Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Delineating privacy aspects of COVID tracing applications embedded with proximity measurement technologies & digital technologies

Tahereh Saheb a,*, Elham Sabour b, Fatimah Qanbary b, Tayebeh Saheb c

a Tarbiat Modares University, Management Studies Center, Tarbiat Modares University, Jalal Al Ahmad, Tehran, Iran
b Tarbiat Modares University, Information Technology Management - Business Intelligence, Iran
c Tarbiat Modares University, Faculty of Law, Iran

ARTICLE INFO

Keywords:
Privacy
Ethics
Covid
Tracing apps
Surveillance
Proximity measurement

ABSTRACT

As the COVID-19 pandemic expanded over the globe, governments implemented a series of technological measures to prevent the disease’s spread. The development of the COVID Tracing Application (CTA) was one of these measures. In this study, we employed bibliometric and topic-based content analysis to determine the most significant entities and research topics. Additionally, we identified significant privacy concerns posed by CTAs, which gather, store, and analyze data in partnership with large technology corporations using proximity measurement technologies, artificial intelligence, and blockchain. We examined a series of key privacy threats identified in our study. These privacy risks include anti-democratic and discriminatory behaviors, politicization of care, derogation of human rights, techno governance, citizen distrust and refusal to adopt, citizen surveillance, and mandatory legislation of the apps’ installation. Finally, sixteen research gaps were identified. Then, based on the identified theoretical gaps, we recommended fourteen prospective study strands. Theoretically, this study contributes to the growing body of knowledge about the privacy of mobile health applications that are embedded with cutting-edge technologies and are employed during global pandemics.

1. Introduction

Throughout history, the use of innovative technical methods has prevented public health disasters. Historically, contact tracing was one of the most promising methods; it was initially handled manually through interviews with infected individuals, followed by phone calls to identified individuals’ connections to inform them of the condition [1]. Nonetheless, a number of challenges, including labor-intensive procedures, long response times, and the need for human intelligence, have fueled the development of digital solutions [2]. Furthermore, manual procedures were insufficient in situations where people were in close proximity to strangers. The popularity of mobile phones, combined with their ability to track short-range communication and the connections of their owners, facilitated the development of algorithms for immediate contact tracing in conjunction with digital proxies. Historically, digital proximity measurement tools, such as Bluetooth, Radio Frequency Identification Device (RFID), 5G, and Internet of Things, have been widely used in infectious disease surveillance [3].

COVID-19 was the most recent pandemic that afflicted billions of people worldwide. The disease has been widely dubbed the greatest threat to humanity since World War II and the worst global health disaster of the century. COVID-19’s increasing prevalence endangers public health, the economy, the environment, and society. The COVID-19 outbreak prompted some governments to build mobile-based proximity measurement applications to alert people in proximity to the infected population and to identify the infected population [4-6].

Prior research has revealed that, if widely adopted by citizens, CTA could be effective in combating the spread of COVID-19 [7]. Previous research concludes that the adoption of CTAs may be hampered by ethical concerns [8,9] and new forms of surveillance and monitoring by governments and corporations collaborating with governments [10,11]. According to prior findings, automatic contact tracing systems exacerbate privacy vulnerabilities by collecting sensitive personal data [12,13] and creating persistent and vulnerable records of individuals’ health, movements, and social contacts [14]. Previously, the definition of privacy has been called into question following scandals involving major technology companies, such as the Apple location tracking scandal [15]. There is mounting evidence that digital contact tracing was insufficient
in the aftermath of the epidemic, emphasizing its short-term nature as a technical solution [16]. Simultaneously, there are questions about whether these data will be shared with other government agencies or technology firms for commercial or national surveillance purposes. As a result, experts like [13] advocate addressing a number of privacy-related concerns in order to determine whether a contact-tracing application is ethically justified.

CTAs have been a popular scholarly topic, and a number of studies have been carried out to conduct systematic literature reviews or bibliometric analyses of scientific endeavors examining CTAs. In these studies, the CTA has been reviewed in broad strokes. Prior research is also carried out, either through bibliometric analysis or qualitative systematic reviews of the literature. We distinguished ourselves from previous bibliometric or review studies of CTAs such as [6,17,18] by focusing solely on the privacy aspect of CTAs in order to elucidate the historical scientific research on the privacy aspect of CTAs. In addition, to supplement the findings from both methodologies, we combined bibliometric and topic-based content analysis. We evaluated papers quantitatively utilizing co-citation analysis and keyword co-occurrence analysis, two commonly used bibliometric analysis techniques, and qualitatively using the topic-based content analysis methodology. Using bibliometric analysis, we identified a set of scholarly topics and then conducted content analysis on the most relevant documents for each topic. The bibliometric methodology entails the examination of a subject’s corpus of literature as well as the evaluation of highly cited publications, nations, institutions, and sources [19]. As a result, our work addresses the following issues:

1. Which documents, sources, and authors have received the most citations in research on the privacy implications of CTAs?
2. What are the most common research topics concerning CTA privacy?
3. What are the most concerning privacy consequences of CTAs?
4. What gaps in the literature exist, and what are the future research agendas?

This study may help health practitioners, governments, developers, and researchers focus on the most serious privacy concerns associated with mobile applications designed to manage global pandemics using proximity measurement technologies. In practice, the goal of this paper is to expose privacy vulnerabilities so that monitoring technologies can be developed in accordance with privacy-preserving principles and public authorities can enact appropriate privacy protection regulations to prevent any potential breach. Theoretically, this paper will add to the existing literature on digital health ethics, specifically the privacy of digital mobile health applications and proximity-measuring technologies in the event of a worldwide pandemic.

The paper is structured as follows: We commence by delving into the study’s research methods. The next part discusses the findings, beginning with a descriptive analysis of the documents evaluated in this study. The remainder of this paper is organized around the research questions posed by our study. We start by explaining the results of our co-citation study, followed by a keyword co-occurrence analysis that identified nine scientific topics. We delved deeply into each topic by conducting a topic-based content analysis. The combination of co-occurrence analysis and content analysis enabled us to identify the most stressing privacy repercussions of CTAs, which is described in the following section. We conclude the paper with an analysis and conclusion section in which we examine the study’s findings, limitations, and prospective future research directions.

2. Research methodology

On July 30, 2021, we collected data from the Scopus database. We set no time constraints. We searched for the terms “COVID-19” OR “corona” OR “pandemic” AND “contact tracing” AND “privacy” in the title, abstract, and keyword sections. We added the broad keyword “contact tracing” to emphasize the primary functionality of mobile applications that incorporate proximity measurement, artificial intelligence, and other digital technologies. CTAs are known by a variety of names, including “contact surveillance applications” [20], “COVID-19 App” [21] or “digital proximity tracing app” [22]. Since the COVID-19 pandemic started in November 2019, we chose 2020–2021 as the timeframe. We imposed no restrictions other than the language, which was limited to English-language papers. Because CTA privacy is an interdisciplinary scientific subject, we considered all fields in our research. Furthermore, we covered all types of publications. The search yielded 339 results. The titles and abstracts of the publications were screened for relevance and duplication. Any article that did not specifically target CTAs was removed. These findings were independently verified by three researchers. The co-authors repeated this procedure three times. The Kappa value was 0.872, indicating a high level of coding reliability. The Kappa value, which ranges from 1 to 0, indicates the degree of agreement among the authors who coded the papers. A value of one indicates that the document should be included, while a value of zero indicates that it should be excluded. Finally, ten papers were dropped. We randomly selected 11 more papers with the highest relevance to the topic for content analysis.

We conducted descriptive, bibliometric, and content-based analyses in this study. We performed a co-citation analysis of documents to address the study’s first inquiry. We utilized keyword co-occurrence analysis and qualitative content analysis of topics to discuss the remaining questions. Co-citation analysis, as one of the most commonly used methods of bibliometric analysis, attempts to answer the following question: which institutions, authors, and documents are most frequently cited in a specific body of literature [23]? Keyword co-occurrence analysis also intends to identify the most common keywords, and thus the most popular research topics pursued by researchers [24,25]. To supplement the findings of the co-occurrence analysis, a method known as topic-based content analysis was used to examine the contents of documents that were most relevant to each topic [26]. We incorporated the VOSviewer software and the Biblioshiny R software library. We visualized social networks by calculating their Total Link Strength (TLS), which takes into account both the number of connections an object has with other objects and the strength of those connections [27]. To classify components such as keywords based on the strength of their associations, the Association Strength normalization technique was used. The Association Strength metric is the best option for normalizing co-occurrence data [28]. We supplemented our quantitative research with a qualitative content analysis of the publications that contained the most relevant information about each topic [29]. This mixed-methods study improved our quantitative analysis, allowing us to conduct gap analysis and identify future research areas more efficiently.

3. Results

The results section is divided into two sections. The first section is a descriptive study of articles relevant to the privacy of CTAs. We next outline co-citation analysis in order to address the study’s first inquiry, followed by co-occurrence and content analysis of topics to address the study’s remaining inquiries.

3.1. Descriptive analysis of documents

We have provided a descriptive analysis of the publications analyzed in this section of the paper. Between 2020 and 2021, the annual growth rate of scientific production climbed by 60.69%: 126 papers were published in 2020, and this number expanded to 203 papers in 2021. As shown in Table 1, the majority of papers are in the fields of medicine, computer science, social sciences, and engineering. Additionally, the publications are predominantly affiliated with the University of Melbourne, King’s College London, and the University of Oxford. The majority of papers are also published as articles. The European Union’s
Table 1
Descriptive analysis of documents.

| Entity                                | Percentage | Entity                                | Percentage |
|----------------------------------------|------------|----------------------------------------|------------|
| Subject Area                          |            | Affiliation                            |            |
| Medicine                              | 40.8       | University of Melbourne               | 3.3        |
| Computer Science                      | 34.7       | King’s College London                  | 2.4        |
| Social Sciences                       | 27.5       | University of Oxford                  | 2.4        |
| Engineering                           | 15         | Imperial College London                | 2          |
| Arts and Humanities                   | 6.3        | University of Toronto                  | 2          |
| Multidisciplinary                     | 6.3        | University College London              | 2          |
| Business, Management and Accounting   | 6          | Seoul National University              | 1.8        |
| Decision Sciences                     | 6          | University of Oxford Medical Sciences Division | 1.5 |
| Biochemistry, Genetics and Molecular Biology | 4.5       | Universität Zürich                    | 1.5        |
| Health Professions                    | 4.5        | University of Bristol                  | 1.5        |
| Materials Science                     | 4.2        | ETH Zürich                            | 1.5        |
| Nursing                               | 3.3        | Universität Gent                      | 1.5        |
| Mathematics                           | 2.7        | The Royal Institute of Technology KTH | 1.2        |
| Psychology                            | 2.7        | Universität McGill                     | 1.2        |
| Environmental Science                 | 2.4        | University of Pennsylvania            | 1.2        |
| Physics and Astronomy                  | 2.4        | Universitet i Oslo                     | 1.2        |
| Chemistry                             | 1.5        | Università degli Studi di Torino      | 1.2        |
| Funding sponsor                       |            |                                        |            |
| Horizon 2020 Framework Programme      | 3.6        | Stanford University                   | 1.2        |
| National Research Foundation of Korea | 2          | King Saud University                   | 1.2        |
| National Institutes of Health         | 1.8        | Radboud Universiteit                  | 1.2        |
| National Science Foundation          | 1.8        | Massachusetts Institute of Technology | 1.2        |
| European Research Council             | 1.5        | London School of Hygiene & Tropical Medicine | 1.2 |
| Horizon 2020                          | 1.5        | Interuniversity Micro-Electronics Center at Leuven | 1.2 |
| Norges Forskningsråd                  | 1.5        | European Commission Joint Research Centre | 1.2 |

| Entity                                | Description                      | Results | Entity                                | Description                      | Results |
|----------------------------------------|----------------------------------|---------|----------------------------------------|----------------------------------|---------|
| Main Information about data            | Timespan                         | 2020:2021 | Document Content                      | Keywords Plus (ID)                | 1357    |
| Sources (Journals, Books, etc.)        | 202                              | Documents | Author’s Keywords (DE)                | 773                              |
| Documents                              | 329                              | Average years from publication        | Authors                            | 1295                             |
| Average years from publication         | 1.38                             | Average citations per documents       | Authors of single-authored documents | 43      |
| Average citations per documents        | 11.42                            | Average citations per year per doc    | Authors of multi-authored documents | 1252                             |
| Average citations per year per doc     | 4.198                            | References                             | Article                            | 247                              |
| Authors                                | Single-authored documents        | 44                                | Document Type                      | Editorial                         | 2       |
| Authors per Author                     | 0.256                            | Documents per Author                  | Letter                             | 7                                 |
| Authors per Document                   | 3.91                             | Authors per Document                  | Note                               | 18                                |
| Co-Authors per Documents               | 4.45                             | Collaboration Index                   | Review                             | 54                                |
| Collaboration Index                    | 4.36                             |                                     | Short survey                       | 1                                 |

Fig. 1. Country collaboration map.
Horizon 2020 Framework Program, the Korean National Research Foundation, the National Institutes of Health, and the US National Science Foundation also sponsor the majority of studies.

As illustrated in Fig. 1, there is a significant degree of collaboration among European nations, many of which have strong ties to the United States and Australia. On the other hand, China has a limited amount of international cooperation with Australia, Europe, and the United States. Additionally, Canada maintains a minimal level of communication with a number of European and American countries.

3.2. Co-citation analysis

In this section of the paper, we report on the co-citation analysis we conducted on documents, sources, and authors to address the study’s first question: Which documents, sources, and authors have garnered the most citations in research on the privacy implications of CTAs? The social networks were then depicted based on their total link strength.

3.2.1. Co-citation analysis of documents

The co-citation analysis of documents reveals that the themes of “acceptability,” “privacy preservation,” “motivations to use,” “data protection,” and “ethics norms” obtained the most citations and had the strongest link strength. This analysis demonstrates the importance of public adoption of CTAs, as well as public concern over personal data and the need for privacy-preserving solutions. As illustrated in Fig. 2, the top five documents with the highest total link strength and citations are as follows:

1. Altmann, Samuel, Luke Millsom, Hannah Zillessen, Raffaele Blasone, Frederic Gerdon, Ruben Bach, Fruuke Kreuter, Daniele Nosenzo, Séverine Toussaert, and Johannes Abeler. “Acceptability of app-based contact tracing for COVID-19: Cross-country survey study.” JMIR mHealth and uHealth 8, no. 8 (2020): e19857
2. Yasaka, Tyler M., Brandon M. Lehrich, and Ronald Sahyouni. “Peer-to-peer contact tracing: development of a privacy-preserving smartphone app.” JMIR mHealth and uHealth 8, no. 4 (2020): e18936
3. Kaspar, Kai. “Motivations for social distancing and app use as complementary measures to combat the COVID-19 pandemic: quantitative survey study.” Journal of Medical Internet Research 22, no. 8 (2020): e21613
4. Abeler, Johannes, Matthias Bäcker, Ulf Buermeyer, and Hannah Zillessen. “COVID-19 contact tracing and data protection can go together.” JMIR mHealth and uHealth 8, no. 4 (2020): e1935
5. Morley, Jessica, Josh Cowls, Mariarosaria Taddeo, and Luciano Floridi. “Ethical guidelines for CTAs.” (2020): 29-31

3.2.2. Co-citation analysis of sources

According to the sources analyzed, JMIR mHealth and UHealth published 17% of the articles, followed by IEEE Access and Journal of Medical Internet Research, which each published 11% of the articles. Moreover, PLOS One published 8% of the publications. JMIR Public Health and Surveillance, IEEE Internet of Things Journal, Scientific Reports, Ethics and Information Technology, and European Journal of Information Systems are additional sources that have published papers at rates of 5% and 4%. Furthermore, Fig. 4 displays the evolution of sources’ scientific productivity from 2020 to 2021. As illustrated in the figure, six of the top ten sources have increased their publication of articles on this subject. The h-index analysis also reveals that the top five sources with the highest h-index are JMIR mHealth and uHealth (h-index of 9), Journal of Medical Internet Research (h-index of 7), IEEE Access and PLOS One (h-index of 6), and European Journal of Information Systems and JMIR mHealth and Surveillance (h-index of 6) (H-
Co-citation analysis of sources (Fig. 3) also revealed that Science has the highest TLS score, followed by IEEE Access. Furthermore, PLOS One, JMIR mHealth, uHealth, and Lancet have the greatest TLS scores.

3.2.3. Co-citation analysis of authors

There are six clusters of researchers focusing on the privacy of CTAs, as shown in Fig. 5. Cluster 1 is shown on the right side of the figure, Fretti Luca; Kendall, Michelle; Nurtay, Anel; and Fraser Christophe are all from the University of Oxford’s Big Data Institute. They contend in their study published in Science that quantification of SARS-CoV-2 transmission suggests that managing the outbreak would be more effective with digital contact tracing and reducing ethical challenges to enhance the uptake of these technical solutions. There is a dense cluster of three authors, Hyunghoon Cho (Broad Institute of MIT and Harvard), Daphne Ippolito (University of Pennsylvania), and Yun William Yu (University of Toronto), at the top of the figure. In their study, they discuss solutions to minimize privacy concerns while maintaining the efficiency of these applications for improved public health management. The other cluster at the top is composed of two authors, Ramesh Raskar and Praneeth Vepakomma from MIT Media Lab, who have offered various privacy preserving solutions such as differential privacy. At the upper left, a cluster includes Samuel Brack and Björn Scheuermann of Humboldt-Universität Berlin and Leibniz Universität Hannover, respectively. Likewise, these researchers have offered methods for ensuring the privacy of CTAs. At the bottom of the figure is a dense cluster of authors, including Nadeem Ahmed, Regio Michelin, Wanli Xue, Sushmita Ruj, and Salil Kanhere, all from Cyber Security Cooperative Research Center, University of New South Wales. They conducted a thorough technical analysis of the characteristics and privacy risks associated with CTAs.

4. Co-occurrence analysis of keywords and content analysis of topics

4.1. Content analysis of topics

As demonstrated in Figs. 6 and 7, this phase of the study resulted in the identification of nine important topics. To show the network, we set the normalization method to the default and most popular option of “association strength,” which allows for the categorization of more closely related keywords into a single topic [27]. The authors manually selected publications with the greatest relevance to each topic for content analysis. These analyses enabled us to respond to the study’s remaining research concerns. As Fig. 6 shows, there were some overlaps between topics, mainly topics at the left side of the network, which is a common pattern in this methodology [30].

Topic 1: Proximity measurement technologies embedded in tracing apps and varied privacy challenges.

We live in an era of tremendous technological growth, and some of these advancements are utilized to determine proximity. When the COVID-19 pandemic ravaged the world, social separation of 1.5 m was recommended to minimize infection. As a result, COVID-19 monitoring apps integrated with digital proximity sensing technologies were developed with the objective of determining exposure distance and duration. Despite the health benefits of these applications, a number of studies have questioned them, suggesting they are vulnerable to user privacy threats [31]. As a result of these problems, as Table 2 summarizes, several solutions have been developed to improve the privacy of CTAs by equipping them with the most privacy-preserving proximity measurement technologies available, including blockchain, Bluetooth, QR, WIFI, GPS, and GIS. Simultaneously, researchers introduced a variety of privacy-preserving alternatives, including decentralized privacy,
One of the technologies embedded in CTAs is blockchain, which has been deployed in the healthcare industry [32] and has been combined with COVID-19 monitoring applications to address privacy, security, and interoperability concerns [33]. In terms of protecting patients’ privacy and personal data, blockchain technology appears to be promising. According to studies, blockchain-based tracing apps have a variety of features that solve privacy concerns and data-related trust issues [34], such as facilitating the secure and legitimate exchange of data between individuals and governments [35]. Moreover, blockchain technology has been crucial in combating disinformation and increasing the transparency of accurate data [36]. Provision of blockchain-based privacy-preserving contact tracing applications for the purpose of desensitizing patient ID and location information [37] has yet to become a primary technical intervention, as does the improvement of blockchain features, including time stamping and data immutability [38]. Consolidating sophisticated cryptographic techniques with blockchain technology may potentially lead to a significant diminution in the vulnerabilities.
connected with tracing applications [39]. For example, crypto-spatiotemporal information contributes to the preservation of personal privacy. Consequently, it is critical to recognize how personal privacy can be jeopardized whenever patients and their close relationships are tracked using spatiotemporal data. Additionally, researchers have designed a blockchain-based solution for preserving transaction anonymity [40]. For illustration, one study developed a self-sovereign identity-enabled contact tracing technology on the blockchain that ensures no user identification is revealed [41]. Various technologies, such as 5G, can be integrated with blockchain to assist users in locating diagnosed COVID-19 patients without jeopardizing privacy [42].

Bluetooth-based apps are one of the most frequently deployed technologies for CTAs given its widespread support by smart devices. However, Bluetooth-tracing applications centralize contact data collection, posing a threat to privacy [43]. One issue of contention in the privacy discussion concerns complex indoor locations, such as nursing homes or hospitals, where short-range wireless devices may generate concerns about privacy [44]. Alternatively, measures such as acquiring large-scale geolocation data are recommended. Nonetheless, some researchers claim that as an application’s reach expands, the risk of data leakage and exploitation escalates [43]. Global Positioning System, or GPS, as one of the most widely adopted location data technologies, is also embedded in CTAs and has been critiqued for its potential risks to health surveillance, for recording users’ exact locations, for threatening location privacy, and for exposing personal data [45]. While Bluetooth-enabled CTAs compromise privacy through the exchange of identifiers, GPS-enabled solutions violate privacy primarily through mass tracing [46].

One significant technical approach for preserving privacy is the use of privacy-enhancing technologies (PETs), such as differential privacy or the method of privacy by design, to mitigate privacy breaches or attacks by malicious third parties [47]. Privacy by design refers to the process of implementing privacy protection into the overall design of technology [48], whereas differential privacy refers to approaches for acquiring information about sensitive data without disclosing too much about any particular individual [49]. As will be discussed in Section 4.2, privacy by design is among the most heated scholarly topics.

Another technical solution is the development of decentralized tracing applications. Several previous research studies from a variety of fields have proposed unique strategies for limiting the privacy risk connected with contact tracing applications, proposing that both legal and technological remedies may be considered [50]. Some governments, in collaboration with technology companies, have devised a number of privacy-preserving alternatives, such as decentralized systems, in reaction to the constraints of centralized applications developed by some countries, including India or Singapore [14]. While some studies assert that centralized methods can more rapidly and reliably detect infected individuals and high-risk public spaces [51], others argue that centralized systems jeopardize individuals’ privacy [52]. Decentralized apps, such as Austria’s Stopp Corona or Vietnam’s Bluezone [53], do not retain data on a single server but rather interchange it between a network of interconnected servers [54].

Topic 2: Democratic and Social Discriminatory Consequences.

Researchers are concerned with two important difficulties with COVID-19-tracing apps: the disclosure of personal data and the consequent breach of democratic values, and the potential for social discrimination as a result of disease revelation. Democratic principles and a just and equitable society may be compromised because of data and disease disclosure. According to studies, state control was heightened during the COVID-19 epidemic not only in authoritarian regimes,
but also in democratic and autocratic countries equally [55]. This dilemma has been aggravated by governments’ compulsion to download applications against citizens’ consent. Voluntary installation of CTAs has been violated in a number of nation [56]. For instance, in India, the government’s requirement that residents install the national CTAs fostered distrust and aversion to adoption [57]; in addition, Israel’s authorities have tracked down cases of the virus by utilizing a phone tracing database often used for counterterrorism [58]. Whereas some researchers argue that digital health surveillance does not threaten a democratic society’s fundamental characteristics [59], some studies have debated whether mandatory app installation is a type of biopower exercise [60] or a form of state surveillance [55]. Prior studies have disputed the extent to which tracing applications can protect citizens in a democratic society and highlighted the peril of undermining the public’s trust if tracing applications do not adhere to data capture privacy principles and result in the unintended disclosing of users’ data, such as their disease, contacts, or location data [61]. Whereas several governments have enacted standards demanding limited or no exposure of users’ information and utilizing a variety of technical approaches [62], investigations reveal that some tracing apps tend to disclose portions of their users’ private information [63]. Certain tracing applications have developed techniques for revealing only a portion of the user’s data, such as their movement patterns [64]. Studies contend that infringing on the app’s voluntariness may erode civil freedoms such as freedom of movement and gathering [65] and may exacerbate social discrimination [66], particularly among affected populations. Demographic data and socioeconomic status are also disclosed by the apps, including users’ race, clan, or region of origin. As a result of this data’s influence on the allocation of COVID-19 resources, social and financial injustice may increase [67]. Another vulnerable group is the working class, which resists the installation of CTAs, fearing that doing so will expose them to personal hazards such as stigma, anxiety, and financial loss [68]. According to several studies, COVID-19 is a stigmatized disease because some individuals anticipate that disclosing their illness may result in social isolation, stigma, and psychological distress from their contacts [69]. As a result, one of the worries that may deter individuals from installing and using COVID-19 tracing tools is the possibility of discriminatory confrontations [70].

### Topic 3: Human rights aspects of CTAs.

The effects of CTA on human rights is one of the major issues being examined by researchers. Concerns about the effectiveness of digital technologies for health monitoring, the involvement of third parties in the collection, use, and storage of personal data, the potential threat to minority groups, and the misuse of these systems by state and non-state actors have sparked human rights concerns about CTAs [59]. Prior research suggests that, despite global attempts to develop

---

**Table 2**

Technical summary of some of COVID-19-tracing applications [12].

| Centralized/Decentralized Application | Country/state | Application Name | Embedded Proximity Measurement Technology |
|--------------------------------------|--------------|-----------------|------------------------------------------|
| Centralized                          | Alberta, Canada | ABTraceTogether | Bluetooth                               |
|                                       | Part of US states, and EU (except UK & France (planned)) | Apple & Google SDK | Bluetooth                               |
|                                       | Austria       | Stopp Corona    | Bluetooth                               |
|                                       | Hong Kong     | Stay Home Safe  | Bluetooth, Wi-Fi                        |
|                                       | Vietnam       | Bluezone        | Bluetooth                               |
|                                       | State of Dekota, US | Care19 | GPS                                      |
|                                       | Germany       | Healthy Toghter | GPS                                      |
|                                       | UK           | Corona Data Donation | GPS                                      |
|                                       | China         | WeChat & Alipay | QR Code, Big data                       |
|                                       | Singapore     | TraceToghter    | Bluetooth                               |
|                                       | Australia     | COVID-19safe    | Bluetooth                               |

---

**Fig. 7.** Conceptual Structure of research on privacy of CTAs.
COVID-19-related legislation, they should be more transparent and explicit about personal data protection and human rights [71]. As [72] recommend, urgent COVID-19 solutions should be accessible to open examination and, unless the government can demonstrate that they are necessary and proportionate, should be immediately terminated, considering the fact that in emergencies, temporary suspension of certain human rights are permitted only to the extent that the necessities of the situation warrant it [73]. For instance, Article 17 of the ICCPR recognizes that the right to privacy is violated when a person’s contact information is traced. Interferences with privacy that are not arbitrary and proportional are allowed under Article 17(1) [74]. As a consequence, governments should strike a reasonable balance between human rights protection and public health promotion, while seamlessly incorporating human rights principles into COVID-19 initiatives [75]. Some studies have criticized existing and proposed regulatory and technical solutions for failing to defend human rights adequately.

According to previous studies, derogation from human rights must meet a number of criteria, including legality, necessity, and proportionality [76]. One study argues that COVID-19-tracing applications should be evaluated according to four human principles: necessary, proportional, scientifically valid, and time-bound. For instance, in Korea, while the tracing app is scientifically valid and viable and satisfies the necessity criterion, it is too ambiguous in terms of adhering to the time-boundness principle [77]. According to some other studies, the human rights implications of CTA can be examined via a variety of perspectives, including privacy, autonomy, and nondiscrimination [59], rights to equality, privacy, human dignity, as well as freedom of speech, association and movement, and security of the person [78].

Topic 4: Governance of the CTAs.

There is debate on the prophylactic purpose and practicality of CTA in light of bioethical and governance concerns [79], as well as the difficulties inherent in incorporating key ethical principles into governance processes, particularly when they lack accountability [80]. The World Health Organization has affirmed the critical importance of adequate tracing application governance [62], owing to reservations and mistrust pertaining to the capacity of existing public health infrastructures [81], as well as government partnerships with large technology companies. Some studies refer to CTAs as “corporate tracing apps” to underline the private sector’s and large technology corporations’ involvement in the deployment of CTAs [82]. These studies offer technical solutions such as decentralized applications [81]. Some research claim that CTAs have been normalized as valid instruments for state governance, leading to the development of a distinct kind of pandemic techno-governance in which the lines between care and control are compromised [83]. Pandemic control may jeopardize data governance, necessitating an assessment of the issue at a time when data may be collected and used without individuals’ knowledge or consent or for government-mandated objectives [84].

To allay public suspicion about the vested interests of CTAs and to legitimate government initiatives, several countries, such as Switzerland or France, have incorporated diverse stakeholders throughout the development of CTAs [85]. Some studies recommend the development of locally contextualized governance frameworks in accordance with factors such as immediate health risk, prior experience with pandemics, societal values and national culture, role of government, trust in government and trust in technology in each society [36]. For instance a governance framework for CTAs can contain four unique sorts of determinants: the entities that might be involved in societal governance and collective action: individuals, organizations, platforms, and governments [86].

Topic 5: Adoption and Trust.

Regardless of the governments’ approach for preventing COVID-19’s spread, public participation is critical in effective management of public health. The efficiency of CTAs is highly dependent on individuals’ acceptance and favorable attitude toward them, as well as their trust in government [87]. Thus, Topic 5 of this analysis focuses on elucidating factors that drive or prevent individuals from adopting applications and determinants of citizen trust in government. A series of barriers prevents individuals from installing applications, including concerns about their privacy, and perceived stigma [69]. Furthermore, some people have expressed distrust in their governments and concerns about their safety on social media [88]. There is a significant disparity between what individuals profess to perceive and how they behave, since the public claims these applications are ineffective but nonetheless downloads them in reaction to government mandates [89].

While one section of the studies concentrates on factors that contribute to or impede the adoption of tracing applications, another section seeks to offer remedies and techniques to accelerate adoption. For example, research indicates that financial incentives such as gift cards can significantly increase app usage [90,91]. However, adoption is influenced by a variety of factors, not just financial incentives. According to one study, once users experience negative emotions such as rage or annoyance, they remain unwilling to adopt the applications; thus, it is recommended that developers increase users’ control over technology to ensure that they avoid experiencing negative emotions [92]. This argument is especially notable given that one study reveals that the app’s access authorization constraints have a negative impact on user adoption rates [93]. Trust is a strong component in adoption [94]; for example, research has demonstrated that cognitive and emotional trust favorably affects people’s willingness to reveal personal information [95]. Additionally, the literature incorporates the Uncertainty Reduction Theory to indicate that initiatives to reduce uncertainty, such as trust in government, will increase adoption [96]. Additionally, studies advocate for the implementation of blockchain due to its decentralized governance structure and privacy-preserving capabilities, which enable the establishment of a “trustless” system that boosts the effectiveness of CTAs [34].

Topic 6: Monitoring and Surveillance Challenges.

Citizen surveillance, disease surveillance, epistemic surveillance, state surveillance, public health surveillance, and capitalist surveillance are just a few of the most frequently hurled criticisms directed at CTAs. Apprehensions regarding surveillance stem from CTAs’ surveillance capabilities, such as the potential to track users’ movements [97]. Concerns about user surveillance and potential threats to democratic society’s principles stimulate efforts to design efficient surveillance systems [98].

In health surveillance, patients and their disease state are monitored using data supplied by citizens via mobile phones and social media, rather than self-reported data [99]. This non-participatory technique was presented as a substitute for local “participatory COVID-19 surveillance tools” [100,101] and due to individuals’ possible reluctance to install the app on their smartphones [98]. According to scholars, the participatory or non-voluntary nature of CTA will blur the lines between health data and existing government surveillance measures [11,102]. As a result, an emphasis is being devoted to the development of non-participatory, privacy-preserving surveillance systems in which users are not obliged to use CTA and diseases are monitored without relying on citizen self-reports [98]. These scholars argue for the inclusion of smartphone-based GPS and social media data, suggesting that relying on patient self-reports of symptoms to prevent transmission is impractical [99].

Surveillance capitalism [103,104] or biopolitics [105] refers to technology corporations’ mishandling of crises and their collaboration with the government to advance their vested interests. With governments increasingly collaborating with technology companies to develop CTAs, concerns about a new model of capitalism based on surveillance technologies and data have arisen. Scholars argue that commercialization of citizens’ personal data and behavioral patterns, such as contacts or locations or other ethnic data, will benefit both private companies and the government, enabling the government to raise state surveillance [102]. According to this research, CTAs can legitimize surveillance capitalism by capturing and exploiting citizens’ social, spatial, and
contact data for commercial advantage [105]. The findings imply that by utilizing CTAs, corporate control over the public domain can be reinforced [82]; as a result, they advocate for remedies such as the socialization of ownership of emerging technology [106]. Epistemic surveillance is another academic discussion that relates to the exploitation of the user’s personal data in this scenario [107].

Topic 7: Digital-Politic Nexus.

The link between politics and digital technologies is one of the key issues with CTAs. When science and politics collide, it is said that politics triumphs [108]. To fully grasp how to maintain the functionality of medical applications while also considering the political consequences of these technological breakthroughs, researchers are recommending a closer analysis of the digital-political nexus and the national conflicts it engenders [109]. Throughout COVID-19 pandemic, governments’ misinformation and disinformation have posed a significant obstacle to promoting transparency and accountability. Due to surveillance apps’ ineffectiveness in reducing COVID-19 patients, studies recommend analyzing the wider context of tracing apps in terms of the influence of complex and interwoven sociopolitical contexts [110]. According to the findings, the COVID-19 “infodemic” is inextricably linked to the pandemic. The term infodemic refers to an abundance of information on a situation that is often erroneous, spreads swiftly, and makes obtaining a solution more complicated and data culture is influenced by pandemics [111,112] and is mostly produced by political misinformation in nations such as the United States of America and India [113]. The majority of COVID-19 misinformation collected on social media varies widely across languages and nations due to cultural and religious diversity, with political position accounting for the majority of misinformation collected [114]. Additionally, reviews of citizen comments on applications reveal that the majority of citizen dialogues or comments on CTAs are political in nature, with less emphasis on the app’s usefulness or performance [110]. In terms of the relationship between citizen adoption and political factors, some scholars claim that because state-level data and people’s political affiliation have a significant impact on the adoption of CTAs, macro-political contexts should be assessed rather than individual-level factors [115].

Topic 8: Non/Supportive Legislations.

Tracing applications have a predisposition for unanticipated negative implications for their users, such as concerns of confidentiality and transparency [96]. This has prompted countries to enact legislation to protect consumers’ privacy and control rights. For instance, data flow and storage have been restricted as a result of the Commonwealth Government’s legislation. The COVID-19 Safe Bill 2020, introduced by the Australian government, forbids any entity to force anyone to use the app for any reason [116]. The GDPR, or General Data Protection Regulation, is one of the most well-known and widely recognized data protection laws in the world. In comparison to sector-specific standards, such as the US Health Insurance Portability and Accountability Act (HIPAA) and California’s new Consumer Privacy Act (CCPA), both of which contain gaps that make it difficult to manage COVID-19 effectively, some researchers argue that a framework with a broader reach, such as GDPR, is preferable under uncertain COVID-19 app conditions [117].

Apart from examining the legislation controlling the use of CTAs, experts have examined the many ways in which governments regulate their usage. While more democratic nations enact supportive legislation to safeguard citizens against unintended negative consequences, certain governments, like in India [57] and Qatar [118], have compelled residents to use the CTAs.

Additionally, as studies reveal, the government’s failure to recognize the legal issues inherent in CTAs and to build permanent regulatory frameworks erodes public faith in the apps, weakening their effectiveness [119]. With the advent of deep learning and complicated artificial intelligence algorithms and their incorporation in digital health care [120], experts have argued for the establishment of regulatory regimes for the advancement, administration, and procurement of AI in order to ensure the ethical and safe use of AI in the national healthcare sector [121].

Topic 9: Artificial Intelligence and Predictive Tracing Practices.

Divergent viewpoints exist regarding the effectiveness of artificial intelligence in boosting the functionality of CTAs. Scholars argue that AI systems lack enough maturity to combat COVID-19 and governments may abuse data-driven AI systems for citizen surveillance [122]. According to one side of the debate, a lack of data for training and pattern extraction may have hampered the deployment of AI in tracing applications [67]. Within the debates, some scholars cast doubts about the validity and accuracy of AI algorithms embedded in contact tracing apps, noting gaps in the detection and prediction of COVID-19 cases, as well as in tracing infected individuals’ contacts [123]. Certain studies advocate for the establishment of regulatory frameworks to ensure the development and deployment of ethical and safe AI that is merged with privacy-preserving solutions, given reservations over the use of AI in CTA [121]. On the other hand, one side of the debate contends that artificial intelligence and high-performance computing accelerated the development of personalized treatments to avoid transmission [124]. Additionally, proponents assert that artificial intelligence (AI) has facilitated social distancing by developing novel solutions like symptom prediction, identification and monitoring of quarantined persons, and contact tracing [125].

4.2. The most stressing privacy repercussions of CTAs

Constraints and solutions relating to privacy have an effect on the effectiveness of CTAs. We have summarized the most concerning privacy implications and solutions related with CTAs in this section of the paper (Fig. 8). The most important privacy concept is privacy by design, which is a technical approach that will most likely promote the adoption of CTA [126]. According to current research, the primary impediment to citizens adopting CTAs is privacy. Several privacy-protection strategies have been offered, including anonymization, encryption, obfuscation, pseudo-anonymization, and hybrid [128]. In order to alleviate citizens’ concerns, human-centered technologies such as privacy by design were introduced [128,129] that were respectful of societal norms and safeguarded civil freedoms [127]. Privacy by design presupposes that privacy must be a de facto characteristic of networked data systems and technologies, which must adhere to several principles: privacy by design systems are proactive and preventive; privacy is the default and is constructed into the design; the systems have full functionality; and there is end-to-end security and respect for user privacy [130]. Data minimization is also incorporated into these principles which means that only the information that is absolutely essential is stored and processed [131].

As mentioned earlier, decentralized privacy was also recommended to alleviate intrusions. Nations such as the United Kingdom updated their first COVID-19 tracing app with a new one based on Apple and Google’s decentralized methodology [132], and several European countries embraced the DP3T (Decentralized Privacy-Preserving Proximity Tracing) protocol [132,133]. Decentralization, in essence, is the transfer of power and authority from a single central authority to a network of distributed participants [134]; thus, a decentralized system is a network that does not rely on a single master node for control; rather, it distributes control among numerous nodes [135].

The second most significant privacy-related issue, surveillance, sparked these solutions. This concern entails reservations about the likelihood of governments and companies misusing individuals’ personal data for their own vested interests. The blurred lines between disease surveillance and individual surveillance, as well as each country’s unique political economy, led some scholars to refer to the CTAs as pandemic surveillance technologies [20] as governments adopted them as political expedients and rapid policy responses to crises [136].

The other significant privacy component of CTAs is connected to citizen attitudes, notably their trust in government-based applications.
developed in collaboration with large technological corporations. During uncertain scenarios such as COVID-19 pandemics, trust in government will promote application adoption, as mistrust of governments in the United Kingdom and Australia was the primary barrier to citizens embracing CTAs [137, 138]. This lack of trust is exacerbated even further among minorities and vulnerable groups. For example, one analysis revealed that reduced trust in the UK’s National Health Service among black, Asian, and minority ethnic populations had an effect on the app’s uptake [139]. Moreover, according to one research, immigrants in the United States fear that these applications are actually owned by police [140].

The human rights implications of COVID-19 are also highlighted in the literature, allowing governments to strike a balance between public health management and individual human rights protection [75]. As a result, some researchers have reviewed various legislations to see whether they safeguard individuals’ privacy in accordance with concepts like as proportionality and minimization. These human rights principles emphasize the anonymization and consent of individuals during data sharing processes, as well as the generation and processing of data only when a legitimate risk of infection persists [141] or when action is justified and the benefits outweigh the risks [77]. Other human rights considerations for CTA include voluntariness and reversibility [142], transparency and verifiability [143], and accountability [117].

5. Analysis and conclusion

This section of the article will address the study’s last query: what gaps exist in the literature and what future research agendas exist?
6. Discussion

We conducted a bibliometric and content analysis of research on the privacy implications of CTAs in this research. We sought to identify the most highly cited countries, institutions, sources, and documents, as well as the most highly addressed academic subjects and most pressing privacy concerns. Additionally, we identified gaps in the literature and proposed future study objectives.

Theoretically, this research contributes to an expanding body of knowledge on digital health ethics, notably the privacy concerns surrounding mobile health applications that include proximity measuring technologies and other cutting-edge digital technologies that capture personal data. This study contributes to the body of knowledge by identifying the most significant entities and research topics that the literature has largely overlooked or not highlighted. The purpose of this study is to identify theoretical research gaps and to recommend prospective research initiatives to address them. Practically, this research serves as a guide for policymakers, governments, application developers, and technology companies interested in garnering citizens’ trust and increasing their adoption of tracing applications through the integration of technical and non-technical solutions that mitigate privacy risks and increase user participation in the development of applications and regulations. This study reveals that significant scientific discussions exist regarding the risks connected with digital mobile health applications that incorporate proximity measurement and other cutting-edge digital technologies, such as blockchain or artificial intelligence. We performed co-citation analysis to determine which entities, such as authors, sources, and documents, obtained the most citations so far. After identifying the research topics by keyword co-occurrence analysis, we conducted a topic-based content analysis to gain a deeper understanding of the research topics. Our investigation yielded nine major scholarly topics. The first topic is the measurement technology integrated into tracing apps and the privacy problems that accompany it. The second subject deals with democratic and social discrimination challenges, while the third topic closely addresses the human rights concerns of CTAs. The fourth subject is governance of CTAs, and the fifth is perceptions, attitudes, adoption behavior, and trust among citizens. The sixth theme examines the discussions about surveillance and monitoring. Furthermore, the seventh subject delves into the relationship and tensions between digital health technology and politics. Topic 8 compares helpful and non-supportive regulatory systems and legislation. The ninth research focus discusses how artificial intelligence and its predictive capabilities may be utilized to manage the COVID-19 tracing crisis. Other topics also encompass the application of proximity-measuring technology and artificial intelligence. Based on these analyses, we identified a list of the most pressing privacy challenges and solutions that are widely discussed in the literature.

In this study, we identified seven major privacy challenges of CTAs depicted in Fig. 9. These challenges are politicization of care; antidemocratic and social discrimination practices; human rights derogation; techno governance; citizen distrust and refusal to adopt; monitoring and surveillance; and mandatory legislations of installing the...
apps. Tracing applications have an unfavorable reputation among the public despite their promise to safeguard healthcare: Certain studies claim that proximity measurement techniques may be manipulated by certain governments to undertake anti-democratic and socially-biased policies. Patients’ anxieties about social shame will be compounded by disclosing their disease, while revealing their location data fuels suspicions of government control and monitoring. Furthermore, researchers contend that governments have established alliances with the world’s largest technological corporations to design privacy measures that are decentralized. These studies suggest that these legal measures would safeguard citizens’ safety, but given the public’s historical mistrust toward governments and their collaboration with major technology corporations, individuals have become more anxious about data privacy and its sharing with tech businesses. Consequently, individuals are concerned not just about government surveillance and control, but also about the partnership between the government and technological firms with economic and vested interests, which will offer such firms incentives to exploit the private information of citizens.

The blurring lines between governments and technological corporations, as well as each party’s entrenched interests, have rendered health care and politics, as well as financial gain, indistinguishable. Hence, the lack of trust in the government, fear of control, financial vested interests of technology corporations, and societal stigma and prejudice have fostered an environment of anxiety about installing and using the applications. This circumstance may be exacerbated among vulnerable groups, especially racial and ethnic minorities, or among families who have lost loved ones due to COVID-19. As a result of the rising incidence of COVID-19 deaths and the subsequent grief, tracing applications are less likely to be adopted by the affected citizens. Mandatory regulations by the governments that compel their citizens to download and install the apps have aggravated the skepticism and lack of motivation to use the applications, leading to a negative perception of the apps. Aside from that, the absence of explicit legislative frameworks for healthcare tracing applications has exacerbated public mistrust of them. It is important to consult more stakeholders, especially doctors, hospitals, and healthcare providers, throughout the development of tracing apps because privacy concerns have been heightened by the low participation of healthcare stakeholders such as hospitals and clinics in the development of tracing apps. Shifting responsibility from governments and their commercial partners to health care providers, including hospitals and healthcare providers, could undoubtedly enhance confidence and lessen privacy concerns. In this way, there have been very few studies that have tried to improve the understanding of other stakeholders, like patients and citizens, about tracing applications. This lack of information would make people more negative about the applications.

While the majority of efforts have been dedicated to developing more advanced technologies and engineering solutions to reduce privacy threats, supplemental steps must be conducted to boost public confidence in these applications through regulatory, educational, and even psychological and emotional support measures. Using a technocratic mindset when introducing new technologies like AI, which are full of unknowns, will not encourage people to use and like tracing applications.

The research also found that data processing must be legitimate from a human rights standpoint. GDPR Articles 1–6 stipulate that data processing is permissible only with the consent of the data subject. A crucial criterion for evaluating the constraints of human rights, particularly the right to privacy, is the need for restrictions. Processing personal data undermines individuals’ right to privacy, making it necessary to limit that right. The word “proportional” suggests a connection between the data processed and the intended purpose of the data. This proportion comprises processed data and tools for processing. Only the data necessary for the processing purpose should be gathered and processed. Adequate security measures should also be taken while processing data to make sure that data privacy is protected to the fullest extent possible.

6.1. Limitations of the study and possible future research streams

Fig. 10 depicts a number of other future research initiatives that we propose. While the majority of previous research has focused on the interaction between the state and commercially dominant technology corporations, we presume that more research should be conducted to examine the triple helix of relationships between people, technology companies, and the government. Since both the government and commercial technology corporations have vested interests, it is critical that citizens’ interests and perspectives be considered in these relationships. As a result, more research should be conducted to better understand the processes that allow people to participate in these partnerships while also having their interests considered. Constructing mechanisms to improve the interactions of these three players, as well as incorporating citizens’ interests, would improve the efficacy of CTAs while also alleviating citizens’ privacy concerns. Similarly, more research should be conducted to determine ways to improve oversight and regulation of technology corporations and their use of citizens’ location data. It is also critical to understand how governments’ political contexts and governance structures influence the triple helix of interactions between the state, citizens, and large corporations. In countries where capitalism is practiced and technological corporations play a significant role in data management, the entrenched interests of each party differ from those in countries where communist principles and fewer commercial companies have an influence. It is critical to understand the impact of governance and political dynamics on government responses to health emergencies in order to meet the demands of all stakeholders. For example, it may be worthwhile to investigate how political and cultural structures influence people’s adoption of proximity tracing applications as well as their perceptions of their functionality.

The adoption of tracing applications is not determined by a single factor and direct relationships. As a result, additional research is required to investigate the configurational and indirect relationships between the components that influence the adoption and perceptions of tracing applications. Scholars can then quantify the moderating or mediating effects of mortality rates as well as other socioeconomic and political factors in this regard. Furthermore, it is critical to investigate the intricate relationships between privacy-related technological breakthroughs, privacy legislative frameworks, and the variety of modalities. With the growth of biopower and surveillance capitalism, more research may be conducted to develop mechanisms that increase people’s participation in triple helix interactions and provide greater control over their personal data. To grant users more control over their personal data, developers and technology companies should design applications so that citizens can set their own limits on the sharing and disclosure of their personal data with third parties.

Social media and the app store’s review section are critical platforms for citizens to express their feelings and thoughts about the CTAs. As a result, more research into social media content and review content may be conducted in order to gain a better understanding of how people perceive CTAs. The exploitation of individuals’ personal location data is a significant reason to exercise caution. Aside from differential privacy, non-technical strategic policies and techniques are required to prevent people’s location data from being exploited for purposes such as patient monitoring and control in settings such as hospitals.

As previously stated, some previous research emphasizes the development of automated data collection systems with little or no public input in reporting them. More attention is needed for these automated systems since they may jeopardize citizens’ control, autonomy, and informed consent. As a result, it is critical to investigate the privacy implications and difficulties associated with disease monitoring systems that use automated data collection systems. The privacy issues surrounding CTA are inextricably linked to double-edged issues such as disease control and citizen control. Furthermore, technology firms are proposing increasingly complex technical solutions that may be perplexing to the public. As a result, additional educational programs
to educate the public and broaden their understanding of complex technical jargon are required.

The study discovered that tracing apps use a variety of technologies, such as Wi-Fi, Bluetooth, and GPS. More research can be performed to better understand the relationships between mortality rate, installation rate, and use of various location technologies in order to determine which technologies may improve both the effectiveness of the apps in managing pandemics and the privacy of citizens. Governments also intervene based on the data generated by these location measurement technologies. It is critical to assess the veracity of data generated by any location technology in order to avoid unintended negative consequences of assumptions derived from the data.

The majority of CTAs are developed and implemented as a result of collaboration between governments and technology companies, which have entrenched interests and, as a result, garner less public trust. The government must delegate responsibility for developing and implementing CTAs to local actors such as hospitals and healthcare stakeholders, who are the primary guardians of healthcare. More academic scrutiny is needed to determine whether the devolution of power and accountability to local and specialized actors will result in increased privacy safeguards and increased adoption of mobile health applications embedded with digital technologies.

This research has limitations of its own. We studied only English-language articles and conducted bibliometric analysis, which has its own limitations, such as old papers that receive more citations [144]. Another limitation of this study is that we did not address the evolution of citations for papers over time. We also did not conduct more in-depth bibliometric analyses, such as the number of self-citations or the percentage of cited versus uncited articles, so that future research studies can address these scientific inquiries. Another limitation of our study is that we chose a time span of two years, which is a limited period for analyzing annual topic development. As a result, one possible future research direction could be to consider a longer time span to measure the evolution of topics over time. Co-citation analysis also has a number of benefits and drawbacks. Its primary strength is that it assesses the intellectual development and structure of scientific disciplines and classifies papers that share a common theme or area of research [144, 145]. As [146] explains, the primary limitation of co-citation analysis is its inconsistency in coverage over time and the possibility of citation errors. In light of these limitations, we recommend that future studies employ alternative quantitative methods, such as topic modeling, to track the evolution of scientific literature. Furthermore, unlike topic modeling techniques, VOSviewer software does not segment papers by topic; thus, future research can leverage topic-modeling techniques for this purpose. Finally, we recommend that additional studies beyond bibliometric and topic analysis be conducted, such as analyzing papers from a methodological and research methods perspective, or analyzing papers through a theoretical lens.

Declaration of competing interest

We declare no conflicts of interest.

Acknowledgement

We wish to express our gratitude to Hedy Lamar, the first female scientist to invent WiFi, Bluetooth, and GPS.

References

[1] L. Ferretti, C. Wyman, M. Kendall, L. Zhao, A. Nurtay, L. Aebler-Dörner, M. Parker, D. Bonsall, C. Fraser, Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing, Science 80– (2020) 368, https://doi.org/10.1126/SCIENCE.ABB6936 SUPPL_FILE/PAPV2.PDF.
[2] T. Smieszek, S. Cantell, A. Barat, C. Cattuto, P.J. White, G. Krause, Contact diaries versus wearable proximity sensors in measuring contact patterns at a conference: method comparison and participants’ attitudes, BMC Infect. Dis. 16 (2016) 1–14, https://doi.org/10.1186/S12879-016-1676-Y FIGURES/3.
[3] A. Wesolowski, C.O. Buckee, K. Enge-Monsen, C.I.E. Metcalf, Connecting mobility to infectious diseases: the promise and limits of mobile phone data, J. Infect. Dis. 214 (2016) S414–S420, https://doi.org/10.1093/INFDIS/JIW273.
[4] R. Jalalbreh, H.Z. Syed, S. Pillai, E.H. Apu, M.R. Hussein, R. Kabir, S.M.Y. Arafat, M.A.A. Majumder, S.K. Saxena, Use of Mobile Phone Apps for Contact Tracing to

Fig. 10. Potential strands of future research.
I.E. Agbehadji, B.O. Awuzie, A.B. Ngowi, R.C. Millham, "Review of big data in technology and health care."

N. D. de Rijder, A.J.J. Santala, P. Fioretti, R. Aben, B. Violat, M. Santolini, B.G. Tovaraz, S. Strinighini, L. Kaiser, J.F. Pradeau, S. Joost, I. Guessous, "Detection of spatiotemporal clusters of COVID-19-associated symptoms and prevention using a participatory surveillance app: protocol for the cho2m study."

D. Taylor, H. Tibble, E. Mossialos, "Health information technology and digital health: innovation for national learning health and care systems."

P. M. Garrett, "Surveillance capitalism, COVID-19 and social work."

R. Bernard, G. Bowsher, R. Sullivan, "COVID-19 and the rise of participatory sigint: an examination of the rise in government surveillance through mobile applications."

S. Zuboff, "Surveillance Capitalism and the Challenge of Collective Action, 2019, pp. 1085-1097."

I. Guessous, "Detection of spatiotemporal clusters of COVID-19 in China, Arthritis Rheumatol 72 (2020) 1806-1808."