FinJeHeW Finnish Journal of eHealth and eWelfare

SCIENTIFIC PAPERS

VERTAISARVIOITU
KOLLEGIALT GRANSKAD
PEER-REVIEWED
www.tsv.fi/tunnus

Features of COVID-19 applications and their impact on contact tracing: results of preliminary review

Riikka Vuokko[1], Kaija Saranto[2], Sari Palojoki[2]

[1] Sosiaali- ja terveysministeriö, Digitalisaation ja tiedonhallinnan yksikkö, Helsinki; [2] Sosiaali- ja terveydenhuollon tiedonhallinta, Sosiaali- ja terveysjohtamisen laitos, Itä-Suomen yliopisto, Kuopio

Riikka Vuokko, FT, Sosiaali- ja terveysministeriö, Digitalisaation ja tiedonhallinnan yksikkö, PL 33, FI-00023 Helsinki, FINLAND. Email: riikka.vuokko@gmail.com

Abstract

Digital technologies and telehealth, specifically contact tracing applications can complement traditional approaches for contact tracing of COVID-19 and overall COVID-19 control strategies. Despite the potential benefits of these novel approaches, concerns regarding privacy and basic rights have challenged application development and adoption. We explore the features of tracing applications, focusing on the trade-off between technical possibilities and privacy concerns. Our main objective is to map out central features of applied technology solutions that may prove as drivers or constrains for future development. Our secondary aim was to review how the effectiveness of tracing applications was being apprehended in research. We conducted a literature review of COVID-19 tracing applications and related privacy issues using the PubMed database. For analysis, we conceptualized contact tracing and data privacy. Our review identified various technologies with potential for contact tracing, with Bluetooth and GPS based solutions being the most common. Effectiveness of the applications is dependent on how widely these are adopted. However, technological approaches of the applications vary markedly, affecting their effectiveness for pandemic control. Privacy and trust are key limitations affecting application adoption. Existing privacy solutions are based on voluntary use, user consent, cryptographic data storage, minimum data collection, limited data usage, and transparency of the contact tracing applications and frameworks. Although evidence of applications' outcomes and benefits is yet tentative, the first evaluation frameworks for the applications are under development. In order to obtain maximum potential benefit from the applications, real-world evidence needs to be analyzed and evaluated carefully. However, along with contact tracing apps and comprehensive health programs, regulatory frameworks and safeguards are necessary to ensure that health information is not used for surveillance purposes and that app users' privacy is maintained.

Keywords: telehealth, COVID-19, contact tracing, privacy, review

Tiivistelmä

Digitaaliset teknologiat ja telelääketiede, erityisesti kontaktien jäljityssovellukset voivat täydentää vakiintuneempia lähestymistapoja Covid-19-kontaktien jäljittämisessä ja yleisesti Covid-19-pandemian hallinnan strategioissa. Tällaisten uusien lähestymistapojen mahdollisista hyödyistä huolimatta yksityisyyteen ja yksilön perusoikeuksiin liittyvät huolet ovat haastaneet sovellusten kehittämistä ja käyttöönottoa. Tarkastelemme jäljityssovellusten piirteitä keskittyen teknisiin mahdollisuuksiin ja tietosuojanäkökulmia koskeviin valintoihin. Päätavoitteemme on kartoittaa keskeisiä teknisten ratkaisujen piirteitä, jotka saattavat toimia jatkokehittämisen mahdollistajina tai esteinä. Toisena tavoitteenamme oli katsaus siitä, miten jäljityssovelluksia tarkastellaan tutkimuksessa. Toteutimme kirjallisuuskatsauksen Covid-19-jäljityssovelluksista ja niihin liittyvistä yksityisyyden suojaan liittyvistä kysymyksistä PubMed-tietokannasta. Analyysin keskeiset käsitteet olivat kontaktien jäljitys ja tietosuoja. Katsauksemme tunnisti eri teknologioita, jotka mahdollistavat kontaktien jäljittämistä. Näissä Bluetooth- ja GPS-pohjaiset ratkaisut olivat yleisimpiä. Vaikka sovellusten tehokkuus on riippuvaista niiden käyttöönoton laajuudesta, sovellusten tekniset lähestymistavat vaihtelivat suuresti, mikä vaikutti niiden tehokkuuteen pandemian hallinnoinnissa. Yksityisyyden suojaan ja luottamukseen liittyvät teemat ovat keskeisiä sovellusten käyttöönottoa rajoittavia tekijöitä. Nykyiset yksityisyyttä suojaavat mekanismit perustuvat vapaaehtoiseen käyttöön, suostumukseen, salaustekniikoihin datan säilyttämisessä, vähimmäisdatan keräämiseen, rajoitettuun datan käyttöön sekä jäljityssovellusten toimintaperiaatteiden läpinäkyvyyteen. Vaikka sovellusten vaikutuksista ja hyödyistä on vasta alustavia tuloksia, on kehitetty ensimmäisiä sovellusten arviointikehikkoja. Jotta sovelluksista saataisiin suurin potentiaalinen hyöty, niiden käytön vaikuttavuutta tulisi tutkia ja arvioida huolellisesti. Kontaktien jäljityssovellusten ja laaja-alaisten terveysohjelmien lisäksi säätelyn mallit ja suojakeinot ovat tarvittavia vakuuksia siitä, että terveystietoa ei käytetä valvonnan tarkoituksiin ja että sovellusten käyttäjän yksityisyyden suojaa ei vaaranneta.

Avainsanat: Telelääketiede, Covid-19, kontaktienjäljitys, yksityisyyden suoja, katsaus

Introduction

In February 2020, the World Health Organization (WHO) developed a global strategic preparedness and response plan in a situation where a total of 25,500 cases of COVID-19 disease (SARS-CoV-2) and nearly 500 deaths were confirmed globally [1-3]. Despite the wide range of measures implemented to mitigate the severe public health threat, by December 2020, more than 68.6 million cases including over 1.5 million deaths have been reported globally [4]. In just a few months, the current pandemic has exposed the need for more rapid response systems and new tools to fight the pandemic [5,6].

As an important part of national and international strategies to stop the spread of the virus, many countries are now developing various technology-based solutions that have a potential to be used in epidemic control and to revive social and economic life [7-9]. For health care, this has meant adopting various technologies for remote care and promoting personal applications for people coping with the pandemic [10]. Colucci et al. [11] remind that dramatic changes, for example in economic, political and social dimensions of society promote evaluation of new solutions like telehealth for care delivery and access to services. Telehealth is deemed suitable for use alongside conventional service delivery methods to allow more flexible care arrangements. During pandemics, telehealth can enable remote triage and diagnosis, support self-monitoring and provide accessible information for patients. Besides personal health maintenance, such solutions can be used to reduce the risk of exposure caused by close contacts. Aligned with telehealth solutions for care delivery, community level benefits and more automated solutions for labor-intensive manual contact tracing have been especially sought after. [10,11] Mobile technology has been envisioned as a potential solution for reporting of COVID-19 since the beginning of the pandemic. Although mobile COVID-19 applications (later apps) or other web-based services provide telehealth solutions for assessable information and innovative tools for self-diagnostics and monitoring [2,9,10], these apps are complementing comprehensive COVID-19 control strategies [2,3, 12,13] and, at the same time, may support individuals to be active participants in their health maintenance [15]. In a relatively short time, various types of applications utilizing different technologies have been developed [9-10].

As digital technology and telehealth can complement traditional approaches to health care [8,16,17], it is significant that the potential benefits of technology-based approaches for pandemic control are recognized and evaluated. Use of technology and implementation of telehealth approaches during pandemics is deemed necessary and justified for protecting public health [2,4,11]. For example, the European Commission has developed with European Union (EU) Member States a common coordinated approach for the use of mobile apps with the goal of cross border data exchange between the Member States launching the apps [12,14]. Mobile contact tracing was estimated to be faster, meaning fewer delays, better recall of errors and increased specificity and scalability [3,16,18]. However, concerns regarding data privacy and people's fundamental rights emerged as governmental authorities started to promote the use of these applications. Privacy issues are thus intertwined with the use of contact tracing apps. Successful use of the apps and the data gathered by them relies on public trust [10]. Due to the short development period, research evidence on the effectiveness of mobile technology interventions in pandemic control is yet scarce. Our research questions are: (1) What kinds of technologies are being applied in contact tracing apps? (2) How do privacy principles affect the development of the apps? (3) What are the implications of the chosen approaches for fulfilment of the functional and privacy-preserving expectations of the apps?

Materials and methods

Based on our research questions, we conceptualize the research area by defining COVID-19 tracing applications and data privacy. Contact tracing is a focal method for health authorities in managing the possible spreading and impact of contagious diseases. Contact tracing involves three basic steps: contact identification, contact alerting, and contact follow-up after a person's infection has been confirmed. With technological solutions, these steps can be speed up and a more detailed list of contacts can be recovered regardless of the infected person's acquaintance with close contact individuals [16,19,20]. Manual contact tracing is labor-intensive work involving regional or local health authorities tracing possible cases based on confirmed infections. In practice, this means that public health workers contact family, friends, coworkers and other known contacts of infected individuals [21]. After contacting possibly infected contacts, they receive region-appropriate guidance for self-isolation, quarantine, testing and treatment. In a pandemic such as COVID-19, contact tracing is typically part of a national strategy. At the national and international level the goal of harnessing advances in digital technology for contact tracing emerged early on, and the first smart phone-based contact tracing applications were implemented in March 2020 [22].

In accordance with international development, in the European context privacy preserving app development was seen as the way forward as individuals' rights to privacy and protection of personal data were seen as crucial for success. Acceptance of the apps by individuals was considered to depend not only on whether the public perceive them as effective and accurate, but also as privacy-protective and trustworthy [12,13]. In this paper, we refer to the concept of data privacy in the context of the European General Data Protection Regulation (GDPR) as a comprehensive approach to privacy although, at the same time, we acknowledge that not all countries have similar widespread principles on which to ground the development. However, fundamental rights and freedom and the protection of personal data are the guiding principles for the processing of persons' personal data [14].

We apply a method for our literature review that is consistent with the guidelines by Templier and Paré for information systems reviews [23]. Here, the review process consists of steps that formulate the research questions, search the literature, screen for inclusion, assess the quality of primary studies, extract data, and analyze the data. Our research team consisted of informatics and information technology experts. The research team concluded agreements through shared discussion and analysis on various steps of the research. Timely literature was searched from PubMed using MeSH (Medical Subject Headings) terms and terms describing the topic ('COVID-19', 'tracing', 'apps', 'privacy') as keywords. An initial search resulted in 32 references, while the inclusion criteria were peer reviewed research articles and language (English). In the first inclusion round, based on the article titles and abstracts, four articles were removed as out of scope, one for not being a peer reviewed research article, and one for language. During the full text reading of the articles, the quality of primary studies was evaluated by assessing, for example, the research design and methods used in the primary studies. A further seven articles were excluded for being out of scope in relation to the research questions of this study. Finally, 13 articles were selected for a further exploration (see Figure 1). As our topic relates to an emerging research area, our selection of original articles remained limited. Therefore, we performed a deductive analysis of the articles with a framework of contact tracing (types and approaches of apps), privacy and, in general, apps development (technologies named) resulting in a descriptive review of results. Narrative review primarily summarizes previously published research on a topic of interest by assembling a comprehensive report based on the current knowledge [23].

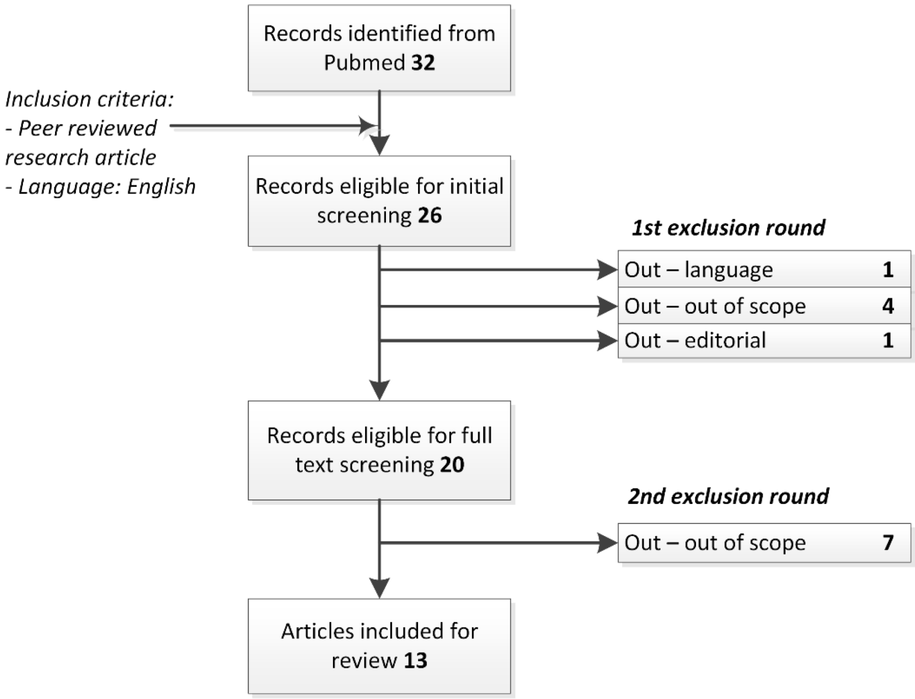

Figure 1. The inclusion and exclusion process.

Results

The 13 original articles were all published recently, between April and November 2020 and one of the included articles was an online pre-publication version of an article to be published in November 2020. The articles provide the first research evidence on the applications and their impact during the COVID-19 epidemic. Although the articles illustrate the first insights of the apps, part of them are descriptive reports of the ongoing development. Based on our assessment of the quality of the original articles, not all of them apply a theoretical framework or a methodology for data collection and analysis. For example, eight of the included original articles documented methods for data acquisition and measurement and nine presented outcome measures or evaluation criteria. A summary of the original articles is shown in Table 1.

Table 1. Summary of original articles.

Reference	Journal	Publication date (in 2020)	Research country	Technologies named	Application type; approach of solution	Approach to privacy
3	JMIR Mhealth Uhealth	Apr	UK, Germany	GPS/geolocation, Bluetooth, QR based solutions	Tracing applications; several approaches discussed	Handled generally
7	JMIR Journal of Medical Internet Research	Aug	Germany	Not specified	Several	Data privacy
8	JMIR Mhealth Uhealth	Aug	UK, Germany, USA, Denmark	Bluetooth	Tracing applications; centralized and decentralized approaches	Data privacy
9	Swiss Medical Weekly	May	Switzerland	Not specified	Several application types and approaches discussed	Data privacy
16	Global Health Research and Policy	Aug	Germany	GPS, Bluetooth	Tracing applications	Handled generally
17	JMIR Public Health and Surveillance	Sep	Belgium	Not specified	Tracing applications	Data privacy
18	Canadian Medical Association Journal	Jun	Canada	GPS, Bluetooth, barcode or QR based solutions	Tracing applications; centralized and decentralized approaches	Data privacy
19	JMIR Mhealth and Uhealth	Jun	China	GPS, geospatial artificial intelligence, social media	Tracing applications	Handled generally
20	IEEE Journal of Biomedical and Health Informatics	Sep	Australia	Bluetooth	Tracing applications; decentralized approach	Data privacy
22	Computer Science Review	Nov (Sep)	India	GPS, Bluetooth	Tracing applications; centralized and decentralized approaches	Data privacy
24	International Journal of Information Management	Jul	Japan	GPS, Bluetooth	Tracing applications; centralized and decentralized approaches	Data privacy
25	Diabetes and Metabolic Syndrome: Clinical Research and Reviews	Aug	Kingdom of Eswatini	Several	Tracing applications	Data privacy
26	JMIR Public Health and Surveillance	Aug	USA	Not specified/other	Web-based tracing application	Data privacy

Our review identified various technologies for contact tracing. According to our review, Bluetooth (Bluetooth Low Energy, BLE) technology and GPS (Global Positioning System) based solutions are most commonly cited [3,8,16,18,20,22,24,25]. Other technologies named include, but are not limited to, social media or other web-based solutions, geospatial artificial intelligence systems, and barcode or Quick Response (QR) code based solutions where codes are scanned by phones or placed in public spaces, such as bus doors and store entrances, allowing users to log visited locations. A related strategy is Wi-Fi fingerprinting, using the received signal strength from each Wi-Fi network to create a 'fingerprint' of each location [18,19,24]. Additionally, emerging technologies such as utilization of big data and the Internet of Things, artificial intelligence in general and blockchain were mentioned [25]. Noteworthy is that the apps may vary considerably in their technological approaches [7], affecting their potential effectiveness for pandemic control or support for individuals.

Our review revealed some well-documented limitations regarding technological premises. These limitations may affect the acceptance and usability of the apps. With BLE technology, signal strength is used to infer the distance between smartphones and define exposure status based on distance from and duration of proximity to an individual identified as infected. Location-based approaches use, e.g., cell phone network data or GPS to identify the locations of app users, and this information is used to determine the proximity to infected individuals [18]. The effectiveness of contact tracing is dependent on how widely the proposed digital solution is adopted, especially when dependent on smartphone ownership. Additionally, there is increasing risk of digital exclusion if guidance is accessible through apps [8,18,20,22,26]. The available technologies can cause sensitivity issues in calculating contact and risk, e.g. based on signal strength between devices, which may limit identifying contacts. Consequently, the apps have limitations dealing with asymptomatic individuals that may cause varied instructions for the app users and thus cause further confusion [3,18,22,25]. Overall, there is no evidence to date that mobile contact tracing reduces transmission of the virus or that the apps are effective [18]. The apps may increase battery drain and thus cause breaks in scanning for contacts. Lack of supporting information and communication technology (ICT) infrastructure is evident when the apps require Internet connection to function [3,18,20,25].

Regarding data privacy, our review captured the discussion between voluntary vs. involuntary approaches and between data driven vs. privacy driven approaches, although there was less research on involuntary approaches. Of the 13 articles, 9 documented voluntary approaches, 1 illustrated additional involuntary examples, and 3 did not consider this approach. Involuntary systems, as adopted in some countries such as South Korea and China, use e.g. security camera footage and cell phone location data [18]. However, lack of consent in such systems and risks to privacy make them less likely to be accepted in countries where ensuring privacy is crucial for acceptance of the apps [18,26]. Voluntary approaches incorporate features to mitigate privacy concerns and ensure compliance with privacy principles in accordance with the EU's General Data Protection Regulation. This includes encryption of personal data, user consent for data storage and use, restrictions on use of the data outside the public health responses to COVID-19, automatic deletion of data, and the option to delete data at any time [18]. Minimal data seems to be crucial to protecting fundamental rights, since contact tracing is possible without extensive data collection in a central database [3, 20]. In addition to allowing users control over their data usage, ensuring transparency by providing open source codes and clean data flow are ways to increase public trust in digital contact tracing [20].

However, public discussions indicate that COVID-19 apps may pose risks for data privacy. The digital and sensitive data emphasizes the importance of safeguarding citizen´s privacy [3]. Invasive monitoring, such as mobile contact tracing, causes privacy concerns beyond those of manual contact tracing. There is evidence of how voluntary or involuntary contact tracing affects adoption of the apps. This is related to the approach chosen for the app and the scope of the data stored, especially when the data covers all movements of an individual. In centralized approaches data is stored for use by health authorities, whereas in decentralized approaches data calculation takes place in the personal app. The latter approach often implements principles for data minimization. However, in some instances apps may cause privacy and security risks or discrimination [8,9,18,25]. One reviewed article expressed a need for international humanitarian laws to be amended to govern responsible state behaviors concerning personal information available in digital infrastructures. Then international laws may oblige states to enact protective measures to prevent e.g., cyberattacks on digital infrastructure [16].

The effectiveness of tracing apps depends on a number of factors, such as the percentage of the population using a smart device and the percentage of users downloading the app and consenting to the processing of personal data [9]. However, our review found less research evidence regarding the outcomes and benefits of mobile contact tracing solutions, although evidence regarding app acceptability and adoption was studied. Possible benefits of mobile contact tracing include individual autonomy through voluntary use allowing persons to indicate or refuse consent to participate, reduced need for continuous self-reporting, circumvention of recall bias from infected persons, reduced risk of human error, and avoidance of the potential stigmatization of face-to-face interviews in manual contact tracing [16]. In a study concerning the motivation for app use [7], factors that affected motivation were the specific app type, trust in contact tracing, transparency of data collecting by official app providers, and perceived data privacy. Simply put, people are more motivated to use a more personally useful app, and general trust in official app providers was the most important independent variable with respect to app use motivation [7]. In app adoption research, the main factors influencing app use were the perceived benefits of the app, self-efficacy, and perceived barriers. In the reviewed research, coping was more consistently associated with health-related intentions and behaviors, whereas individuals' belief in the gravity of the pandemic and their personal vulnerability did not predict intention for app uptake. A significant barrier was data privacy, for which no use of location data and data minimization were deemed as effective solutions [17]. A European study noted that the main barriers to app adoption are concerns about cybersecurity and privacy, together with a lack of trust in the government. In app design, addressing privacy and cybersecurity concerns thus require respecting the use of personal data and considering when de-identified data could be used [8].

A common assumption is that the effectiveness of contact tracing apps in identifying exposures depends on widespread use of individual apps and the ability of their underlying technologies to identify nearby phones [17,18]. Trust in official app providers has a role in individuals' motivation for using an app. This is likely to affect the benefits of the app [7]. Additional factors include, for example, lack of supporting information and ICT infrastructure, socio-economic inequalities, interoperability and standardization issues, political and other social dimensions, such as ethical and legal risks or discrimination and the digital divide [8,25].

To systematically assess the apps, the first evaluation frameworks have been published. These tools support the trustworthiness of digital health efforts [3, 9]. For example, Fahey and Hino [24] note recent cases of illicit use of digital information. These incidents have heightened public consciousness of the risks related to centralized data repositories and to data privacy as a right. Vokinger et al. [9] propose a framework that covers domains on the purpose, usability, information accuracy, organizational attributes or reputation, transparency, privacy and user control or self-determination of apps. The purpose of this evaluative framework is to guide individuals in choosing safe and valuable apps. Dar et al. [22] developed a framework for evaluating the applicability of contact tracing apps that includes the following characteristics: nature of app approach (centralized or decentralized), technique employed (Bluetooth or GPS) privacy, techniques of identifying attackers besides indicators of an attack, and scalability. Other factors are also suggested, such as transparency or legal and ethical aspects [22].

Discussion

In this review, we identified factors affecting the development and use of contact tracing apps. The technological characteristics of the apps vary, with some clear implications. In the review, Bluetooth technology was most commonly used. Location data could increase users' mistrust of tracing apps but, at the same time, the limitations of Bluetooth technology are known. Of the design approaches, distributed apps may increase the work burden of health authorities or cause unnecessary alarm and, thus, mental health risks for citizens [3,8,9,17,18,22]. Centralized apps are more closely linked with authorities and users are more likely to be required to hand over their personal data. Decentralized apps implement data minimization principles and require no user registration as core functions are built into the app. Additionally, decentralized apps are backed up by Apple and Google protocols that prohibit use of location data [20,24].

Privacy protection establishes a trust basis for the use of apps, but another key starting point is their effectiveness [3,8,9,18,20,22,26]. The challenge, therefore, is how to save lives while at the same time protecting personal privacy. Weakened data privacy might be preferable to the restrictions and economic cost of lockdown [3]. It is evident that apps will not be accepted without trust and, in most cases, apps are being developed with regard to data privacy and basic rights [8,9,18,25]. To summarize, existing privacy solutions are based on voluntary use, user control and consent, cryptographic data storage, minimum data collection, limited data usage, and transparency of the contact tracing apps and frameworks [20,24,26]. However, a cause for concern is that there is little evidence of how effective these apps will be for contact tracing or in relation to privacy concerns, if widely used, at stopping the spread of the disease. Their benefits for contact tracing are frequently highlighted, yet continued discussion of their risks to privacy is also essential [9,22,24]. Beyond its use for mitigating and containing COVID-19, digital technology can complement or in some cases enhance traditional approaches to global health program implementation [16].

For epidemiologists, the mass data harvested from these digital platforms presents a repository of evidence that is beneficial in informing preparative steps for future pandemics. However, extra measures, such as privacy protection, are warranted to avoid harmful use of data that could overshadow the benefits [16]. Additional concerns are that the apps can cause false positives, e.g., in case of symptoms increasing the burden on the health authorities, or cause false negatives, which cannot be verified clinically because the app does not transmit necessary contact information of the infected person. The apps could also cause stigmatization of persons with certain characteristics because of a perceived link with the disease. Moreover, incorrect information could cause unnecessary alarm when alerting a wide range of contacts and wrongly send people into quarantine [9].

It seems that despite the potential benefits of digital contact tracing, health authorities need to evaluate and consider the documented technical limitations and possible imbalance between privacy and effective contact tracing. Successful digital contact tracing is dependent on public trust and adoption of solutions, access to testing, and related guidance of care [7,11,18]. Based on the review, there seem to be slightly different approaches when designing for individual users to adopt a personal app or when designing for health authorities and health care teams [20,26]. A recent study has developed a framework providing guidance on evaluating an app's trustworthiness, epidemiological rationale, and legal robustness [9]. The framework has potential to guide necessary safeguards and to steer individuals towards assessing the data privacy of tracing apps.

The main limitations of our review relate to the relative short timeframe of the original research. Due to the ongoing situation, preliminary reporting is descriptive and may be based on selective or biased data in a situation where no universal frameworks, even common terminology, or a classification for evaluation purposes are available [10,11]. The use or development of an appropriate analysis framework or methodology for data collection and analysis is essential for ensuring the reliability and validity of research, and this deserves attention when documenting seminal research. An additional limitation of our review is the yet scarce evidence of mobile contact tracing outcomes.

Concerning recommendations for further research, our review suggests that further exploration of the topic is needed. It is an opportune time to examine the effectiveness of apps as tracing tools and their impact on privacy and fundamental rights. Studies on user experiences are also needed to illustrate the impact apps may have in daily lives and on personal health empowerment.

We conclude that even though there are several different types of technologies, in order to gain most of the potential benefits of COVID-19 apps and mobile solutions either for personal health maintenance or for contact tracing, real-world evidence needs to be analyzed and evaluated more to gain insight for further development. Regarding efficiency in regards to the primary goal of contact tracing, based on the review the effectiveness is dependent on several interlinked features, and technology is just one dimension. However, more evidence is needed. Telehealth or, specifically, mobile applications are urgently needed to complement conventional epidemiological methods due to their potential to improve control of the spread of the virus within a community, and to support individuals in coping with the pandemic and personal health maintenance. To foster individuals' trust to these apps, privacy principles are of paramount importance. Thus, along with contact tracing apps and comprehensive health programs, regulatory frameworks and safeguards are necessary to ensure that health information is not used for surveillance purposes and that app users' privacy is maintained.

Acknowledgments

The authors want to thank University of Eastern Finland for support in language review.

Conflict of interest

The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

References

[1] World Health Organization WHO. Novel Coronavirus (2019-nCoV) Situation Report 16. Data as reported by 5 February 2020. Available from: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200205-sitrep-16-ncov.pdf?sfvrsn=23af287f_2

[2] Ferretti L, Wymant C, Kendall M, Zhao L, Nurtay A, Abeler-Dörner L, Parker M, Bonsall D, Fraser C. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science. 2020 May 8;368(6491):eabb6936. https://doi.org/10.1126/science.abb6936

[3] Abeler J, Bäcker M, Buermeyer U, Zillessen H. COVID-19 Contact Tracing and Data Protection Can Go Together. JMIR Mhealth Uhealth. 2020 Apr 20;8(4):e19359. https://doi.org/10.2196/19359

[4] ECDC. COVID-19 situation update worldwide, as of 11 December 2020. European Centre for Disease Prevention and Control (ECDC); 2020 [cited 11.12.2020]. Available from: https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

[5] Rozanova L, Temerev A, Flahault A. Comparing the Scope and Efficacy of COVID-19 Response Strategies in 16 Countries: An Overview. Int J Environ Res Public Health. 2020 Dec 16;17(24):9421. https://doi.org/10.3390/ijerph17249421

[6] Fernández L, Cima-Cabal MD, Duarte AC, Rodriguez A, García P, García-Suárez MDM. Developing Diagnostic and Therapeutic Approaches to Bacterial Infections for a New Era: Implications of Globalization. Antibiotics (Basel). 2020 Dec 16;9(12):916. https://doi.org/10.3390/antibiotics9120916

[7] Kaspar K. Motivations for Social Distancing and App Use as Complementary Measures to Combat the COVID-19 Pandemic: Quantitative Survey Study. J Med Internet Res. 2020 Aug 27;22(8):e21613. https://doi.org/10.2196/21613

[8] Altmann S, Milsom L, Zillessen H, Blasone R, Gerdon F, Bach R, Kreuter F, Nosenzo D, Toussaert S, Abeler J. Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study. JMIR Mhealth Uhealth. 2020 Aug 28;8(8):e19857. https://doi.org/10.2196/19857

[9] Vokinger KN, Nittas V, Witt CM, Fabrikant SI, von Wyl V. Digital health and the COVID-19 epidemic: an assessment framework for apps from an epidemiological and legal perspective. Swiss Med Wkly. 2020 May 17;150:w20282. https://doi.org/10.4414/smw.2020.20282

[10] Vuokko R, Saranto K, Palojoki S. Typology-Based Analysis of Covid-19 Mobile Applications:

Implications for Patient Empowerment. Stud Health Technol Inform. 2020 Nov 23;275:212-216. https://doi.org/10.3233/SHTI200725

[11] Colucci M, Baldo V, Baldovin T, Bertoncello C. A "matter of communication": A new classification to compare and evaluate telehealth and telemedicine interventions and understand their effectiveness as a communication process. Health Informatics J. 2019 Jun;25(2):446-460. https://doi.org/10.1177/1460458217747109

[12] European Commission. Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States. Version 1.0, 15.04.2020. Available from: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

[13] European Commission. eHealth Network Guidelines to the EU Member States and the European Commission on Interoperability specifications for cross-border transmission chains between approved apps. Basic interoperability elements between COVID+ Keys driven solutions. V 1.0, 12.6.2020. Available from: https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interoperabilityspecs_en.pdf

[14] EUR-Lex. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing. Directive 95/46/EC (General Data Protection Regulation). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[15] Spanakis EG, Santana S, Tsiknakis M, Marias K, Sakkalis V, Teixeira A, Janssen JH, de Jong H, Tziraki C. Technology-Based Innovations to Foster Personalized Healthy Lifestyles and Well-Being: A Targeted Review. J Med Internet Res. 2016 Jun 24;18(6):e128. https://doi.org/10.2196/jmir.4863

[16] Owusu PN. Digital technology applications for contact tracing: the new promise for COVID-19 and beyond? Glob Health Res Policy. 2020 Aug 3;5:36. https://doi.org/10.1186/s41256-020-00164-1

[17] Walrave M, Waeterloos C, Ponnet K. Adoption of a Contact Tracing App for Containing COVID-19: A Health Belief Model Approach. JMIR Public Health Surveill. 2020 Sep 1;6(3):e20572. https://doi.org/10.2196/20572

[18] Kleinman RA, Merkel C. Digital contact tracing for COVID-19. CMAJ. 2020;192(24):E653-E656. https://doi.org/10.1503/cmaj.200922

[19] Wang S, Ding S, Xiong L. A New System for Surveillance and Digital Contact Tracing for COVID-19: Spatiotemporal Reporting Over Network and GPS. JMIR Mhealth Uhealth. 2020 Jun 10;8(6):e19457. https://doi.org/10.2196/19457

[20] Whaiduzzaman M, Hossain MR, Shovon AR, Roy S, Laszka A, Buyya R, Barros A. A Privacy-Preserving Mobile and Fog Computing Framework to Trace and Prevent COVID-19 Community Transmission. IEEE J Biomed Health Inform. 2020;24(12):3564-3575. https://doi.org/10.1109/JBHI.2020.3026060

[21] Keeling MJ, Hollingsworth TD, Read JM. Efficacy of contact tracing for the containment of the 2019 novel coronavirus (COVID-19). J Epidemiol Community Health. 2020 Oct;74(10):861-866. https://doi.org/10.1136/jech-2020-214051

[22] Dar AB, Lone AH, Zahoor S, Khan AA, Naaz R. Applicability of mobile contact tracing in fighting pandemic (COVID-19): Issues, challenges and solutions. Comput Sci Rev. 2020 Nov;38:100307. https://doi.org/10.1016/j.cosrev.2020.100307

[23] Templier M, Pare GA. Framework for Guiding and Evaluation Literature Reviews. Communications of the Association for Information Systems. 2015;37(6):112-137. https://doi.org/10.17705/1CAIS.03706

[24] Fahey RA, Hino A. COVID-19, digital privacy, and the social limits on data-focused public health responses. Int J Inf Manage. 2020 Dec;55:102181. https://doi.org/10.1016/j.ijinfomgt.2020.102181

[25] Mbunge E. Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls. Diabetes Metab Syndr. Nov-Dec 2020;14(6):1631-1636. https://doi.org/10.1016/j.dsx.2020.08.029

[26] Kassaye SG, Spence AB, Lau E, Bridgeland DM, Cederholm J, Dimolitsas S, Smart JC. Rapid Deployment of a Free, Privacy-Assured COVID-19 Symptom Tracker for Public Safety During Reopening: System Development and Feasibility Study. JMIR Public Health Surveill. 2020 Aug 13;6(3):e19399. https://doi.org/10.2196/19399