1770959.

635 Chang MC, Park D. How can blockchain help people in the event of pandemics such as the
636     COVID-19? J Med Syst. 2020;44:102. https://doi. org/10.1007/s10916-020-01577-8.

637 Chamberlain SD, Singh I, Ariza C, Daitch A, Philips P, Dalziel BD. Realtime detection of
638     COVID-19 epicenters within the United States using a network of smart thermometers.
639     MedRxiv. 2020. https://doi.org/10. 1101/2020.04.06.20039909.

640 Cho H, Ippolito D, Yu YW. 2020. Contact-tracing mobile apps for COVID-19: privacy
641     considerations and related trade-offs, http://arxiv.org/abs/2003.11511 (accessed 15
642     November 2020).

643 Culnane C, Leins K, Rubinstein BI. 2020. Tracking, tracing, trust: contemplating mitigating the
644     impact of COVID -19 through technological interventions. Medical Journal of Australia
645     213:94-94.e1 DOI: https://doi.org/10.5694/mja2.50683.

646 De R, Pandey N, Pal A. 2020. Impact of digital surge during Covid-19 pandemic: a viewpoint on
647     research and practice. International Journal of Information Management 55:102171 DOI:
648     10.1016/j.ijinfomgt.2020.102171.

649 Dwivedi YK, Hughes L, Coombs C, et al. 2020. Impact of COVID-19 pandemic on information
650     management research and practice: transforming education, work and life. International
651     Journal of Information Management 55:102211 DOI: 10.1016/j.ijinfomgt.2020.102211.

652 Eisenstadt M, Ramachandran M, Chowdhury N, et al. 2020. COVID-19 antibody
653     test/vaccination certification: there's an app for that. IEEE Open Journal of Engineering in
654     Medicine and Biology 1:148–155 DOI: 10.1109/OJEMB.2020.2999214.

655 Fahey RA, Hino A. 2020. COVID-19, digital privacy, and the social limits on data-focused
656     public health responses. International Journal of Information Management 55:102181
657     DOI: 10.1016/j.ijinfomgt.2020.102181.

658 Fu Y, Ma W, Wu J. 2020. Fostering voluntary compliance in the COVID-19 pandemic: an
659      analytical framework of information disclosure. The American Review of Public
660      Administration 50:685–691 DOI: 10.1177/0275074020942102.
661 Galloway K. 2020. The COVID cyborg: protecting data status. Alternative Law Journal 45:162–
662      167 DOI: 10.1177/1037969X20930431.
663 Garg L, Chukwu E, Nasser N, et al., 2020. Anonymity preserving IoT-based COVID-19 and
664      other infectious disease contact-tracing model. IEEE Access 8:159402–159414 DOI:
665      10.1109/ACCESS.2020.3020513.
666 Goggin G. 2020. COVID-19 apps in Singapore and Australia: reimagining healthy nations with
667      digital technology. Media International Australia 177: 61–75 DOI:
668      10.1177/1329878X20949770.
669 Golinelli D, Boetto E, Carullo G, et al., 2020. How the COVID-19 pandemic is favoring the
670      adoption of digital technologies in healthcare: a rapid literature review. MedRxiv.
671      [Preprint]. Available at:
672      https://www.medrxiv.org/content/medrxiv/early/2020/05/01/2020.04.26.20080341.full.pdf
673 He W, Zhang ZJ, Li W. Information technology solutions, challenges, and suggestions for
674      tackling the COVID-19 pandemic. Int J Inf Manag. 2021;57:102287.
675      https://doi.org/10.1016/j.ijinfomgt.2020.102287.
676 Hendl T, Chung R, Wild V. 2020. Pandemic surveillance and racialized subpopulations:
677      mitigating vulnerabilities in COVID-19 apps. Journal of Bioethical Inquiry 17: 829–834
678      DOI: 10.1007/s11673-020-10034-7.
679 Hussein MR, Apu EH, Shahabuddin S, et al. 2020. Overview of digital health surveillance
680      system during COVID-19 pandemic: public health issues and misapprehensions. arXiv,
681      preprint arXiv:2007.13633 [Preprint]. Available from: https://arxiv.org/abs/2007.13633
682      (accessed 20 Dec 2020).
683 IEEE Xplore. Available at: https://ieeexplore.ieee.org/Xplore/home.jsp (accessed 1 January
684      2021)
685 Islam MN, Islam I, Munim KMd, et al. 2020. A review on the mobile applications developed for
686      COVID-19: an exploratory analysis. IEEE Access 8: 145601–145610 DOI:
687      10.1109/ACCESS.2020.3015102.
688 Jalabneh R, Syed HZ, Pillai S, et al. 2020. Use of mobile phone apps for contact-tracing to
689      control the COVID-19 pandemic: a literature review. SSRN DOI: 10.2139/ssrn.3641961.
690 Jalali, Mohammad S, Landman, Adam & William J Gordon. 2021. Telemedicine, privacy, and
691      information security in the age of COVID-19, Journal of the American Medical
692      Informatics Association, (28) 3, 671–672
693 Joo J, Shin MM. 2020. Resolving the tension between full utilization of contact-tracing app
694      services and user stress as an effort to control the COVID-19 pandemic. Service Business
695      14: 461–478 DOI: 10.1007/s11628-020-00424-7.
696 Klar R, Lanzerath D. 2020. The ethics of COVID-19 tracking apps – challenges and
697      voluntariness. Research Ethics 16:1–9 DOI: 10.1177/1747016120943622.

698 Knutas A, Hajikhani A, Salminen J, et al. 2015. Cloud-based bibliometric analysis service for
699     systematic mapping studies. Proceedings of the 16th International Conference on
700     Computer Systems and Technologies - CompSysTech'15 184 –91 DOI:
701     10.1145/2812428.2812442.

702 Kumar S, Shahrabani S, Das M. 2020. Developing a mobile app (iGAM) to promote gingival
703     health by professional monitoring of dental selfies: user-centered design approach. JMIR
704     mHealth and uHealth 8:e19433 DOI: 10.2196/19433.

705 Labs J, Terry S. 2020. Privacy in the COVID-19virus era. Genetic Testing and Molecular
706     Biomarkers 24: 535–536 DOI: 10.1089/gtmb.2020.29055.sjt.

707 Lee T, Lee H. 2020. Tracing surveillance and auto-regulation in Singapore: 'smart' responses to
708     COVID-19. Media International Australia 177: 47–60 DOI: 10.1177/1329878X20949545.

709 Liao, Ben, Ali, Yasser, Nazir, Shah, He, Long. 2020. Security analysis of IoT devices by using
710     mobile computing: a systematic literature review. IEEE Access 8:120331–120350 DOI:
711     10.1109/ACCESS.2020.3006358.

712 Lodders A, Paterson JM. 2020. Scrutinising COVIDSafe: frameworks for evaluating digital
713     contact-tracing technologies. Alternate Law Journal 45:153–61 DOI:
714     10.1177/1037969X20948262.

715 Lucivero F, Hallowell N, Johnson S, Prainsack B, Samuel G, Sharon T. COVID-19 and contact
716     tracing apps: ethical challenges for a social experiment on a global scale. J Bioeth Inq.
717     2020. https://doi.org/10. 1007/s11673-020-10016-9.

718 Mbunge E. 2020. Integrating emerging technologies into COVID-19 contact-tracing:
719     opportunities, challenges and pitfalls. Diabetes & Metabolic Syndrome 14: 1631–1636.
720     DOI:  10.1016/j.dsx.2020.08.029 .

721 McLachlan S, Lucas P, Dube K, et al. 2020. Bluetooth smartphone apps: are they the most
722     private and effective solution for COVID-19 contact-tracing? Available at:
723     https://arxiv.org/abs/2005.06621 (accessed 3 March 2021).

724 Microsoft Academic. Available at: https://academic.microsoft.com/home (accessed 5 January
725     2020)

726 Mohammed MN, Hazairin NA, Syamsudin H, Al-Zubaidi S, Sairah AK, Mustapha S, Yusuf E.
727     2019 novel coronavirus disease (Covid-19): detection and diagnosis system using iot
728     based smart glasses, Int. J. Adv. Sci. Technol. (2020)

729 Monroe, Callie , Tazi, Faiza, &  Sanchari, Das. 2021 Location Data and COVID-19 Contact
730     Tracing: How Data Privacy Regulations and Cell Service Providers Work In Tandem.
731     Cryptography and Security, 18(2) 20.

732 Nabity-Grover T, Cheung CMK, Thatcher JB. 2020. Inside out and outside in: how the COVID-
733     19 pandemic affects self-disclosure on social media. International Journal of Information
734     Management 55: 102188 DOI: 10.1016/j.ijinfomgt.2020.102188.

735 Nanni M, Andrienko G, Barabási AL, et al. 2020. Give more data, awareness and control to
736     individual citizens, and they will help COVID-19 containment. Ethics and Information
737     Technology, DOI: 10.1007/s10676-020-09572-w.

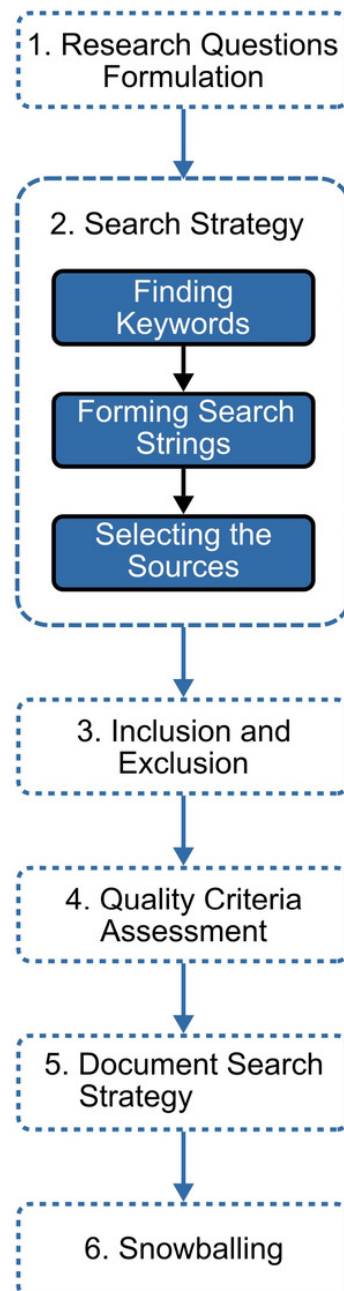
738    O'Leary DE. 2020. Evolving information systems and technology research issues for COVID-19
739        and other pandemics. Journal of Organizational Computing and Electronic Commerce 30:
740        1–8 DOI: 10.1080/10919392.2020.1755790.
741    Riemer K, Ciriello R, Peter S, et al. 2020. Digital contact-tracing adoption in the COVID-19
742        pandemic: IT governance for collective action at the societal level. European Journal of
743        Information Systems 29: 731–745 DOI: 10.1080/0960085X.2020.1819898.
744    Rowe F. 2020. Contact-tracing apps and values dilemmas: A privacy paradox in a neo-liberal
745        world. International Journal of Information Management 55: 102178 DOI:
746        10.1016/j.ijinfomgt.2020.102178. Sage Publications Inc. Available at:
747        http://us.sagepub.com/ (accessed 10 February 2020)
748    Salminen J, Knutas A, Hajikhani A. 2020. nailsproject.net [Internet] Network Analysis Interface
749        for Literature Studies. by Juho Salminen, Antti Knutas and Arash Hajikhani. Available
750        atfrom: https://nailsproject.net/ (accessed 1 March 2020)
751    Schneble CO, Elger BS, Shaw DM. 2020. Data protection during the COVID-19virus crisis.
752        EMBO Reports 21: e51362 DOI: 10.15252/embr.202051362. ScienceDirect. Available at:
753        https://www.sciencedirect.com/ (accessed 1 March 2020)
754    Scopus Preview. Available at: https://www.scopus.com/home.uri (accessed 5 March 2020)
755    Sharma S, Singh G, Sharma R, et al. 2020. Digital health innovation: exploring adoption of
756        COVID-19 digital contact-tracing Apps. IEEE Transactions on Engineering Management
757        1–17 DOI: 10.1109/TEM.2020.3019033.
758    Shekhawat RS, Meshram VP, Kanchan T, et al. 2020. Privacy and patient confidentiality in
759        times of Covid-19. Medico-Legal Journal 88: 229-230 DOI: 10.1177/0025817220935908.
760    Skoll D, Miller JC, Saxon LA. 2020. COVID-19 testing and infection surveillance: is a
761        combined digital contact-tracing and mass-testing solution feasible in the United States.
762        Cardiovascular Digital Health Journal 1: 149–159 DOI: 10.1016/j.cvdhj.2020.09.004.
763    Springer Link. Available at: https://link.springer.com/ (accessed 10 January 2020)
764    Taylor & Francis Group. Available at: https://taylorandfrancis.com/online/ (accessed 10 January)
765    Ting DSW, Carin L, Dzau V, Wong TY. Digital technology and COVID-19. Nat Med.
766        2020;26:459– https://doi.org/10.1038/s41591-020-0824-5
767    Trang S, Trenz M, Weiger WH, et al. 2020. One app to trace them all? Examining app
768        specifications for mass acceptance of contact-tracing apps. European Journal of
769        Information Systems 29: 415–428 DOI: 10.1080/0960085X.2020.1784046.
770    Vaishya R, Javaid M, Khan IH, Haleem A. Artifcial Intelligence (AI) applications for COVID-
771        19 pandemic. Diabetes Metab Syndr Clin Res Rev. 2020.
772        https://doi.org/10.1016/j.dsx.2020.04.012
773    Van Kolfschooten H, de Ruijter A. 2020. COVID-19 and privacy in the European Union: a legal
774        perspective on contact-tracing. Contemporary Security Policy 41: 478–491 DOI:
775        10.1080/13523260.2020.1771509.
776    Verma J, Mishra AS. 2020. COVID-19 infection: disease detection and mobile technology. PeerJ
777        8: e10345 DOI: 10.7717/peerj.10345

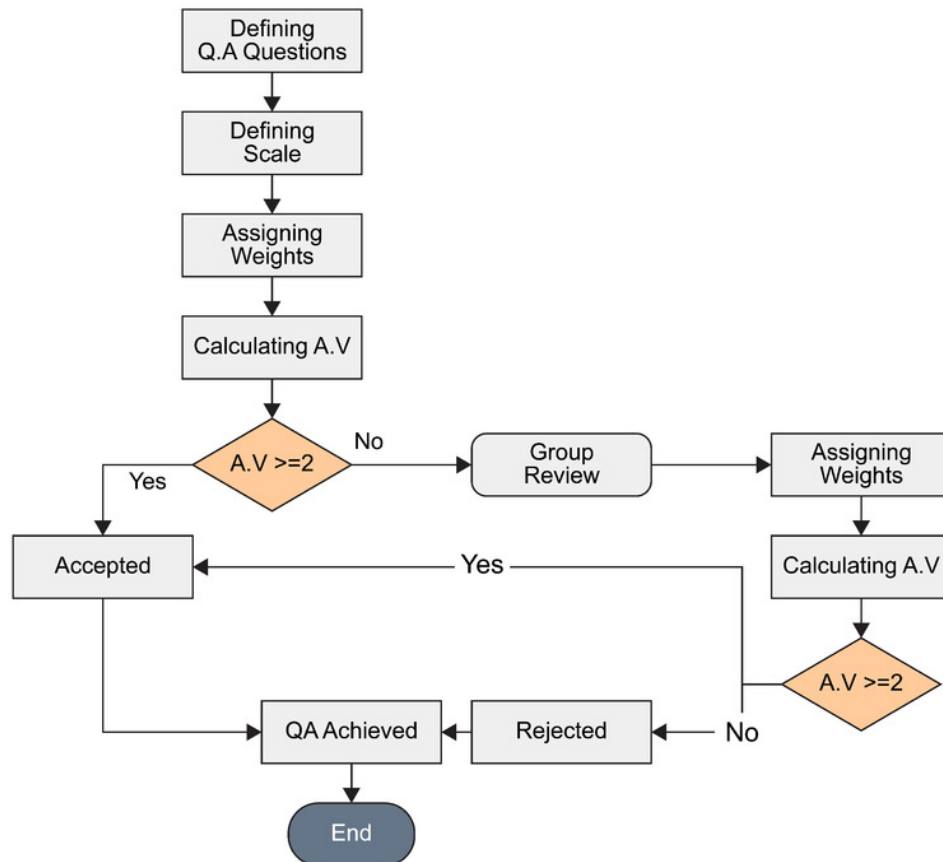
778    Vitak J, Zimmer M. 2020. More than just privacy: using contextual integrity to evaluate the long-
779        term risks from COVID-19 surveillance technologies. Social Media + Society. 6:
780        205630512094825 DOI: 10.1177/2056305120948250.
781    Vokinger, Krestin N, Visilious, Nittas, Witt, Claudia M, Fabrikantd, Sara Irina, von
782        Wylbe,Viktor. 2020. Digital health and the COVID-19 epidemic: an assessment
783        framework for apps from an epidemiological and legal perspective. Swiss Medical
784        Weekly 150: w20282 DOI: 10.4414/smw.2020.20282.
785    Wang D, Liu F. 2020. Privacy risk and preservation in contact-tracing of COVID-19. CHANCE
786        33: 49–55 DOI: 10.1080/09332480.2020.1820252.
787    Web of Science. Available at: https://www.webofknowledge.com/ (accessed 12 February 2020)
788    Whaiduzzaman Md, Hossain MR, Shovon AR, et al. 2020. A Privacy-preserving mobile and fog
789        computing framework to trace and prevent COVID-19 community transmission. IEEE
790        Journal of Biomedical and Health Informatics 24: 3564–3575 DOI:
791        10.1109/JBHI.2020.3026060.
792    Wiley Online Library. Available at: https://onlinelibrary.wiley.com/ (accessed 15 January 2020)
793    Yang T, Gentile M, Shen CF, Cheng CM. Combining point-of-care diagnostics and internet of
794        medical things (IOMT) to combat the Covid-19 pandemic. Diagnostics. 2020.
795        https://doi.org/10.3390/diagnostics1004 0224.
796    Zhang C, Xu C, Sharif K, Zhu L. Privacy-preserving contact tracing in 5G-integrated and
797        blockchain-based medical applications. Comput Stand Interfaces. 2021; 77:103520.
798        https://doi.org/10.1016/j.csi.2021. 103520.
799    Zimmermann, Bettina Maria, Fiske, Amelia, Prainsack, Barbara, Hangel, Nora, McLennan,
800        Stuart, Buyx, Alena. 2021. Early perceptions of COVID-19 contact-tracing apps in
801        German-speaking countries: comparative mixed methods study. J Med Internet Res 23:
802        e25525 DOI: https://www.jmir.org/2021/2/e25525

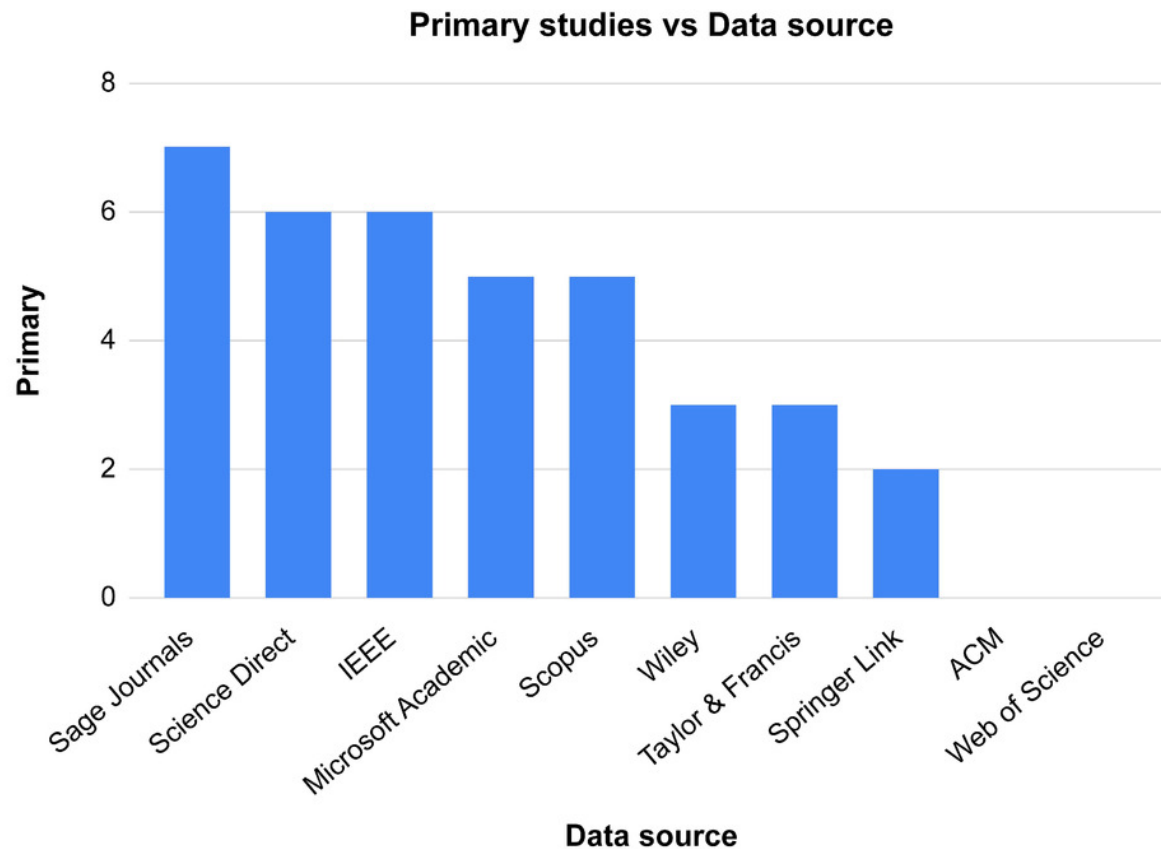
803
804    **Figure Legends**

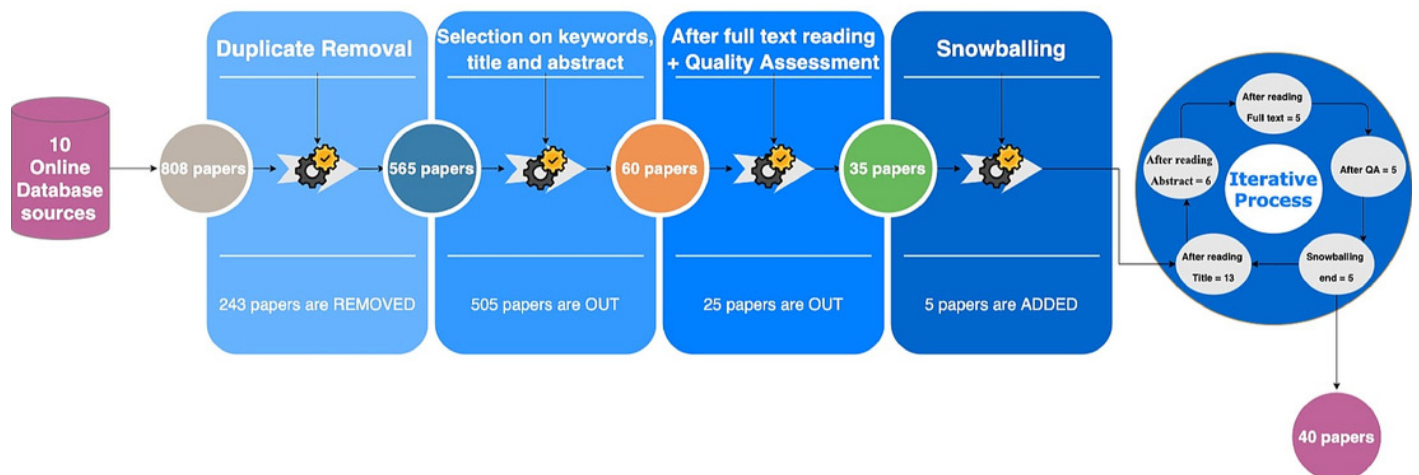
805    Figure 1. The Methodology's Main Stages.
806    Figure 2. Quality Assessment Flow Chart
807    Figure 3. Total Number of Papers from Each Data Source
808    Figure 4. Paper Selection Process
809    Figure 5 Map to Visualize Contact-tracing Applications around the World
810    Figure 6 Privacy Issues of Contact-tracing Applications
811    Figure 7. Classification of Privacy during the the COVID-19 Pandemic

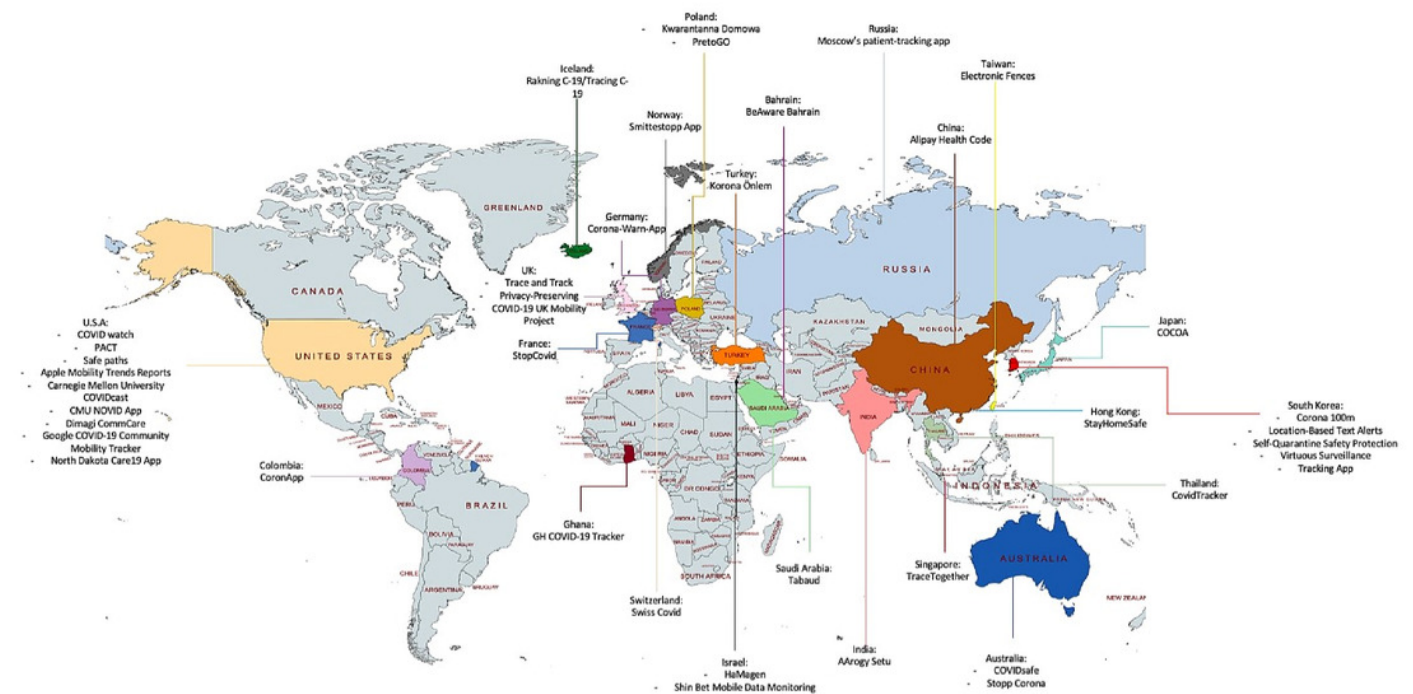
# Figure 1

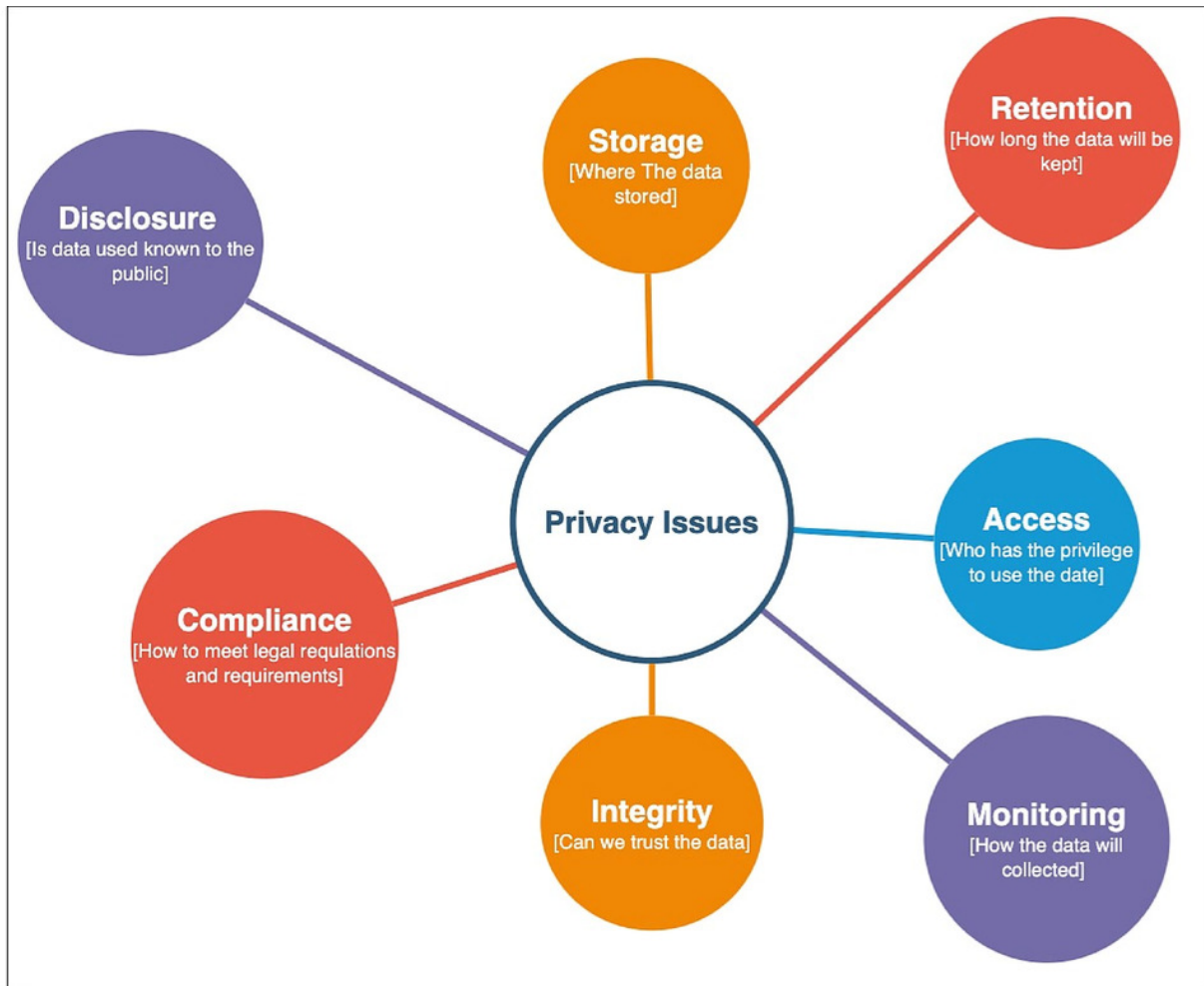
The Methodology's Main Stages

# Figure 2

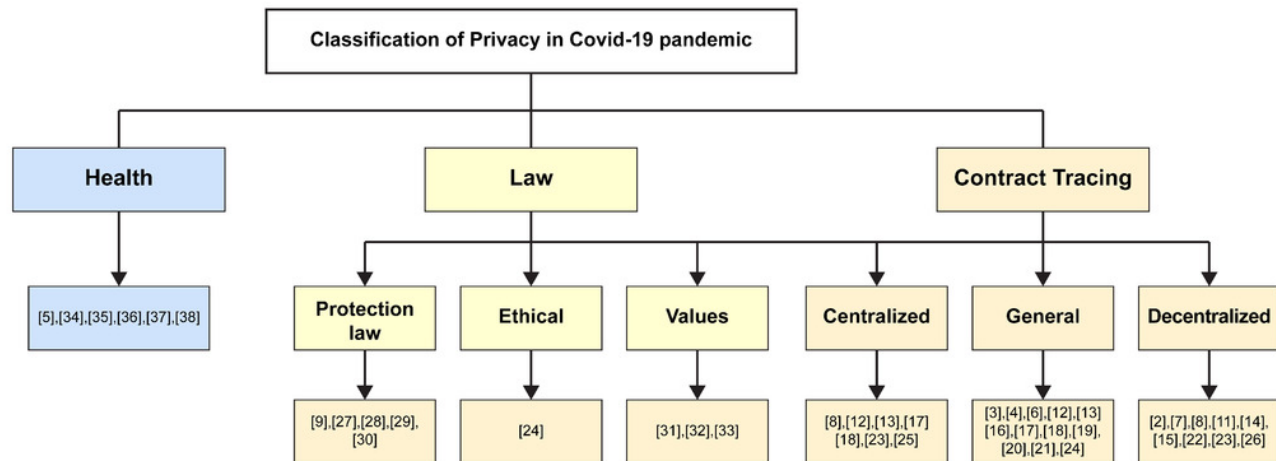
Quality Assessment Flow Chart

# Figure 3

Total Number of Papers from Each Data Source

# Figure 4

Paper Selection Process

# Figure 5

Map to Visualize Contact-tracing Applications around the World

# Figure 6

Privacy Issues of Contact-tracing Applications

# Figure 7

Classification of Privacy during the the COVID-19 Pandemic

Inclusion and Exclusion Criteria

1    Table 1. Inclusion and Exclusion Criteria

| Inclusion criteria | Exclusion criteria |
|---|---|
| English language | Non-English language |
| Between 2019 and 2020 | Before 2019 |
| Journals and magazines | Any document types other than journals and magazines |
| Use exact keyword strings | Papers that mention COVID-19 without privacy, and vice versa |

Quality Assessment Questions

1 Table 2. Quality Assessment Questions

| Q.ID | Quality Assessment Questions |
| --- | --- |
| **Q1** | Is the aim clearly stated? |
| **Q2** | Have any COVID-19 privacy issues been reported? |
| **Q3** | Has it answered its RQs? |
| **Q4** | What are the applied techniques related to COVID-19? |

Included and Excluded Papers

1    Table 3. Included and Excluded papers

| Data source | Search results | Candidate papers | Primary studies |
|---|---|---|---|
| Microsoft Academic | 142 | 4 | 3 |
| Wiley | 157 | 10 | 3 |
| IEEE | 18 | 8 | 6 |
| Sage Journals | 134 | 12 | 7 |
| Taylor & Francis | 113 | 6 | 3 |
| Springer Link | 14 | 3 | 2 |
| Science Direct | 97 | 6 | 6 |
| Scopus | 58 | 10 | 5 |
| ACM | 41 | 0 | 0 |
| Web of Science | **34** | **1** | **0** |
| Total | **808** | **60** | **35** |

Contact-tracing applications around the world along with their privacy concerns

1      Table 4. Contact-tracing applications around the world along with their privacy concerns

| Application Name | Country | Model | Technology | Privacy Concerns |
|---|---|---|---|---|
| AArogy Setu | India | Centralized | GPS+ Bluetooth [26] | This app is mandatory in India to reduce Covid-19 cases, app privacy policy has been deleted from apple and google stores and individual data is hashed and stored as an anonymous on government server |
| Apple Mobility Trends Reports | US | NA | NA | This app provides the policies in Apple that specifies data is encrypted, but there is no mention to the data deletion process. |
| BeAware Bahrain App | Bahrain | NA | GPS | The data is encrypted, and the users have the ability to request deleting their data. Also, it has access to users' phone numbers which raise privacy concerns. |
| Carnegie Mellon University COVIDcast | US | NA | NA | This app does not have clear policies provided with it, and once individual files the survey there is no deletion on data and data encrypted not specified. |
| CMU NOVID App | US | Decentralized | Bluetooth | This app provides NOVID policies that mention each user gets a random anonymous ID and notification token. It encrypts the individual ID, and individuals can request deletion of data and copy of data at any time, also data may be shared with other companies anonymously. |
| COCOA | Japan | NA | Bluetooth (Google/ Apple API) | This app faces privacy concerns upon the third-party API's used since it may reach the data, another concern is that this app does not provide control over data. |
| COVID-19 100m | South Korea | Centralized | GPS | Collects diagnose data, nationality, gender, age and locations. The individual locations only are tracked and stored to notify them if there was an infected individual visiting the same location. |
| *COVID-19-Warn-App* | Germany | Decentralized | Bluetooth (Google/ Apple API) | Personal data is not stored which make the individual trust the use of it, but it has two concerns the first one there is lack of data control from user, the second concern is using API as a third party raise the privacy concern of personal |

| | | | | information access from Google and Apple API's. |
|---|---|---|---|---|
| COVID-19pp | Colombia | NA | GPS | Collects users' location data. |
| COVID-19virus Impact Dashboard | Latin America | NA | NA | Regarding privacy, this app does not provide any privacy policies which raise privacy concerns, since it does not encrypt the data and it does not provide any information about data deletion. |
| COVID watch | U.S.A | Decentralized | Bluetooth | Used by volunteers from many different countries to exposure alerts when some infected users become near. Papers did not discuss its privacy violence clearly but for sure it has been mentioned as one of the applications that has privacy problems |
| COVID-19 UK Mobility Project | UK | Decentralized | NA | This app accesses the device ID and personal information, these data may be deleted by the user, but data encryption is not mentioned on the privacy policies provided. |
| COVIDsafe | Australia | Centralized | Bluetooth (BlueTrace protocol) | This app provides a level of privacy since it provides the user the freedom to delete the data anytime which will delete the entire application data from the phone, but these data are stored on the government server unencrypted and it will be deleted at the end of the pandemic. There is a privacy concern since the data on the government server is not encrypted which makes it open for the attackers to steal it. |
| CovidTracker | Thailand | Centralized | GPS | It collects Both infected and healthy users' information and sends it to a centralized server that is controlled by government and authority health. |
| Dimagi CommCare | U.S.A | NA | NA | This app does not provide data encryption, so it raises the privacy concern since it stores personal data on the server, but it allows the user to request deletion of the data. |
| Electronic Fences | Taiwan | Centralized | GPS | Collects the location and insurance card data and sends it to the Central Epidemic Command Center (CECC) to check their |

|  |  |  |  | last 14-days activity. |
| --- | --- | --- | --- | --- |
| GH COVID-19 Tracker | Ghana | NA | GPS | Collects users' location data. Papers did not discuss its privacy violence clearly but for sure it has been mentioned as one of the applications that has privacy problems |
| Google COVID-19 Community Mobility Tracker | U.S.A | Centralized | GPS | This app's privacy policy is controlled by Google, location data is stored locally by Google, and the encryption of data is done on the transit of data to the server. |
| HaMagen | Israel | Decentralized | GPS+Bluetooth | This app does not have privacy risk since it provides the policies to all the individuals, and it stores personal data on the individual device unless this individual is infected his/her data will be known. When the individual deletes the application, all of the data will be deleted. |
| Alipay Health Code | China | Centralized [26] | GPS [26] | This app is using individual QR codes, phone location, facial recognition, and drones to identify an individual's movement, this is threatening individual privacy. The Alipay app encrypts the storage, and it provides the chance to the individual to request personal data deletion. |
| Korona Önlem App | Turkey | NA | NA | The app requests access to contacts microphone, camera and calendar. Does not clearly if data is encrypted or not and if the users are able to request deleting their data. |
| Kwarantanna Domowa | Poland | NA | NA | The user is able to view the collected data about him following the EU's General Data Protection Regulation (GDPR) that appears unencrypted and the data will be stored for six years after the user deactivated his account. |
| Location-Based Text Alerts | South Korea | NA | GPS | Infected users' data are only collected. |
| Moscow's patient-tracking app | Russia | Centralized | GPS | Collects users' location data if the user provides access in Moscow. |

| | | | | |
|---|---|---|---|---|
| North Dakota Care19 App | U.S.A | Decentralized | GPS | This app gives the user a random ID and stores the location data only without personal data, the location will be tracked during the day, and the data deletion will be after 14 days. |
| PACT | U.S.A | Decentralized | Bluetooth | Only the Bluetooth tokens of infected users are sent to the authority and the authority will create and send to the infected user a permission number that will be announced publicly associated with all the contacts event numbers, then the public will be able to compare their contact event number with the announced number to know if they get affected. |
| Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) | EU | Decentralized | Bluetooth | Only the Bluetooth tokens of infected users are sent to the authority and the authority will create and send to the infected user a permission number that will be announced publicly associated with all the contact event numbers, then the public will be able to compare their contact event number with the announced number to know if they get affected. |
| PretoGO | Poland | Centralized | GPS based | Papers did not discuss its privacy violence clearly but for sure it has been mentioned as one of the applications that has privacy problems |
| Privacy-Preserving | UK | Centralized | Bluetooth | They clearly state their privacy policies and what the data will be stored, infected users' identity is anonymized after they agreed to transmit their data to the authority. Whereas the uninfected users' data will stay local. |
| Rakning C-19/Tracing C-19 | Iceland | Centralized | GPS | infected users' identity is anonymized after they agreed to transmit their data to the authority. Whereas the uninfected users' data will stay local. Both data are encrypted either locally stored or on the central server which will be deleted after 14 days. |
| Safe paths | U.S.A | Decentralized | GPS | The uninfected users' information will be locally stored but if they get infected their location will be encrypted and shared with SafePlaces web application, then healthy users will use PrivateKit |

| | | | | application to compare their personal location with the announced locations of the infected persons. The user has the ability to delete the local data but not the one that has been shared with SafePlaces. |
|---|---|---|---|---|
| Self-Quarantine Safety Protection | South korea | Centralized | GPS | The data are collected from many locations, CCTV, and credit card usage and sent to Korea Centers for Disease Control (KCDC) twice a day. Only the user's locations are reported immediately to KCDC to ensure that the user does not leave his quarantine, which causes high stress to the users. The infected users' data are deleted after two months and all users' data will be deleted after six months if they deactivate their accounts. |
| Shin Bet Mobile Data Monitoring | Israel | NA | GPS | The data is not encrypted, and it will be deleted after six months if they did not find the need to extend the time. |
| Smittestopp App | Norway | Centralized | GPS+ Bluetooth | The app collects users' phone number, location, age, mobile operating system and phone model. All these data will be deleted after 30 days. |
| StayHomeSafe | Hong Kong | Centralized | GPS | Collects users' location data by scanning their wristband's QR code to track the users if they left their home and force the passengers to do so. |
| StopCovid | France | Centralized | Bluetooth | This app was developed based on the TraceTogether model, the France government adopted Bluetooth technology rather than GPS to protect the privacy still Bluetooth technology is vulnerable to data breaches. Until now the anonymity level is preserved but it is expected to be sacrificed if the number of users increased. |
| Stopp COVID-19 | Australia | Centralized | Bluetooth technology | Send data to the government central server. |
| Swiss Covid | Switzerland | NA | Bluetooth (Google/Apple API) | This app faces privacy concerns upon the third-party API's used since it may reach the data], another concern is that this app does not provide control over data. |
| Tabaud | Saudi Arabia | NA | Bluetooth | They are conflict on using innovation or protect users' privacy. |

| | | | | |
|---|---|---|---|---|
| trace and track | UK | Centralized | Bluetooth | This app provides an anonymity level since the ID is anonymous and data is stored on the phone then after 14 days it will be uploaded to the cloud. |
| TraceTogether | Singapore | Centralized | Bluetooth (BlueTrace protocol) | It does not store any geolocation or personal data but requires phone numbers that are anonymous for the public but not anonymous for the government, which raises the concern about government privacy protection policies. First, there is a security risk since the data is not encrypted and it is vulnerable to malicious attacks. Second, there is an ethical risk for the infected people because if an individual passes by an infected person there will be an alert to notify the healthy person. However, data is stored locally on the individual's phone and after 21 days it will be deleted. |
| Tracking App | South Korea | Centralized | NA | Privacy issue since the government controls the data. |
| Virtuous Surveillance | South Korea | Centralized | GPS | This app several privacy concerns, as it publicly announces the infected user's information that include: last name, gender, credit card history and all recent location visits. |